В.А. Галатенко

Стандарты информационной безопасности

ИНТУИТ
НАЦИОНАЛЬНЫЙ ОТКРЫТЫЙ УНИВЕРСИТЕТ

Стандарты информационной безопасности

2-е издание, исправленное

Галатенко В.А.

Национальный Открытый Университет "ИНТУИТ"
2016

УДК 004.738.5.056(075.8)
ББК 21
Г15
Стандарты информационной безопасности / Галатенко В.А. - М.: Национальный Открытый Университет "ИНТУИТ", 2016 (Основы информационных технологий)
ISBN 5-9556-0053-1

В курс включены сведения о стандартах и спецификациях, необходимые всем специалистам в области информационной безопасности (ИБ). Рассматриваются международные, национальные и промышленные стандарты, а также спецификации, разработанные в рамках Internet-сообщества.

Специалистам в области информационной безопасности (ИБ) сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин. Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины. Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в Internet-сообществе это средство действительно работает, и весьма эффективно. С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно. В курсе рассматриваются наиболее важные из них, знание которых необходимо всем или почти всем разработчикам и оценщикам защитных средств, многим сетевым и системным администраторам, руководителям соответствующих подразделений, пользователям. Отбор проводился таким образом, чтобы охватить различные аспекты информационной безопасности, разные виды и конфигурации информационных систем, предоставить полезные сведения для самых разнообразных групп целевой аудитории. Часть стандартов и спецификаций была рассмотрена в курсе "Основы информационной безопасности" и в монографии автора "Информационная безопасность - практический подход"; в данном курсе о них приводятся лишь краткие сведения. Основное внимание уделяется международному стандарту ISO/IEC 15408-1999 и его российскому аналогу ГОСТ Р ИСО/МЭК 15408-2002 "Критерии оценки безопасности информационных технологий", а также спецификациям Internet-сообщества.

Обзор наиболее важных стандартов и спецификаций в области информационной безопасности

Выделяются наиболее важные стандарты и спецификации. Приводятся краткие сведения о стандартах, не являющихся предметом данного курса. Аннотируются спецификации, детально рассматриваемые в последующей части курса.

Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности

Специалистам в области информационной безопасности (ИБ) сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин.

Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины. Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в Internet-сообществе это средство действительно работает, и весьма эффективно.

Отмеченная роль стандартов зафиксирована в основных понятиях закона РФ "О техническом регулировании" от 27 декабря 2002 года под номером 184-ФЗ (принят Государственной Думой 15 декабря 2002 года):

- стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и

утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;

- стандартизация - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Примечательно также, что в число принципов стандартизации, провозглашенных в статье 12 упомянутого закона, входит принцип применения международного стандарта как основы разработки национального, за исключением случаев, если "такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация, в соответствии с установленными процедурами, выступала против принятия международного стандарта или отдельного его положения". С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно. В курсе рассматриваются наиболее важные из них, знание которых необходимо всем или почти всем разработчикам и оценщикам защитных средств, многим сетевым и системным администраторам, руководителям соответствующих подразделений, пользователям.

Отбор проводился таким образом, чтобы охватить различные аспекты информационной безопасности, разные виды и конфигурации информационных систем (ИС), предоставить полезные сведения для самых разнообразных групп целевой аудитории.

На верхнем уровне можно выделить две существенно отличающиеся друг от друга группы стандартов и спецификаций:

- оценочные стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности;

- спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Эти группы, разумеется, не конфликтуют, а дополняют друг друга. Оценочные стандарты описывают важнейшие, с точки зрения информационной безопасности, понятия и аспекты ИС, играя роль организационных и архитектурных спецификаций. Другие спецификации определяют, как именно строить ИС предписанной архитектуры и выполнять организационные требования.

Из числа оценочных необходимо выделить стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" и его интерпретацию для сетевых конфигураций, "Гармонизированные критерии Европейских стран", международный стандарт "Критерии оценки безопасности информационных технологий" и, конечно, Руководящие документы Гостехкомиссии России. К этой же группе относится и Федеральный стандарт США "Требования безопасности для криптографических модулей", регламентирующий конкретный, но очень важный и сложный аспект информационной безопасности.

Технические спецификации, применимые к современным распределенным ИС, создаются, главным образом, "Тематической группой по технологии Internet" (Internet Engineering Task Force, IETF) и ее подразделением - рабочей группой по безопасности. Ядром рассматриваемых технических спецификаций служат документы по безопасности на IP-уровне (IPsec). Кроме этого, анализируется защита на транспортном уровне (Transport Layer Security, TLS), а также на уровне приложений (спецификации GSS-API, Kerberos). Необходимо отметить, что Internet-сообщество уделяет должное внимание административному и процедурному уровням безопасности ("Руководство по информационной безопасности предприятия", "Как выбирать поставщика Интернет-услуг", "Как реагировать на нарушения информационной безопасности").

В вопросах сетевой безопасности невозможно разобраться без освоения спецификаций X.800 "Архитектура безопасности для взаимодействия открытых систем", X.500 "Служба директорий: обзор концепций, моделей и сервисов" и X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов".

Британский стандарт BS 7799 "Управление информационной безопасностью. Практические правила", полезный для руководителей организаций и лиц, отвечающих за информационную безопасность, без сколько-нибудь существенных изменений воспроизведен в международном стандарте ISO/IEC 17799.

Таков, на наш взгляд, "стандартный минимум", которым должны активно владеть все действующие специалисты в области информационной безопасности.

Краткие сведения о стандартах и спецификациях, не являющихся предметом данного курса.

Упоминаемые в данном разделе стандарты и спецификации детально рассмотрены в курсе "Основы информационной безопасности" и в книге "Информационная безопасность - практический подход" [83]. Только по этой причине они не включены в настоящий курс в качестве предмета изучения.

Первым оценочным стандартом, получившим международное признание и оказавшим исключительно сильное влияние на последующие разработки в области информационной безопасности, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, [38]), более известный (по цвету обложки) под названием "Оранжевая книга".

Без преувеличения можно утверждать, что в "Оранжевой книге" заложен понятийный базис ИБ. Достаточно лишь перечислить содержащиеся в нем понятия: безопасная и доверенная системы, политика безопасности, уровень гарантированности, подотчетность, доверенная вычислительная база, монитор обращений, ядро и периметр безопасности. Исключительно важно и выделение таких аспектов политики безопасности, как добровольное (дискреционное) и принудительное (мандатное) управление доступом, безопасность повторного использования объектов. Последним по порядку, но отнюдь не по значению следует назвать принципы классификации по требованиям безопасности на основе параллельного ужесточения

требований к политике безопасности и уровню гарантированности.

После "Оранжевой книги" была выпущена целая "Радужная серия". С концептуальной точки зрения, наиболее значимый документ в ней - "Интерпретация "Оранжевой книги" для сетевых конфигураций" (Trusted Network Interpretation, [68]). Он состоит из двух частей. Первая содержит собственно интерпретацию, во второй описываются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Важнейшее понятие, введенное в первой части, - сетевая доверенная вычислительная база. Другой принципиальный аспект - учет динамичности сетевых конфигураций. Среди защитных механизмов выделена криптография, помогающая поддерживать как конфиденциальность, так и целостность.

Новым для своего времени стал систематический подход к вопросам доступности, формирование архитектурных принципов ее обеспечения.

Упомянем также достаточное условие корректности фрагментирования монитора обращений, являющееся теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

Переходя к знакомству с "Гармонизированными критериями Европейских стран", отметим отсутствие в них априорных требований к условиям, в которых должна работать информационная система. Предполагается, что сначала формулируется цель оценки, затем орган сертификации определяет, насколько полно она достигается, т. е. в какой мере корректны и эффективны архитектура и реализация механизмов безопасности в конкретной ситуации. Чтобы облегчить формулировку цели оценки, стандарт содержит описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем.

В "Гармонизированных критериях" подчеркивается различие между системами и продуктами информационных технологий, но для унификации требований вводится единое понятие - объект оценки.

Важно указание и на различие между функциями (сервисами)

безопасности и реализующими их механизмами, а также выделение двух аспектов гарантированности - эффективности и корректности средств безопасности. Руководящие документы (РД) Гостехкомиссии России [13] начали появляться несколько позже, уже после опубликования "Гармонизированных критериев", и, по аналогии с последними, подтверждают разницу между автоматизированными системами (АС) и продуктами (средствами вычислительной техники, СВТ), но в общем и целом они долгое время следовали в фарватере "Оранжевой книги".

Первое примечательное отклонение от этого курса произошло в 1997 году, когда был принят РД по отдельному сервису безопасности - межсетевым экранам (МЭ) [18]. Его основная идея - классифицировать МЭ на основании осуществляющих фильтрацию потоков данных уровней эталонной семиуровневой модели - получила международное признание и продолжает оставаться актуальной.

В 2002 году Гостехкомиссия России приняла в качестве РД русский перевод [19] международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" [50], что послужило толчком для кардинальной и весьма своевременной со всех точек зрения переориентации (вспомним приведенный выше принцип стандартизации из закона "О техническом регулировании"). Конечно, переход на рельсы "Общих критериев" будет непростым, но главное, что он начался.

Среди технических спецификаций на первое место, безусловно, следует поставить документ X.800 "Архитектура безопасности для взаимодействия открытых систем" [75]. Здесь выделены важнейшие сетевые сервисы безопасности: аутентификация, управление доступом, обеспечение конфиденциальности и/или целостности данных, а также невозможность отказаться от совершенных действий. Для реализации сервисов предусмотрены следующие сетевые механизмы безопасности и их комбинации: шифрование, электронная цифровая подпись (ЭЦП), управление доступом, контроль целостности данных, аутентификация, дополнение трафика, управление маршрутизацией, нотаризация. Выбраны уровни эталонной семиуровневой модели, на которых могут быть реализованы сервисы и механизмы безопасности. Наконец, детально рассмотрены вопросы администрирования средств

безопасности для распределенных конфигураций.

Спецификация Internet-сообщества RFC 1510 "Сетевой сервис аутентификации Kerberos (V5)" [61] относится к более частной, но весьма важной и актуальной проблеме - аутентификации в разнородной распределенной среде с поддержкой концепции единого входа в сеть. Сервер аутентификации Kerberos представляет собой доверенную третью сторону, владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. О весомости данной спецификации свидетельствует тот факт, что клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем. Далее предполагается, что читатель свободно разбирается в особенностях охарактеризованных выше стандартов и спецификаций.

Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций

"Гармонизированные критерии Европейских стран" стали весьма передовым документом для своего времени, они подготовили появление международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" (Evaluation criteria for IT security) [50], в русскоязычной литературе обычно (но не совсем верно) именуемого "Общими критериями" (ОК).

На сегодняшний день "Общие критерии" - самый полный и современный оценочный стандарт . На самом деле, это метастандарт, определяющий инструменты оценки безопасности ИС и порядок их использования; он не содержит предопределенных классов безопасности. Такие классы можно строить, опираясь на заданные требования.

ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям (сервисам) безопасности и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту; они

предъявляются к технологии и процессу разработки и эксплуатации.

Требования безопасности формулируются, и их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или информационной системы.

Подчеркнем, что безопасность в ОК рассматривается не статично, а в соответствии с жизненным циклом объекта оценки. Кроме того, последний предстает в контексте среды безопасности, характеризующейся определенными условиями и угрозами.

"Общие критерии" способствуют формированию двух базовых видов используемых на практике нормативных документов - это профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса.

Задание по безопасности содержит совокупность требований к конкретной разработке, их выполнение позволит решить поставленные задачи по обеспечению безопасности.

В последующей части курса будут детально рассмотрены как сами "Общие критерии", так и разработанные на их основе профили защиты и проекты профилей.

Криптография - область специфическая, но общее представление о ее месте в архитектуре безопасности и о требованиях к криптографическим компонентам иметь необходимо. Для этого целесообразно ознакомиться с Федеральным стандартом США FIPS 140-2 "Требования безопасности для криптографических модулей" (Security Requirements for Cryptographic Modules) [41]. Он выполняет организующую функцию, описывая внешний интерфейс криптографического модуля, общие требования к подобным модулям и их окружению. Наличие такого стандарта упрощает разработку сервисов безопасности и профилей защиты для них.

Криптография как средство реализации сервисов безопасности имеет

две стороны: алгоритмическую и интерфейсную. Нас будет интересовать исключительно интерфейсный аспект, поэтому, наряду со стандартом FIPS 140-2, мы рассмотрим предложенную в рамках Internet-сообщества техническую спецификацию "Обобщенный прикладной программный интерфейс службы безопасности" (Generic Security Service Application Program Interface, GSS-API) [64].

Интерфейс безопасности GSS-API предназначен для защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Он создает условия для взаимной аутентификации общающихся партнеров, контролирует целостность пересылаемых сообщений и служит гарантией их конфиденциальности. Пользователями интерфейса безопасности GSS-API являются коммуникационные протоколы (обычно прикладного уровня) или другие программные системы, самостоятельно выполняющие пересылку данных.

Технические спецификации IPsec [IPsec] имеют, без преувеличения, фундаментальное значение, описывая полный набор средств обеспечения конфиденциальности и целостности на сетевом уровне. Для доминирующего в настоящее время протокола IP версии 4 они носят факультативный характер; в перспективной версии IPv6 их реализация обязательна. На основе IPsec строятся защитные механизмы протоколов более высокого уровня, вплоть до прикладного, а также законченные средства безопасности, в том числе виртуальные частные сети. Разумеется, IPsec существенным образом опирается на криптографические механизмы и ключевую инфраструктуру.

Точно так же характеризуются и средства безопасности транспортного уровня (Transport Layer Security, TLS) [39]. Спецификация TLS развивает и уточняет популярный протокол Secure Socket Layer (SSL), используемый в большом числе программных продуктов самого разного назначения.

В упомянутом выше инфраструктурном плане очень важны рекомендации X.500 "Служба директорий: обзор концепций, моделей и сервисов" (The Directory: Overview of concepts, models and services) [46] и X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов" (The Directory: Public-key and attribute certificate frameworks) [48].

В рекомендациях X.509 описан формат сертификатов открытых ключей и атрибутов - базовых элементов инфраструктур открытых ключей и управления привилегиями.

Как известно, обеспечение информационной безопасности - проблема комплексная, требующая согласованного принятия мер на законодательном, административном, процедурном и программно-техническом уровнях. При разработке и реализации базового документа административного уровня - политики безопасности организации - отличным подспорьем может стать рекомендация Internet-сообщества "Руководство по информационной безопасности предприятия" (Site Security Handbook, см. [44], [42]). В нем освещаются практические аспекты формирования политики и процедур безопасности, поясняются основные понятия административного и процедурного уровней, содержится мотивировка рекомендуемых действий, затрагиваются темы анализа рисков, реакции на нарушения ИБ и действий после ликвидации нарушения. Более подробно последние вопросы рассмотрены в рекомендации "Как реагировать на нарушения информационной безопасности" (Expectations for Computer Security Incident Response) [30]. В этом документе можно найти и ссылки на полезные информационные ресурсы, и практические советы процедурного уровня.

При развитии и реорганизации корпоративных информационных систем, несомненно, окажется полезной рекомендация "Как выбирать поставщика Internet-услуг" (Site Security Handbook Addendum for ISPs) [37]. В первую очередь ее положений необходимо придерживаться в ходе формирования организационной и архитектурной безопасности, на которой базируются прочие меры процедурного и программно-технического уровней.

Для практического создания и поддержания режима информационной безопасности с помощью регуляторов административного и процедурного уровней пригодится знакомство с британским стандартом BS 7799 "Управление информационной безопасностью. Практические правила" (Code of practice for information security management) [28] и его второй частью BS 7799-2:2002 "Системы управления информационной безопасностью - спецификация с руководством по использованию" (Information security management systems - Specification with guidance for use)

[29]. В нем разъясняются такие понятия и процедуры, как политика безопасности, общие принципы организации защиты, классификация ресурсов и управление ими, безопасность персонала, физическая безопасность, принципы администрирования систем и сетей, управление доступом, разработка и сопровождение ИС, планирование бесперебойной работы организации.

Можно видеть, что отобранные для курса стандарты и спецификации затрагивают все уровни информационной безопасности, кроме законодательного. Далее мы приступим к их детальному рассмотрению.

"Общие критерии", часть 1. Основные идеи

Рассматривается история создания "Общих критериев", описывается их текущий статус, анализируются основные идеи.

История создания и текущий статус "Общих критериев"

В 1990 году Рабочая группа 3 Подкомитета 27 Первого совместного технического комитета (JTC1/SC27/WG3) Международной организации по стандартизации (ISO) приступила к разработке "Критериев оценки безопасности информационных технологий " (Evaluation Criteria for IT Security, ECITS). Несколько позже, в 1993 году, правительственные организации шести североамериканских и европейских стран - Канады, США, Великобритании, Германии, Нидерландов и Франции - занялись составлением так называемых " Общих критериев оценки безопасности информационных технологий " (Common Criteria for IT Security Evaluation). За этим документом исторически закрепилось более короткое название - " Общие критерии ", или ОК (Common Criteria, CC).

Рабочая группа ISO, возглавляемая представителем Швеции, функционировала на общественных началах и действовала весьма неторопливо, пытаясь собрать и увязать между собой мнения экспертов примерно из двух десятков стран, в то время как коллектив "Проекта ОК", финансируемый своими правительствами, несмотря на первоначальное трехлетнее отставание, весьма быстро начал выдавать реальные результаты. Объяснить это нетрудно: в "Проекте ОК" требовалось объединить и развить всего три весьма продвинутых и близких по духу документа - "Гармонизированные критерии Европейских стран", а также "Канадские критерии оценки доверенных компьютерных продуктов " и "Федеральные критерии безопасности информационных технологий " (США). (Сами разработчики " Общих критериев " относят к числу первоисточников еще и "Оранжевую книгу".)

Как правило, круг людей, заседающих в комитетах и комиссиях по информационной безопасности, довольно узок, поэтому нет ничего удивительного в том, что одни и те же представители стран (в частности, США и Великобритании) входили в обе группы

разработчиков. Естественно, в таких условиях между коллективом "Проекта ОК" и Рабочей группой 3 установилось тесное взаимодействие. Практически это означало, что группа WG3 стала бесплатным приложением к "Проекту ОК", а сами " Общие критерии " автоматически должны были получить статус не межгосударственного, а международного стандарта.

В ОС Unix есть утилита tee, создающая ответвления каналов путем копирования стандартного вывода в файлы и довольно точно моделирующая взаимоотношения между коллективом "Проекта ОК" и группой WG3. С 1994 года ранние версии ОК становятся рабочими проектами WG3. В 1996 году появилась версия 1.0 " Общих критериев ", которая, помимо публикации в Internet для всеобщего свободного доступа, была одобрена ISO и обнародована в качестве Проекта Комитета.

Широкое открытое обсуждение документа и "опытная эксплуатация" привели к его существенной переработке и выходу версии 2.0 ОК в мае 1998 года. Разумеется, эксперты WG3 не могли ее не отредактировать. Их замечания были учтены в версии 2.1 ОК [31]-[33], принятой в августе 1999 года. (Дополнение: В июле 2005 г. опубликованы новые версии 3.0 ОК и ОМО, в которых предыдущие версии ОК и ОМО подверглись существенной ревизии. В сентябре 2006 года появились версии 3.1 ОК и ОМО, которые и были признаны Управляющим комитетом по Общим критериям официальными версиями ОК и ОМО наряду (на переходный период) с версиями 2.3 ОК и ОМО.) Соответствующий международный стандарт ISO/IEC 15408-1999 [50]-[52] введен в действие с 1 декабря 1999 года. Таким образом, фактически стандарт ISO/IEC 15408-1999 и версия 2.1 ОК совпадают, а если пренебречь описываемыми ниже нюансами, их названия могут считаться взаимозаменяемыми. Однако, строго говоря, "Критерии оценки безопасности информационных технологий " и " Общие критерии оценки безопасности информационных технологий " - разные документы, поскольку выпущены под эгидой разных организаций, руководствующихся разными правилами распространения и обновления.

ISO не предоставляет свободный доступ к своим стандартам, они относительно статичны, поскольку их обновляют или подтверждают

один раз в пять лет (какие-либо изменения в стандарте ISO/IEC 15408 можно ожидать в 2004 году. Дополнение: ООО "Центр безопасности информации" подготовлена первая редакция проекта ГОСТ Р ИСО/МЭК 15408-1 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель". Соответствующее уведомление о разработке проекта государственного стандарта размещено на сайте Федерального агентства по техническому регулированию и метрологии 20.09.2011 г.). Напротив, портал "Проекта ОК" (ссылка: http://www.commoncriteriaportal.org - http://www.commoncriteriaportal.org) открыт для всех желающих, а разработчики " Общих критериев " постоянно предлагают и принимают изменения, уточнения, интерпретации отдельных положений и готовят третью версию своего документа. Поэтому, с формальной точки зрения, международный стандарт ISO/IEC 15408-1999 по-русски правильнее сокращенно именовать КОБИТ, а не ОК. (Правда, велика вероятность, что рабочая группа ISO любезно согласится и дальше пользоваться плодами "Проекта ОК", естественно, внося в них свои редакторские правки...)

Уточним, что далее, в рамках этой темы, мы будем иметь в виду именно " Общие критерии ", а не стандарт ISO.

С целью унификации процедуры сертификации по " Общим критериям " в августе 1999 года была опубликована "Общая методология оценки безопасности информационных технологий " (Common Methodology for Information Technology Security Evaluation) [34], описывающая минимальный набор действий при проведении оценки. "Проект ОК" с самого начала носил не только технический, но и экономико-политический характер. Его цель состояла, в частности, в том, чтобы упростить, удешевить и ускорить выход сертифицированных изделий информационных технологий (ИТ) на мировой рынок. Для этого в мае 2000 года уполномоченные правительственные организации шести стран-основателей "Проекта ОК", а также Австралии и Новой Зеландии, Греции, Италии, Испании, Норвегии, Финляндии и Швеции подписали соглашение "О признании сертификатов по Общим критериям в области безопасности информационных технологий " (позднее к нему присоединились Австрия и Израиль, а в 2003 году — Турция, Венгрия и Япония).

Участие в соглашении предполагает соблюдение двух независимых условий: признание сертификатов, выданных соответствующими органами других стран-участниц, а также возможность осуществления подобной сертификации. Очевидно, от взаимного признания сертификатов выигрывают не только производители, но и потребители изделий ИТ. Что же касается их выдачи, то соглашение предусматривает жесткий контроль при получении и подтверждении этого права (например, предусмотрено проведение так называемых теневых сертификационных испытаний под контролем независимых экспертов). Таким образом, для полноценного участия в соглашении, помимо желания, государство должно располагать органами сертификации с достаточными ресурсами и штатом специалистов, квалификация которых получила официальное международное признание. По данным на конец 2002 года, правом выдачи сертификатов, признаваемых участниками соглашения, обладали Австралия и Новая Зеландия, Великобритания, Германия, Канада, США и Франция.

К началу 2003 года сертификаты по " Общим критериям " получили около семидесяти разнообразных изделий ИТ ведущих производителей: операционные системы, системы управления базами данных, межсетевые экраны, коммуникационные средства, интеллектуальные карты и т.п.; еще почти сорок находились в процессе сертификации.

Определяя статус " Общих критериев " в России, следует отметить, что отечественные специалисты с самого начала внимательно следили за этим проектом, публиковали аналитические обзоры и переводы (см., например, [JI981K]). В 1999 году была организована работа по подготовке российского стандарта и Руководящего документа (РД) Гостехкомиссии России на основе аутентичного перевода ОК. Она велась в тесном контакте с зарубежными коллегами и успешно завершена в 2002 году. Именно тогда был официально издан ГОСТ Р ИСО/МЭК 15408-2002 "Критерии оценки безопасности информационных технологий " 10-[12] с датой введения в действие 1 января 2004 года. А пока положение регулируется РД Гостехкомиссии России [19], который, как и " Общие критерии ", по замыслу разработчиков, должен быть динамичнее стандарта, модифицируясь вместе с ОК.

Российские специалисты - активные участники "Проекта ОК", они

вносят предложения по доработке " Общих критериев ", выступают с докладами на конференциях, ведут научно-исследовательские работы, внедряют ОК в практику различных организаций. Следующим логичным шагом стало бы присоединение России к соглашению "О признании сертификатов ".

Основные понятия и идеи "Общих критериев"

Основным свойством, которым должны обладать действительно общие критерии оценки безопасности информационных технологий, является универсальность. Следовательно, они не должны содержать априорных предположений об объекте оценки. В ОК данное условие выполнено: под объектом оценки (ОО) понимается аппаратно-программный продукт или информационная система с соответствующей документацией.

Система - это специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации.

Продукт, согласно ОК, есть совокупность средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы . В качестве собирательного термина для систем и продуктов применяют словосочетание " изделие ИТ ". Оно может быть как уже существующим, так и проектируемым. В первом случае - доработано по результатам оценки, во втором - сама перспектива подобного контроля способна дисциплинировать разработчиков; так или иначе проведение оценки должно оказать положительное влияние на безопасность ОО.

Объект оценки рассматривается в определенном контексте - среде безопасности, в которую включается все, что имеет отношение к его безопасности, а именно:

- законодательная среда - законы и нормативные акты, затрагивающие ОО;
- административная среда - положения политик и программ безопасности, учитывающие особенности ОО;
- процедурная среда - физическая среда ОО и меры физической защиты, персонал и его свойства (знания, опыт и т.п.), принятые

эксплуатационные и иные процедуры;
- программно-техническая среда - предназначение объекта оценки и предполагаемые области его применения, активы (ресурсы), которые требуют защиты средствами ОО.

Дальнейший этап технологического цикла подготовки к оценке, согласно " Общим критериям ", - описание следующих аспектов среды ОО:

- предположения безопасности. Они выделяют объект оценки из общего контекста, задают границы рассмотрения. Истинность этих предположений принимается без доказательства, а из множества возможных отбирается только то, что заведомо необходимо для обеспечения безопасности ОО;
- угрозы безопасности ОО, наличие которых в рассматриваемой среде установлено или предполагается. Они характеризуются несколькими параметрами: источник, метод воздействия, опасные с точки зрения злонамеренного использования уязвимости, ресурсы (активы), потенциально подверженные повреждению. При анализе рисков принимаются во внимание вероятность активизации угрозы и ее успешного осуществления, а также размер возможного ущерба. По результатам анализа из множества допустимых угроз отбираются только те, ущерб от которых нуждается в уменьшении;
- положения политики безопасности, предназначенные для применения к объекту оценки. Для системы ИТ такие положения могут быть описаны точно, для продукта - в общих чертах.

На основании предположений, при учете угроз и положений политики безопасности формулируются цели безопасности для объекта оценки, направленные на обеспечение противостояния угрозам и выполнение политики безопасности. В зависимости от непосредственного отношения к ОО или к среде они подразделяются на две группы. Часть целей для среды может достигаться нетехническими (процедурными) мерами. Все остальные (для объекта и среды) носят программно-технический характер. Для их достижения к объекту и среде предъявляются требования безопасности.

" Общие критерии " в главной своей части как раз и являются каталогом

(библиотекой) требований безопасности. Спектр стандартизованных требований чрезвычайно широк - это необходимое условие универсальности ОК. Высокий уровень детализации делает их конкретными, допускающими однозначную проверку, что важно для обеспечения повторяемости результатов оценки. Наличие параметров обусловливает гибкость требований, а дополнительную возможность ее достижения (через расширяемость) привносит использование нестандартных (не входящих в каталог ОК) требований.

Для структуризации пространства требований в " Общих критериях " введена иерархия класс - семейство - компонент - элемент.

Классы определяют наиболее общую (как правило, предметную) группировку требований.

Семейства в пределах класса различаются по строгости и другим характеристикам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Между компонентами могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Соответственно, при включении такого компонента необходимо добавить всю "гроздь" его зависимостей.

" Общие критерии " содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности ОО и реализующим их механизмам;
- требования доверия, которые соответствуют пассивному аспекту, предъявляются к технологии и процессу разработки и эксплуатации ОО.

Библиотека функциональных требований составляет вторую часть " Общих критериев ", а каталог требований доверия - третью (первая

часть содержит изложение основных концепций ОК).

Сформулировав функциональные требования, требования доверия и требования к среде, можно приступать к оценке безопасности готового изделия ИТ. Для типовых изделий " Общие критерии " предусматривают разработку типовых совокупностей требований безопасности, называемых профилями защиты (ПЗ).

Для проектируемого изделия за выработкой требований следует разработка краткой спецификации, входящей в задание по безопасности (ЗБ).

(Как вспомогательный элемент, упрощающий создание профилей защиты и заданий по безопасности, могут применяться функциональные пакеты (ФП) - неоднократно используемые совокупности компонентов, объединенных для достижения установленных целей безопасности .)

Краткая спецификация определяет отображение требований на функции безопасности (ФБ). " Общие критерии " не предписывают конкретной методологии или дисциплины разработки изделий ИТ, но предусматривают наличие нескольких уровней представления проекта с его декомпозицией и детализацией. За требованиями безопасности следует функциональная спецификация, затем проект верхнего уровня, необходимое число промежуточных уровней, проект нижнего уровня, после этого, в зависимости от типа изделия, исходный код или схемы аппаратуры и, наконец, реализация в виде исполняемых файлов, аппаратных продуктов и т.п. Между уровнями представления должно демонстрироваться соответствие, то есть все сущности более высоких уровней обязаны фигурировать и "ниже", а "внизу" нет места лишним сущностям, не обусловленным потребностями более высоких уровней.

При проведении оценки изделия ИТ главными являются следующие вопросы:

- отвечают ли функции безопасности ОО функциональным требованиям?
- корректна ли реализация функций безопасности?

Если оба ответа положительны, можно говорить о достижении целей безопасности.

Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий"

"Общая методология оценки безопасности информационных технологий " - второй по важности документ (после " Общих критериев "), подготовленный в рамках "Проекта ОК". Основная цель "Общей методологии" - добиться объективности, повторяемости и воспроизводимости результатов оценки.

Следуя принципам структурной декомпозиции, разработчики выделили в процессе оценки три задачи (этапа):

- входная задача;
- задача оценки;
- выходная задача.

Входная задача имеет дело с представленными для оценки свидетельствами (далее для краткости мы будем именовать их свидетельствами оценки). Ее назначение - убедиться, что версии свидетельств корректны и должным образом защищены.

Обычно для оценки представляются стабильные, официально выпущенные версии свидетельств, однако в ситуациях, когда оценка ведется параллельно разработке или доработке ОО, возможно предъявление рабочих версий. Оценщику вместе со спонсором этого процесса необходимо составить каталог и в дальнейшем производить конфигурационный контроль версий. Он обязан обеспечить защиту свидетельств от изменения и утери, а по окончании процесса оценки возвратить их, поместить в архив или уничтожить.

На всех этапах оценки должна обеспечиваться конфиденциальность.

Задача оценки в общем случае разбивается на следующие подзадачи:

- оценка задания по безопасности ;

- оценка управления конфигурацией ОО;
- оценка документации по передаче ОО потребителю и эксплуатационной документации;
- оценка документации разработчиков;
- оценка руководств;
- оценка поддержки жизненного цикла ОО;
- оценка тестов;
- тестирование;
- оценка анализа уязвимостей.

Нередко проводятся выборочные проверки, когда вместо всего (относительно однородного) множества свидетельств анализируется представительное подмножество, что позволяет сэкономить ресурсы при сохранении необходимого уровня доверия безопасности. Размер выборки должен быть обоснован математически и экономически, но при анализе реализации объекта оценки он должен составлять не менее 20%.

Ошибки, обнаруженные при выборочной проверке, подразделяются на систематические и случайные. После исправления систематической ошибки необходимо произвести новую выборку; после случайной этого не требуется.

Допускается выборочная проверка доказательств, тестов, результатов анализа скрытых каналов, выполнения требований к содержанию и представлению свидетельств, выборочное тестирование.

В остальных ситуациях такой способ можно применять только в исключительных случаях, когда полная проверка требует слишком много ресурсов по сравнению с другими действиями в процессе оценки или когда она не существенно увеличивает доверие безопасности. При этом необходимо обосновать допустимость и целесообразность выборочного подхода.

В "Общей методологии" специально подчеркивается, что сами по себе большие размеры и высокая сложность объекта оценки не оправдывают замены полных проверок выборочными, поскольку для оценки безопасности подобных объектов заведомо требуется много сил и средств.

Необходимый элемент оценки - проверка внутренней согласованности каждого из представленных свидетельств, а также внешней взаимной согласованности различных свидетельств.

Внутренняя согласованность проверяется в первую очередь для сущностей, имеющих несколько представлений: для спецификаций и проектов всех уровней, а также для руководств.

Проверка внешней согласованности производится для описаний функций, параметров безопасности, процедур и событий, связанных с безопасностью, поскольку эти описания могут содержаться в разных документах.

Внутренняя несогласованность высокоуровневых сущностей может иметь глобальные последствия для процесса оценки. Например, выявление противоречий в целях заставляет заново проанализировать требования и функции безопасности.

Разные подзадачи в процессе оценки могут выполняться в произвольном порядке или параллельно, однако существуют зависимости, накладывающие некоторые ограничения на очередность выполнения. Наиболее очевидное из них состоит в том, что анализ задания по безопасности должен выполняться до каких бы то ни было проверок объекта оценки.

Задание по безопасности среди других характеристик объекта оценки определяет его границы и спектр рассматриваемых угроз. Следовательно, процесс и результат оценки одного и того же продукта в сочетании с разными заданиями могут быть разными. Например, если в нем содержатся средства межсетевого экранирования и поддержки виртуальных частных сетей (ВЧС), но в задании по безопасности предусмотрена исключительно защита внутренней сети от внешних угроз, то свойства ВЧС-функций важны лишь в контексте возможности обхода средств экранирования. Даже если ВЧС-функции не обеспечивают конфиденциальности сетевых потоков данных, продукт с таким заданием получит положительную оценку.

(Заметим, что набор проверяемых требований необходим при сертификации не только по " Общим критериям ". Нередко производитель в рекламных целях ограничивается кратким " продукт

сертифицирован", что, по сути, бессодержательно и может ввести в заблуждение потребителя, так как зачастую означает соответствие каким-либо условиям общего характера, вроде отсутствия недекларированных возможностей.)

Важным моментом, обычно вызывающим много вопросов, является анализ уязвимостей и стойкости функций безопасности.

Цель обоих видов проверки заключается в выявлении степени устойчивости объекта оценки по отношению к атакам, выполняемым нарушителем с определенным (низким, умеренным или высоким) потенциалом нападения.

Анализ уязвимостей применяется ко всем функциям безопасности; при этом не делается каких-либо предположений относительно корректности их реализации, сохранения целостности, возможности обхода и т.п.

Анализу стойкости подвергаются только функции безопасности, реализованные с помощью вероятностных или перестановочных механизмов, у которых и проверяется стойкость - базовая, средняя или высокая (базовая означает защищенность от нарушителя с низким потенциалом нападения). В принципе, все вероятностные функции можно считать уязвимыми, а подобный анализ классифицировать как анализ уязвимостей специального вида.

Для успешного нападения необходимо сначала идентифицировать, а затем использовать некоторую уязвимость. Оба действия оцениваются с точки зрения временных затрат, необходимой квалификации, уровня знаний об ОО, характера и продолжительности доступа к ОО, необходимых аппаратно-программных и иных ресурсов.

Перечисленные составляющие не являются независимыми. Высокая квалификация может сэкономить время, а специальное оборудование - упростить и ускорить доступ к ОО. Следовательно, если оценивать каждый параметр количественно, то результирующую функцию, характеризующую серьезность уязвимости, естественно сделать аддитивной.

В таблицах 2.1 - 2.5 содержатся условные баллы, присваиваемые

параметрам уязвимости в зависимости от того, в какой диапазон или на какой уровень они попадают. Для получения общего рейтинга нужно выбрать по одному значению из обоих числовых столбцов всех таблиц и сложить эти десять чисел. При оценке стойкости функций безопасности фаза идентификации не рассматривается (предполагается, что уязвимость известна), поэтому достаточно выбрать и сложить пять чисел из последних столбцов.

Таблица 2.1. Условные баллы, присваиваемые уязвимости в зависимости от времени, которое понадобится для ее идентификации и использования.

Диапазон	Идентификация уязвимости	Использование уязвимости
< 0.5 часа	0	0
< суток	2	3
< месяца	3	5
> месяца	5	8

Таблица 2.2. Условные баллы, присваиваемые уязвимости в зависимости от уровня квалификации, необходимого для ее идентификации и использования.

Уровень	Идентификация уязвимости	Использование уязвимости
Любитель	0	0
Специалист	2	2
Эксперт	5	4

Таблица 2.3. Условные баллы, присваиваемые уязвимости в зависимости от уровня знаний об объекте оценки, необходимого для ее идентификации и использования.

Уровень	Идентификация уязвимости	Использование уязвимости
Отсутствие знаний	0	0
Общедоступные знания	2	2
Конфиденциальные сведения	5	4

Таблица 2.4. Условные баллы, присваиваемые уязвимости в зависимости от времени доступа к объекту оценки, требуемого для ее

идентификации и использования.

Диапазон	Идентификация уязвимости	Использование уязвимости
< 0.5 часа или доступ незаметен	0	0
< суток	2	4
< месяца	3	6
> месяца	4	9

Таблица 2.5. Условные баллы, присваиваемые уязвимости в зависимости от аппаратно-программных и иных ресурсов (оборудования), необходимых для ее идентификации и использования.

Уровень	Идентификация уязвимости	Использование уязвимости
Отсутствие оборудования	0	0
Стандартное оборудование	1	2
Специальное оборудование	3	4
Заказное оборудование	5	6

Если уязвимость можно идентифицировать и/или использовать несколькими способами, для каждого из них вычисляется рейтинг и из полученных значений выбирается минимальное, то есть уязвимость характеризуется самым простым методом успешного нападения.

В табл. 2.6 приведены диапазоны рейтинга, которые характеризуют стойкость функции безопасности.

Таблица 2.6. Диапазоны рейтинга, характеризующие стойкость функции безопасности.

Диапазон	Стойкость функции безопасности
10 - 17	Базовая
18 - 24	Средняя

> 24	Высокая

Согласно "Общей методологии", потенциал нападения оценивается в общем и целом по той же схеме, что и степень риска от наличия уязвимостей, с некоторыми очевидными отличиями (например, из нескольких сценариев нападения выбирается худший, с наибольшим потенциалом). Считается, что он является функцией уровня мотивации злоумышленника, его квалификации и имеющихся ресурсов. Мотивация влияет на выделяемое на атаки время и, возможно, на привлекаемые ресурсы и подбор нападающих.

В табл. 2.7 приведены диапазоны рейтинга, иллюстрирующие определенный потенциал нападения.

Таблица 2.7. Диапазоны рейтинга, характеризующие потенциал нападения.

Диапазон	Потенциал нападения
< 10	Низкий
10 - 17	Умеренный
18 - 24	Высокий
> 24	Нереально высокий

Нападение может быть успешным, только если его потенциал не меньше рейтинга уязвимости. Отсюда следует, в частности, что уязвимости с рейтингом выше 24 устойчивы к нападению с высоким потенциалом, поэтому их практическое использование злоумышленниками представляется нереальным.

Отметим, что потенциал предполагаемых нападений на ОО выявляется дважды: при анализе задания по безопасности для выбора надлежащих мер противодействия и при анализе уязвимостей для определения достаточности выбранных мер и качества их реализации.

Рассмотрим пример анализа стойкости функции безопасности. Пусть доступ к информационной системе осуществляется посредством территориально разнесенных терминалов, работа за которыми не контролируется. Авторизованные пользователи проходят

аутентификацию путем введения паролей, состоящих из четырех различных цифр. Если пароль введен неверно, терминал блокируется на одну минуту. Требуется оценить стойкость такой парольной защиты для заданного пользователя с известным нападающему входным именем. Для нападения выбран один терминал, временем ввода можно пренебречь.

Очевидно, число возможных парольных последовательностей составляет

10*9*8*7 = 5040

Для успешного подбора пароля методом полного перебора требуется примерно 2520 попыток, которые можно произвести за 42 часа, что больше суток, но меньше месяца. Никакой квалификации, знаний и/или оборудования для этого не нужно. Следовательно, чтобы определить стойкость функции, достаточно сложить два числа: 5 из табл. 2.1 и 6 из табл. 2.4. Сумма 11 позволяет сделать вывод, что данная функция безопасности обладает базовой стойкостью и является устойчивой к нападению с низким потенциалом.

Возвращаясь к трем основным задачам процесса оценки, рассмотрим последнюю, выходную задачу. Ее цель - сформулировать замечания и получить технический отчет оценки.

Текст с замечаниями не является обязательным. Он нужен, если в процессе оценки выявились какие-либо неясности или проблемы.

Технический отчет оценки - это главный выходной документ, от качества которого во многом зависит повторяемость и воспроизводимость результатов оценки, т. е. возможность их многократного использования. "Общая методология" предписывает следующую структуру подобных отчетов:

- введение;
- архитектурное (высокоуровневое) описание объекта оценки с рассмотрением основных компонентов ;
- описание процесса оценки, примененных методов, методологий, инструментальных средств и стандартов;
- представление результатов оценки;

- выводы и рекомендации;
- список представленных свидетельств;
- список сокращений, словарь терминов;
- список замечаний.

Изучение "Общей методологии" полезно не только оценщикам, но и разработчикам, так как дает представление о вопросах, которые могут возникать в процессе оценки. К сожалению, более детальное рассмотрение этого документа выходит за рамки настоящего курса.

"Общие критерии", часть 2. Функциональные требования безопасности

Детально рассматриваются семейства функциональных требований безопасности, представленные в "Общих критериях". Анализируются достоинства и недостатки принятого в них подхода.

Классификация функциональных требований безопасности

Часть 2 "Общих критериев", представляющая собой весьма обширную библиотеку функциональных требований безопасности, описывает 11 классов, 66 семейств, 135 компонентов и содержит сведения о том, какие цели безопасности могут быть достигнуты при современном уровне информационных технологий и каким образом.

Аналогия между библиотекой функциональных требований безопасности и библиотекой программных модулей является в данном случае довольно полной. Функциональные компоненты могут быть не до конца конкретизированы, поэтому фактические параметры подставляются не в самих "Общих критериях", а в определенных профилях защиты, заданиях по безопасности и функциональных пакетах. (Правда, в ГОСТ Р ИСО/МЭК 15408-2002 параметризация не очень удачно названа "назначением".) В качестве параметров могут выступать весьма сложные сущности, такие, например, как политика безопасности (ПБ).

Некоторые функциональные компоненты "Общих критериев" задаются "с запасом", в них включается список возможностей, из которых затем с помощью соответствующей операции выбирается только то, что нужно в конкретной ситуации. Пример - обнаружение и/или предотвращение определенных нарушений политики безопасности. На программистском языке подобный отбор называется частичным применением.

Разумеется, любой функциональный компонент допускает многократное использование (например, чтобы охватить разные аспекты объекта оценки), называемое в ОК итерацией , а также уточнение и добавление дополнительных деталей (последнее можно считать еще одной формой

частичного применения).

Между компонентами функциональных требований, как и между привычными библиотечными функциями, могут существовать зависимости. Они возникают, когда компонент не является самодостаточным и для своей реализации нуждается в привлечении других компонентов. Очевидно, размещая в ПЗ, ЗБ или ФП подобный компонент, нужно включить туда и всю гроздь зависимостей (это похоже на разрешение внешних ссылок при формировании выполняемого модуля).

Классы функциональных требований "Общих критериев" можно разделить в зависимости от того, описывают ли они элементарные сервисы безопасности или производные, реализуемые на основе элементарных, направлены ли они на достижение высокоуровневых целей безопасности или играют инфраструктурную роль.

К первой группе относятся следующие классы:

- FAU - аудит безопасности (описывает требования к сервису протоколирования/аудита);
- FIA - идентификация / аутентификация ;
- FRU - использование ресурсов (прежде всего - обеспечение отказоустойчивости).

Классы второй группы:

- FCO - связь (обслуживает неотказуемость отправителя/ получателя);
- FPR - приватность ;

Достичь высокоуровневых целей безопасности помогают два класса:

- FDP - защита данных пользователя;
- FPT - защита функций безопасности объекта оценки.

Наиболее многочисленны классы, играющие инфраструктурную роль:

- FCS - криптографическая поддержка (обслуживает управление

криптографическими ключами и криптографические операции);
- FMT - управление безопасностью ;
- FTA - доступ к объекту оценки (управление сеансами работы пользователей);
- FTP - доверенный маршрут / канал.

Приведенная классификация содержит несколько примечательных моментов. Во-первых, функциональные требования ОК довольно разнородны. Трудно объяснить, например, почему протоколированию/ аудиту соответствует собственный класс, а такой важнейший, без преувеличения, классический сервис безопасности, как управление доступом, "спрятан" среди других требований защиты данных пользователя.

Во-вторых, в ОК не выделены архитектурные требования. Правда, некоторые весьма важные архитектурные компоненты, в числе которых - посредничество при обращениях (частный случай невозможности обхода защитных средств) и разделение доменов, вошли в класс FPT (защита функций безопасности).

В-третьих, требования для защиты данных пользователя и функций безопасности объекта оценки разделены, хотя, очевидно, в обоих случаях необходимо применять сходные механизмы. Возможно, такой подход объясняется желанием выделить ядро безопасности и сохранить его компактность.

Далее мы кратко рассмотрим все 11 классов функциональных требований безопасности "Общих критериев".

Классы функциональных требований, описывающие элементарные сервисы безопасности

В этом разделе рассматриваются три класса функциональных требований безопасности:

- FAU - аудит безопасности ;
- FIA - идентификация / аутентификация ;
- FRU - использование ресурсов.

Класс FAU состоит из шести семейств, содержащих требования к отбору, протоколированию (регистрации), хранению и анализу данных о действиях и событиях, затрагивающих безопасность объекта оценки.

Семейство FAU_GEN (генерация данных аудита безопасности) включает два компонента. Первый, FAU_GEN.1 (генерация данных аудита), специфицирует потенциально подвергаемые протоколированию и аудиту события, вводит понятие уровня протоколирования (минимальный, базовый, детализированный, неопределенный), определяет минимум регистрационных данных о событии (дата, время, тип, результат события, а также идентификатор субъекта). Второй, FAU_GEN.2 (ассоциация идентификатора пользователя), предписывает ассоциировать каждое потенциально регистрируемое событие с идентификатором пользователя, его инициирующего.

Семейство FAU_SEL (выбор событий аудита безопасности) определяет требования к средствам отбора (включения или исключения) событий из числа потенциально регистрируемых, которые будут реально протоколироваться и подвергаться аудиту в процессе функционирования объекта оценки. Отбор может производиться на основе таких атрибутов, как идентификаторы объекта, пользователя, субъекта, узла сети или тип события. Предусматривается задание дополнительных атрибутов.

Семейство FAU_STG (хранение событий аудита безопасности) содержит две пары компонентов. Первая, FAU_STG.1 (защищенное хранение журнала аудита) и FAU_STG.2 (гарантии доступности данных аудита), специфицирует защиту регистрационного журнала от несанкционированного удаления, модификации, а также от повреждения регистрационных данных при его переполнении, сбое или атаке. Вторая пара, FAU_STG.3 (действия в случае возможной потери данных аудита) и FAU_STG.4 (предотвращение потери данных аудита), определяет последовательность действий, если объем информации в регистрационном журнале превышает заранее заданный порог. В их число входят игнорирование и своевременное запрещение протоколируемых событий, запись поверх самых старых регистрационных данных и т.д.

Семейство FAU_SAR (просмотр аудита безопасности) предоставляет право на чтение (полное или выборочное, на основе критериев с логическими отношениями) регистрационного журнала уполномоченным пользователям и запрет на доступ к журналу для прочих пользователей.

Семейство FAU_SAA (анализ аудита безопасности) устанавливает требования к средствам автоматического анализа функционирования объекта оценки, позволяющим выявлять возможные нарушения безопасности. Базовым компонентом семейства является FAU_SAA.1 (анализ потенциального нарушения), регламентирующий применение набора правил, основанных на накоплении или объединении событий, сигнализирующих о вероятном нарушении безопасности. В рамках семейства этот компонент усилен по двум направлениям. В FAU_SAA.2 (выявление аномалий, опирающееся на профиль) вводится понятия профиля поведения, рейтинга подозрительной активности для каждого пользователя, чьи действия отражены в профиле, а также порога, превышение которого указывает на ожидаемое нарушение политики безопасности. FAU_SAA.3 (простая эвристика атаки) и FAU_SAA.4 (сложная эвристика атаки) содержит понятие сигнатуры атаки (разной степени сложности) и специфические функции выявления сигнатур в реальном масштабе времени.

Шестое семейство класса FAU - FAU_ARP (автоматическая реакция аудита безопасности) - определяет действия, которые необходимо предпринять при выявлении возможных нарушений безопасности. Действия эти характеризуются как "наименее разрушительные".

Можно сделать вывод, что в "Общих критериях" нашли отражение такие важные достижения относительно недавнего прошлого, как разработка и применение методов активного аудита.

Шесть семейств класса FIA (идентификация / аутентификация) содержат требования к функциям установления и проверки подлинности заявленного идентификатора пользователя, а также связывания атрибутов безопасности с уполномоченным пользователем.

Семейство FIA_UID (идентификация пользователя) включает два компонента и определяет набор действий (например, получение справочной информации), которые разрешается выполнять до

идентификации. Обычно применяют более сильный компонент FIA_UID.2 - идентификация до любых действий, выполняемых пользователем при посредничестве функций безопасности.

Семейство FIA_UAU (аутентификация пользователя) устроено сложнее. Оно специфицирует типы механизмов аутентификации и используемые при этом атрибуты. Два первых компонента, FIA_UAU.1 (выбор момента аутентификации) и FIA_UAU.2 (аутентификация до любых действий пользователя), играют (применительно к аутентификации) ту же роль, что и компоненты семейства FIA_UID. На реализацию надежной аутентификации, устойчивой к сетевым угрозам, направлены компоненты FIA_UAU.3 (аутентификация, защищенная от подделок), FIA_UAU.4 (механизмы одноразовой аутентификации) и FIA_UAU.5 (сочетание механизмов аутентификации). После периода неактивности пользователя и в ряде других ситуаций уместно применение компонента FIA_UAU.6 (повторная аутентификация). Наконец, FIA_UAU.7 (аутентификация с защищенной обратной связью) указывает, как отображать пароль при вводе.

Семейство FIA_ATD (определение атрибутов пользователя) предусматривает наличие у пользователей не только идентификаторов, но и других атрибутов безопасности, предписываемых политикой безопасности.

Обычно после успешной идентификации и аутентификации от имени пользователя начинает действовать некий процесс (субъект). Семейство FIA_USB (связывание пользователь-субъект) содержит требования по ассоциированию атрибутов безопасности пользователя с этим субъектом.

Выявлением и реагированием на неудачи аутентификации ведает семейство FIA_AFL (отказы аутентификации). Разумеется, и число допустимых неудачных попыток, и действия, выполняемые при превышении порога неудач, - все это параметры единственного компонента семейства.

Обычно пользователь доказывает свою подлинность, сообщая нечто, что знает только он ("секрет" в терминологии ОК). Семейство FIA_SOS (спецификация секретов) вводит понятие метрики качества секретов и содержит требования к средствам проверки качества и генерации

секретов заданного качества. Примеры подобных средств - проверка выполнения технических ограничений на пользовательские пароли в ОС Unix и программные генераторы паролей.

В целом класс FIA, по сравнению с FAU, менее конкретен, его компоненты слишком параметризованы. Вероятно, это связано с тем, что криптография, без которой надежная и удобная для пользователя аутентификация невозможна, находится вне рамок "Общих критериев".

Класс FRU (использование ресурсов) включает три семейства, призванные разными способами поддерживать высокую доступность.

Выполнение требований семейства FRU_FLT (отказоустойчивость) должно обеспечить корректную работу всех или хотя бы некоторых функций объекта оценки даже в случае сбоев.

FRU_PRS (приоритет обслуживания) регламентирует действия по защите высокоприоритетных операций от препятствий или задержек со стороны операций с более низким приоритетом.

Семейство FRU_RSA (распределение ресурсов) для достижения высокой доступности ресурсов привлекает механизм квот.

Обращение к вопросу высокой доступности - несомненное достоинство "Общих критериев", которое, к сожалению, несколько проигрывает из-за отсутствия системного подхода. По неясным причинам в качестве сущностей одного уровня выделен один из трех высокоуровневых аспектов доступности и два механизма, способствующих ее поддержанию.

За пределами рассмотрения остались надежность и обслуживаемость, да и отказоустойчивость может достигаться очень разными способами - от использования многопроцессорных конфигураций до организации резервных вычислительных центров.

Помимо двух рассмотренных механизмов поддержания доступности существуют и другие, не менее важные, например, балансировка загрузки, проактивное управление и т.п. На наш взгляд, было бы целесообразным обобщить требования к доступности регистрационного журнала (см. выше семейство FAU_STG) на случай произвольных

ресурсов.

Отметим также, что включение в класс FRU конкретных механизмов еще резче обозначает излишнюю обобщенность требований класса FIA.

Классы функциональных требований, описывающие производные сервисы безопасности

Мы приступаем к рассмотрению двух следующих классов функциональных требований безопасности:

- FCO - связь;
- FPR - приватность.

Класс FCO состоит из двух семейств, FCO_NRO и FCO_NRR, ведающих неотказуемостью (невозможностью отказаться от факта отправки или получения данных), которая достигается путем избирательной или принудительной генерации допускающих верификацию свидетельств, позволяющих ассоциировать атрибуты отправителя (получателя) с элементами передаваемых данных.

Класс FPR (приватность) содержит четыре семейства функциональных требований, обеспечивающих защиту пользователя от раскрытия и несанкционированного использования его идентификационных данных.

Семейство FPR_ANO (анонимность) дает возможность выполнения действий без идентификатора пользователя. Анонимность может быть полной или выборочной. В первом случае функции безопасности обязаны предоставить заданный набор услуг без запроса идентификатора пользователя. Во втором предусмотрено более слабое требование, в соответствии с которым идентификатор может запрашиваться, но должен скрываться от заранее указанных пользователей и/или субъектов.

Семейство FPR_PSE (псевдонимность) обеспечивает условия, когда пользователь может использовать ресурс или услугу без раскрытия своего идентификатора, оставаясь в то же время подотчетным за свои

действия. Базовый компонент семейства, FPR_PSE.1, предписывает выборочную анонимность, а также наличие средств генерации заданного числа псевдонимов и определения или принятия псевдонима от пользователя с верификацией соответствия некоторой метрике псевдонимов. Эти требования дополняются в компоненте FPR_PSE.2 (обратимая псевдонимность) возможностью определения доверенными субъектами идентификатора пользователя по представленному псевдониму, а в компоненте FPR_PSE.3 (альтернативная псевдонимность) - возможностью оперативного перехода на новый псевдоним, связь которого со старым проявляется лишь в заранее оговоренных ситуациях.

Семейство FPR_UNL (невозможность ассоциации) содержит единственный компонент, предусматривающий неоднократное применение пользователем информационных сервисов, не позволяя заданным субъектам ассоциировать их между собой и приписывать одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (см. выше компонент FAU_SAA.2).

Самым сложным в классе FPR является семейство FPR_UNO (скрытность). Его требования направлены на то, чтобы пользователь мог незаметно для кого бы то ни было работать с определенными информационными сервисами. Наиболее интересны два из четырех имеющихся компонентов семейства. FPR_UNO.2 (распределение информации, влияющее на скрытность) предписывает рассредоточить соответствующие данные по различным частям объекта оценки. Это одно из немногих архитектурных требований "Общих критериев" (правда, выраженное в очень общей форме). В некотором смысле противоположную роль играет компонент FPR_UNO.4 (открытость для уполномоченного пользователя), согласно которому уполномоченные пользователи должны иметь возможность наблюдать за тем, как употребляются заданные ресурсы и/или услуги. (Как сказал один пессимист: "Я так и знал, что этим все кончится!")

Требования приватности ставят очень серьезную проблему многоаспектности информационной безопасности, заставляют искать баланс конфликтующих интересов субъектов информационных отношений. Разработчики заданий по безопасности должны учесть и конкретизировать эти требования с учетом действующего

законодательства и специфики систем ИТ.

Защита данных пользователя

Мы переходим к рассмотрению классов функциональных требований, направленных на достижение высокоуровневых целей безопасности.

К высокоуровневым целям безопасности относятся защита данных пользователя и защита функций безопасности объекта оценки. Соответствующие классы функциональных требований характеризуются большим числом входящих в них семейств и разнородностью компонентов.

Класс FDP (защита данных пользователя) включает тринадцать семейств, которые можно разбить на четыре группы:

- политики защиты данных пользователя;
- виды защиты данных пользователя;
- импорт и экспорт данных пользователя ;
- защита данных пользователя при передаче между доверенными изделиями ИТ.

В первую группу входят два семейства - FDP_ACC (политика управления доступом) и FDP_IFC (политика управления информационными потоками), - играющие, по сути, формальную роль именования политик, распространяющихся на определенные множества субъектов, объектов (потоков) и операций. Управление может быть ограниченным и полным. В последнем случае требуется, чтобы все операции всех субъектов на любом объекте (потоке) из области действия функций безопасности были охвачены некоторой политикой.

Вторая группа объединяет семь семейств. Содержательные аспекты управления доступом (информационными потоками) регламентируются семействами FDP_ACF (функции управления доступом) и FDP_IFF (функции управления информационными потоками). Первое устроено очень просто, состоит из одного компонента и требует наличия политик, основанных на атрибутах безопасности, а также дополнительных правил, явно разрешающих или запрещающих доступ.

Требования к функциям управления информационными потоками, представленные шестью компонентами, существенно сложнее и многообразнее. Компонент FDP_IFF.1 аналогичен FDP_ACF.1. Усиливающий его компонент FDP_IFF.2 требует поддержки многоуровневых политик, основанных на иерархических атрибутах (метках) безопасности. FDP_IFF.3, FDP_IFF.4 и FDP_IFF.5 направлены, соответственно, на ограничение пропускной способности, частичное или полное устранение скрытых каналов. Наконец, FDP_IFF.6 требует осуществления мониторинга скрытых каналов, пропускная способность которых превышает заданный порог.

Семейство FDP_DAU (аутентификация данных) обслуживает один из видов статической целостности данных. В соответствии с его требованиями функции безопасности должны предоставить возможность генерировать и верифицировать свидетельства правильности определенных объектов или типов информации (компонент FDP_DAU.1), а также (усиливающий компонент FDP_DAU.2) идентификатора пользователя, создавшего свидетельство.

Отметим, что компонент FDP_DAU.2 ведает неотказуемостью авторства, а рассмотренный выше класс FCO - неотказуемостью отправки и получения данных, что можно считать разновидностью динамической целостности.

Семейство FDP_ITT (передача в пределах ОО) содержит требования, связанные с защитой данных пользователя при их передаче по внутренним каналам объекта оценки. Предусматривается базовая защита внутренней передачи (FDP_ITT.1), направленная на предотвращение раскрытия, модификация ситуаций недоступности, а также мониторинг целостности данных (FDP_ITT.3). При обнаружении ошибок целостности должны выполняться заданные действия. Эти требования усиливаются, соответственно, компонентами FDP_ITT.2 и FDP_ITT.4 за счет раздельной передачи данных, обладающих разными атрибутами безопасности.

Согласно требованиям семейства FDP_RIP (защита остаточной информации), унаследованным от "Оранжевой книги", функции безопасности должны обеспечить уничтожение любого предыдущего содержания ресурсов при их выдаче и/или освобождении.

Семейство FDP_ROL (откат) предусматривает возможность отмены последней операции и возврат к предшествующему состоянию с сохранением целостности данных пользователя.

Последнее семейство второй группы, FDP_SDI (целостность хранимых данных), содержит требования мониторинга целостности всех контролируемых объектов и выполнения заданных действий при обнаружении ошибок целостности хранимых данных.

В третью группу семейств класса FDP, обслуживающую импорт и экспорт данных пользователя в/за пределы области действия функций безопасности объекта оценки, мы включили, как и следовало ожидать, два сходных по структуре двухкомпонентных семейства: FDP_ETC (экспорт) и FDP_ITC (импорт). Они различаются по наличию или отсутствию (использованию или игнорированию) ассоциированных с данными атрибутов безопасности. Согласованная интерпретация атрибутов оговорена экспортером и импортером.

В последнюю, четвертую группу (защита данных пользователя при передаче между доверенными изделиями ИТ) входят два семейства, ведающих обеспечением конфиденциальности (FDP_UCT) и целостности (FDP_UIT). Имеется в виду, что одним из доверенных изделий является объект оценки, а для передачи используются внешние (по отношению к ОО) каналы.

FDP_UCT состоит из одного компонента, требующего защиты от несанкционированного раскрытия.

В семейство FDP_UIT включены более содержательные требования. Во-первых, предусматривается всеобъемлющая защита от модификации, удаления, вставки и повторения данных. Во-вторых, обнаруженная ошибка целостности может быть восстановлена как с помощью отправителя, доверенного изделия ИТ, так и силами самого объекта оценки.

Обратим внимание на различие требований к защите данных пользователя при передаче по внутреннему (семейство FDP_ITT) и внешнему (семейства FDP_UCT и FDP_UIT) каналам, что можно считать проявлением гибкости "Общих критериев". Для внешних каналов требования заданы более детально (особенно это касается

целостности), однако не предусматривается обеспечение высокой доступности данных.

Отметим также, что за различные аспекты целостности данных пользователя отвечают пять семейств: FDP_DAU, FDP_ITT (точнее, компонент FDP_ITT.3), FDP_ROL, FDP_SDI и FDP_UIT. Первое контролирует аутентичность избранных наборов данных, компонент FDP_ITT.3 и семейство FDP_UIT отвечают за (динамическую) целостность передаваемых данных, FDP_ROL - за восстановление целостности после сбоев или ошибок, а FDP_SDI предусматривает тотальный мониторинг статической целостности.

На практике эти варианты целостности контролируются и восстанавливаются разными методами (например, для выполнения требований FDP_DAU естественно воспользоваться криптографическими хэш-функциями или цифровой подписью, для FDP_SDI - обычными контрольными суммами), поэтому разнесение требований, относящихся к одному аспекту ИБ, представляется в данном случае оправданным, хотя, на наш взгляд, предпочтительнее было бы ограничиться уровнем компонентов, а не семейств. Примером могут служить рассмотренные выше компоненты FAU_SAA.2 и FAU_SAA.4, обслуживающие различные методы выявления подозрительной активности.

Защита функций безопасности объекта оценки

Мы продолжаем рассмотрение классов функциональных требований, направленных на достижение высокоуровневых целей безопасности.

Класс FPT (защита функций безопасности объекта оценки) включает шестнадцать семейств (больше, чем какой-либо другой класс функциональных требований), которые можно разбить на четыре группы:

- архитектурная безопасность ;
- защита реализации функций безопасности;
- защита данных функций безопасности;
- инфраструктурные требования.

Важнейший принцип архитектурной безопасности - невозможность обхода защитных средств. Семейство FPT_RVM (посредничество при обращениях) предназначено для достижения этой цели. Входящий в него единственный компонент FPT_RVM.1 (невозможность обхода политики безопасности ОО) предписывает, чтобы функции, проводящие в жизнь политику безопасности, вызывались и успешно выполнялись прежде любого другого действия, предусмотренного ПБ.

Еще один фундаментальный принцип архитектурной безопасности поддерживается семейством FPT_SEP (разделение доменов). Минимально необходимо отделение домена функций безопасности (компонент FPT_SEP.1), то есть функции безопасности должны поддерживать домен безопасности, который защищает их от вмешательства не облеченных доверием субъектов и искажений с их стороны (кроме того, должно быть реализовано разделение доменов безопасности субъектов). Максимальный уровень потребует реализации полного монитора обращений (компонент FPT_SEP.3), то есть предоставление отдельного домена той части функций безопасности, которая проводит в жизнь политики управления доступом и/или информационными потоками.

Защитой реализации функций безопасности занимаются четыре семейства. Самое простое из них (по формулировке, но не по воплощению и/или проверке), FPT_FLS (безопасность при сбое), содержит требование, чтобы политика безопасности не нарушалась при сбоях заданных типов.

Обеспечения высокой доступности и корректной работы функций безопасности вопреки возможным сбоям добивается и более сложное семейство FPT_RCV (надежное восстановление). FPT_RCV.4 (восстановление функции) предписывает, что функция безопасности либо нормально завершается, либо, для предусмотренных сценариев сбоев, восстанавливается ее устойчивое и безопасное состояние. Первые три его компонента отвечают за восстановление - ручное, автоматическое и автоматическое без недопустимой потери. Для ручного восстановления требуется, чтобы после сбоя функции безопасности перешли в режим аварийной поддержки, оставляющего возможность возврата ОО к безопасному состоянию. Автоматическое восстановление без недопустимой потери означает следующее:

- при сбоях заданных типов возврат к безопасному состоянию обеспечивается автоматическими процедурами;
- безопасное состояние восстанавливается без превышения заранее определенной меры потери данных;
- функции безопасности помогают выяснить, какие объекты могут быть восстановлены, а какие нет.

Семейство FPT_PHP (физическая защита) требует наличия средств выявления и реагирования на несанкционированный физический доступ к частям ОО, участвующим в реализации функций безопасности. Компонент FPT_PHP.1 (пассивное обнаружение физического нападения) можно отнести к средствам контроля целостности, так как он требует однозначного обнаружения физического воздействия, которое может угрожать выполнению функций безопасности; информация о наличии или отсутствии подобного воздействия предоставляется по запросу. Усиливающий компонент FPT_PHP.2 (оповещение о физическом нападении) предусматривает постоянный контроль за определенными элементами и оповещение назначенного пользователя о подобных происшествиях. Наконец, компонент FPT_PHP.3 (противодействие физическому нападению) требует автоматической реакции, предотвращающей нарушение политики безопасности.

Семейство FPT_TST (самотестирование функций безопасности) состоит из одного компонента, но служит сразу двум целям: выполняет собственно самотестирование (при запуске, периодически, по запросу уполномоченного пользователя и т.п.), а также осуществляет контроль целостности данных и выполняемого кода функций.

Объединение в одном компоненте двух существенно разных видов требований представляется странным (тестирование имеет мало общего с контролем целостности кода и, тем более, изменяемых данных), но позволяет плавно перейти к третьей группе семейств класса FPT (защита данных функций безопасности). В эту группу входят шесть семейств, три из которых, FPT_ITA, FPT_ITC и FPT_ITI, отвечают, соответственно, за доступность, конфиденциальность и целостность экспортируемых данных функций безопасности. Отметим, что доступность должна быть обеспечена с заданной вероятностью, а контроль целостности в общем случае предусматривает возможность

восстановления поврежденных данных удаленным доверенным изделием ИТ.

Семейство FPT_TDC содержит требование согласованной интерпретации данных, совместно используемых функциями безопасности ОО и другим доверенным изделием ИТ. Явных требований к контролю импортируемых данных в классе FPT (в отличие от FDP) нет, хотя из соображений симметрии они, безусловно, должны присутствовать (см. выше семейства FDP_ETC и FDP_ITC).

Пятое семейство группы, FPT_ITT (передача данных функций безопасности в пределах объекта оценки), аналогично рассмотренному ранее семейству из класса защиты данных пользователя FDP_ITT (передача в пределах ОО), но не предусматривает обеспечения доступности и разделения по атрибутам при контроле целостности. Справедливости ради укажем, однако, что в компоненте FPT_ITT.3 более детально специфицированы обнаруживаемые виды нарушений целостности: модификация, подмена, перестановка, удаление данных.

Семейство FPT_TRC отвечает за согласованность данных функций безопасности при дублировании в пределах ОО. Здесь следует обратить внимание на требования элемента FPT_TRC.1.2: если части ОО, содержащие дублируемые данные, были разъединены, необходимо обеспечить согласованность таких данных после восстановления соединения перед обработкой запросов к заданным функциям безопасности. Отметим, что к взаимодействию с удаленным доверенным изделием ИТ требование согласованности данных не предъявляется. В целом же остается неясным смысл разнесения по разным классам требований защиты данных пользователя и функций безопасности. Последние, кроме того, трактуются как одноуровневые, для них не предусмотрено разделение по атрибутам, что для сложных систем может оказаться неприемлемым.

Требования, которые мы назвали инфраструктурными, вошли в состав четырех семейств. Семейство FPT_AMT (тестирование базовой абстрактной машины) определяет требования к тестированию, демонстрирующему правильность предположений, обеспечиваемых абстрактной машиной (аппаратно-программной платформой), лежащей в основе функций безопасности.

Семейство FPT_RPL (обнаружение повторного использования) нацелено на выявление повторного использования сущностей различных типов (например, сообщений, запросов на обслуживание и ответов на запросы) и выполнение заданных ответных действий.

Семейство FPT_SSP (протокол синхронизации состояний) на самом деле содержит требования одностороннего или взаимного надежного подтверждения при обмене данными между функциями безопасности в распределенной среде.

Наконец, семейство FPT_STM (метки времени) требует предоставления надежных меток времени в пределах объекта оценки. Подобные метки необходимы, например, функциям протоколирования и управления.

Классы функциональных требований, играющие инфраструктурную роль

Криптографические механизмы - обязательный элемент защищенных систем. Класс FCS (криптографическая поддержка) состоит из 2 семейств, где в самом общем виде (точнее, в виде параметризованных шаблонов) рассматриваются генерация, распределение, доступ и уничтожение ключей, а также криптографические операции. Смысл требований состоит в том, что необходимо действовать в соответствии с некими алгоритмами, длинами ключей и стандартами; какие-либо содержательные спецификации отсутствуют.

Класс FMT (управление безопасностью), включающий шесть семейств, регламентирует управление функциями безопасности и их данными, атрибутами и ролями безопасности.

Семейство FMT_MOF (управление отдельными функциями) содержит единственное требование: только уполномоченные пользователи (точнее, уполномоченные идентифицированные роли) могут управлять режимами выполнения, подключением и отключением функций безопасности.

К управлению атрибутами безопасности (семейство FMT_MSA) предъявляется больше требований. Во-первых, оно должно быть доступно только определенным ролям. Во-вторых, необходимо

контролировать безопасность присваиваемых значений. В-третьих, при создании объектов должна существовать возможность задания значений, отличных от подразумеваемых.

Аналогичным образом устроено семейство FMT_MTD (управление данными функций безопасности), только вместо переопределения подразумеваемых значений в компоненте FMT_MTD.2 специфицируются граничные значения и действия, предпринимаемые в случае выхода за допустимые границы.

FMT_REV (отмена) предусматривает возможность отмены (отзыва) атрибутов безопасности пользователей, субъектов и объектов.

FMT_SAE позволяет устанавливать сроки действия атрибутов безопасности. Для каждого атрибута могут задаваться действия, выполняемые по истечении срока.

Наконец, семейство FMT_SMR (роли управления безопасностью) предназначено для управления назначением различных ролей пользователям. Предусмотрено наличие правил, управляющих отношениями между ролями.

Шесть семейств простой структуры содержит и класс FTA (доступ к объекту оценки), куда вошли требования управления сеансами работы пользователей (помимо идентификации и аутентификации).

Семейство FTA_LSA определяет требования по ограничению атрибутов безопасности сеанса, которые может выбирать пользователь.

Семейство FTA_MCS ограничивает количество параллельных сеансов, предоставляемых пользователю. Оно может быть как общим, так и индивидуальным (с учетом атрибутов безопасности).

Семейство FTA_SSL (блокирование сеанса) определяет возможность блокирования или завершения интерактивного сеанса как по инициативе пользователя, так и по инициативе функций безопасности (если пользователь неактивен заданное время). Действия, осуществляемые при блокировании, описаны весьма детально:

- очистка или перезапись устройств отображения, придание их

текущему содержанию нечитаемого вида;
- блокирование любых действий по доступу к данным пользователя и устройствам отображения, кроме необходимых для разблокирования сеанса.

Еще три однокомпонентных семейства содержат некоторые подробности открытия сеанса.

Семейство FTA_TAB (предупреждения перед предоставлением доступа к ОО) предписывает, чтобы перед открытием сеанса отображалось предупреждающее сообщение относительно несанкционированного использования объекта оценки. Это одно из весьма немногих функциональных требований без управляющих конструкций назначения или выбора.

Семейство FTA_TAH (история доступа к ОО) при успешном открытии сеанса определяет требования к отображению истории попыток получить доступ от имени пользователя, выполняющего вход в систему. Здесь проявлена просто-таки трогательная забота о пользователе: оговаривается, что справочная информация не должна исчезать с экрана до того, как пользователь успеет ее просмотреть.

Кроме того, функции безопасности могут отказать пользователю в открытии сеанса, основываясь на атрибутах безопасности, такая возможность с обманчивым названием "Открытие сеанса с ОО" предусмотрена семейством FTA_TSE.

Если сопоставить степень детализации требований к криптографической поддержке и к управлению сеансами, то различие представляется слишком большим. Впрочем, выдержать единый уровень в столь большом и сложном документе, как "Общие критерии", едва ли возможно.

Привычные, традиционные требования предъявляет класс FTP (доверенный маршрут / канал), состоящий из двух семейств, содержащих по одному компоненту в каждом. Доверенный маршрут (семейство FTP_TRP) позволяет выполнять определенные действия в режиме прямого взаимодействия с функциями безопасности (например, при начальной аутентификации). Доверенные каналы (семейство FTP_ITC)

предназначены для передачи критичных по безопасности данных между функциями безопасности с другими доверенными изделиями ИТ. Доверенный маршрут / канал должен быть логически отличим от других маршрутов (каналов), обеспечивать уверенную идентификацию взаимодействующих сторон, а также конфиденциальность и целостность передаваемых данных.

На этом мы завершаем рассмотрение функциональных требований безопасности.

"Общие критерии", часть 3. Требования доверия безопасности

Детально рассматриваются семейства требований и оценочные уровни доверия безопасности, представленные в "Общих критериях". Анализируются достоинства и недостатки принятого в них подхода.

Основные понятия и классификация требований доверия безопасности

Требования доверия безопасности составляют содержание третьей части "Общих критериев".

Доверие в трактовке "Общих критериев" - это основа для уверенности в том, что изделие ИТ отвечает целям безопасности. Доверие обеспечивается через активное исследование (оценку) изделия ИТ.

Требования доверия безопасности охватывают весь жизненный цикл изделий ИТ и предполагают выполнение следующих действий:

- оцениваются задания по безопасности (ЗБ) и профили защиты (ПЗ), ставшие источниками требований безопасности;
- анализируются различные представления проекта объекта оценки и соответствие между ними, а также соответствие каждого из них требованиям безопасности;
- проверяются процессы и процедуры безопасности, их применение;
- анализируется документация;
- верифицируются представленные доказательства;
- анализируются тесты и их результаты;
- анализируются уязвимости объекта оценки;
- проводится независимое тестирование, в том числе тестовые "взломы" (называемые далее тестированием проникновения).

Каждое требование (элемент) доверия принадлежит одному из трех типов:

- элементы действий разработчика (помечаются буквой "D" после

номера элемента); эти действия должны подтверждаться доказательным материалом (свидетельствами);

- элементы представления и содержания свидетельств (помечаются буквой "C");
- элементы действий оценщика (помечаются буквой "E"); оценщики обязаны проверить представленные разработчиками свидетельства, а также выполнить необходимые дополнительные действия (например, провести независимое тестирование).

Требования доверия разделены на 10 классов, 44 семейства и 93 компонента. Классы можно сгруппировать в зависимости от охватываемых этапов жизненного цикла изделий ИТ.

К первой группе, логически предшествующей разработке и оценке ОО, принадлежат классы APE (оценка профиля защиты) и ASE (оценка задания по безопасности).

Во вторую группу входят классы ADV (разработка), ALC (поддержка жизненного цикла) и ACM (управление конфигурацией).

К этапу получения, представления и анализа результатов разработки можно отнести классы AGD (руководства), ATE (тестирование) и AVA (оценка уязвимостей).

Требования к поставке и эксплуатации составляют содержание класса ADO.

Наконец, класс AMA (поддержка доверия) включает требования, применяемые после сертификации объекта оценки на соответствие "Общим критериям".

По сравнению с функциональными, требования доверия устроены несколько проще. Во-первых, к их элементам не применяются операции назначения и выбора. Во-вторых, компоненты в пределах семейства линейно упорядочены, то есть компонент с большим номером всегда усиливает предыдущий.

Одна из целей "Общих критериев" состоит в минимизации усилий разработчиков и оценщиков, направленных на обеспечение заданного уровня доверия. Этому способствует введение семи оценочных уровней

доверия (ОУД), содержащих полезные для практического применения комбинации компонентов, упорядоченные по степени усиления. Повысить уровень доверия помогут дополнительные действия:

- расширение границ объекта оценки;
- увеличение уровня детализации рассматриваемых аспектов ОО;
- повышение строгости рассмотрения, применение более формальных методов верификации.

Далее мы кратко рассмотрим семейства требований и оценочные уровни доверия безопасности.

Оценка профилей защиты и заданий по безопасности

Цель требований, вошедших в классы APE (оценка профиля защиты) и ASE (оценка задания по безопасности), - проверить полноту, непротиворечивость и реализуемость ПЗ или ЗБ.

Класс APE состоит из шести однокомпонентных семейств, соответствующих предписанной структуре профилей защиты.

Семейство APE_INT (введение ПЗ) требует от разработчика представить введение как часть ПЗ, содержащую данные идентификации и аннотацию ПЗ. Оценщик должен подтвердить, что имеющаяся информация удовлетворяет всем требованиям к содержанию и представлению свидетельств, что введение является логически последовательным и внутренне непротиворечивым и согласуется с другими частями ПЗ. Перечисленные требования к действиям оценщика носят стандартный характер и далее упоминаться не будут.

Семейство APE_DES (описание ОО) специфицирует, что описание объекта оценки должно включать в себя, как минимум, тип продукта и его общую характеристику.

Требования семейства APE_ENV (среда безопасности) более содержательны. Необходимо идентифицировать и объяснить все допущения о предполагаемом применении ОО и среде использования, все угрозы, от которых нужна защита, и все политики безопасности, обязательные для исполнения.

Еще содержательнее требования семейства APE_OBJ (цели безопасности). Разработчик должен не только сформулировать цели безопасности для объекта оценки и его среды, но и представить их логическое обоснование, продемонстрировав противостояние всем идентифицированным угрозам, охват всех установленных положений политик безопасности и предположений безопасности.

Основное содержание профиля защиты составляют требования безопасности. К этой части применимы семейства APE_REQ (требования безопасности ИТ) и APE_SRE (требования безопасности ИТ, сформулированные в явном виде). Первое относится к стандартным требованиям "Общих критериев", второе - к расширениям ОК, введенным разработчиком ПЗ. Логическое обоснование требований безопасности должно демонстрировать их решающую роль в достижении целей безопасности.

Класс ASE устроен аналогично классу APE, некоторые отличия вызваны большей конкретностью задания по безопасности в сравнении с профилем защиты и наличием дополнительных разделов. Модифицированы требования шести рассмотренных выше семейств и добавлены два новых.

Семейство ASE_TSS (краткая спецификация ОО) определяет в самом общем виде функции безопасности и меры доверия, предназначенные, соответственно, для выполнения функциональных требований и требований доверия.

Функции безопасности и функциональные требования сопоставляют таким образом, чтобы можно было понять, какие из них обслуживают отдельно взятое требование и, наоборот, для выполнения каких требований предназначена каждая из функций. Логическое обоснование краткой спецификации ОО должно демонстрировать, что специфицированные функции пригодны для удовлетворения функциональных требований. Функции, реализованные вероятностными или перестановочными механизмами, нуждаются в определении требований к стойкости.

Если задание по безопасности является конкретизацией некоторых ПЗ, к нему применяются требования семейства ASE_PPC (утверждения о соответствии профилям защиты).

Подчеркнем важность тщательной разработки и оценки профилей защиты и заданий по безопасности. Просчеты на стадиях выработки требований и спецификаций изделий ИТ чреваты особо тяжелыми последствиями, исправлять которые сложно и дорого.

Требования доверия к этапу разработки

Функциональные требования, политика безопасности и краткая спецификация объекта оценки служат отправным пунктом процесса разработки функций безопасности ОО. Класс ADV (разработка) состоит из семи многокомпонентных семейств и содержит требования для постепенного повышения уровня детализации проекта вплоть до представления реализации с демонстрацией соответствия между уровнями.

В этом классе предусмотрены три стиля изложения спецификаций: неформальный, полуформальный и формальный - и три способа демонстрации соответствия.

Неформальная спецификация пишется как обычный текст с определением необходимых терминов. Неформальная демонстрация соответствия требует установления "соответствия по сути".

Полуформальная спецификация создается при помощи языка с ограниченным синтаксисом и, как правило, сопровождается пояснительным текстом. Полуформальная демонстрация соответствия невозможна без структурированного подхода.

В формальной спецификации используется математическая нотация, а методом демонстрации соответствия служит формальное доказательство.

Ранжирование компонентов в семействах класса ADV в основном соответствует стилю изложения спецификаций, ужесточаясь от неформального к формальному.

В классе ADV выделены четыре уровня детализации проекта: функциональная спецификация, проект верхнего уровня, проект нижнего уровня, представление реализации. Поскольку в конкретной

разработке некоторые из них могут отсутствовать, предусмотрена независимая демонстрация соответствия каждого функциональным требованиям.

Требования к функциональной спецификации, сосредоточенные в семействе ADV_FSP, указывают на обязательность включения в функциональную спецификацию описания назначения и методов использования всех внешних интерфейсов функций безопасности объекта оценки с добавлением, где это необходимо, детализации результатов, нештатных ситуаций и сообщений об ошибках. Из описания должно быть понятно, как учтены функциональные требования и каким образом строить тесты соответствия.

Требования семейства ADV_SPM (моделирование политики безопасности) охватывают еще один аспект функциональной спецификации - соответствие политике безопасности объекта оценки, возможности ее осуществления. Средством демонстрации соответствия служит модель политики безопасности: необходимо показать, что все функции безопасности в функциональной спецификации непротиворечивы и их полнота адекватна модели.

Семейство ADV_HLD содержит требования к проекту верхнего уровня, описывающего структуру функций безопасности ОО в терминах подсистем. Проект должен идентифицировать все необходимые базовые аппаратные, программно-аппаратные и/или программные средства с представлением функций, обеспечиваемых поддержкой реализуемых этими средствами механизмов защиты, а также все интерфейсы подсистем, выделяя те из них, которые предполагаются видимыми извне. Каждый интерфейс необходимо снабдить описанием назначения и методов использования (то же касается и функциональных спецификаций - это означает демонстрацию соответствия функциональным требованиям и позволяет организовать тестирование.) Следует выделить подсистемы, осуществляющие политику безопасности. Наконец, проект верхнего уровня должен содержать обоснование того, что выбранные механизмы достаточны для реализации функций безопасности.

Требования к проекту нижнего уровня образуют семейство ADV_LLD, в котором детализация доходит до уровня модуля. Специфицируются все

интерфейсы модулей (с выделением видимых извне), реализующих функции безопасности. Обязательное условие - описание разделения на модули, выполняющие политику безопасности, и прочие, а также предоставление осуществляющих эту политику функций. Взаимосвязи между модулями следует определять в терминах имеющихся функциональных возможностей безопасности и зависимостей от других модулей. Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей, а при необходимости - возможность создания детального отчета о результатах, нештатных ситуациях и отправки уведомлений об ошибках.

Очень важно, чтобы представление реализации (семейство ADV_IMP) однозначно определяло функции безопасности объекта оценки на высоком уровне детализации, тогда впоследствии их возможно создать без дальнейших проектных решений. Представление реализации должно быть структурировано в малые и понятные разделы, включать в себя описание связей между всеми частями реализации.

Семейство ADV_RCR ведает соответствием всех имеющихся смежных уровней представления функций безопасности. Надо доказать, что все функциональные возможности более абстрактного представления, относящиеся к безопасности, правильно и полностью уточнены на менее абстрактном уровне.

Требования семейства ADV_INT (внутренняя структура функций безопасности ОО) носят технологический характер и сходны по смыслу с требованиями структурированного программирования. Основная идея состоит в минимизации сложности процесса и результата разработки путем разбиения на модули и использования нескольких уровней абстракции. Здесь придется впервые сформулировать требования к действиям разработчика (до этого мы ограничивались требованиями к представлению и содержанию свидетельств).

Разработчик должен проектировать и структурировать функции безопасности объекта оценки в модульном, многоуровневом виде, облегчая связи между модулями, а также между уровнями проекта, уменьшая общую сложность, в особенности тех частей, которые отвечают за политику безопасности, чтобы они были простыми для анализа.

Разработчик обязан представить описание архитектуры с изложением назначения, интерфейсов, параметров и результатов применения каждого модуля и выделением частей, осуществляющих политику безопасности, с разбиением на уровни и демонстрацией того, что сложность минимизирована.

На наш взгляд, подобные архитектурные требования крайне важны, они заслуживают развития и вынесения в отдельный класс. Есть еще целый ряд других архитектурных принципов, специфичных для информационной безопасности (например, эшелонированность обороны, разнообразие защитных средств), которые, к сожалению, остались за рамками "Общих критериев".

Технологические требования процедурного характера составляют содержание класса ALC (поддержка жизненного цикла), состоящего из четырех семейств.

Прежде всего определяется модель жизненного цикла (семейство ALC_LCD), описывающая процессы разработки и сопровождения ОО, включая детализацию количественных параметров и/или метрик, используемых для оценки соответствия процесса разработки и принятой модели.

Затем следует обосновать выбор инструментальных средств и методов (семейство ALC_TAT). Это относится, в частности, к используемым языкам программирования, средствам подготовки документации, стандартам реализации и т.п.

Безопасность разработки организуется в соответствии с требованиями семейства ALC_DVS. Разработчик должен не только иметь описание и обоснование всех физических, относящихся к персоналу и иных мер безопасности, которые необходимы для обеспечения конфиденциальности и целостности проекта ОО и его реализации, но и соблюдать эти меры во время создания и сопровождения ОО, что проверяется оценщиками.

Важным элементом этапа сопровождения является устранение недостатков (семейство ALC_FLR). Процедуры отслеживания и устранения недостатков фиксируются разработчиком. Они должны содержать требование представления описания природы и проявлений

каждого недостатка безопасности, а также статуса завершения исправления этого недостатка. Разработчик устанавливает процедуру приема и отработки сообщений о недостатках, запросов на их исправление с указанием контактных адресов и автоматическим распространением сообщений о недостатках и их исправлении зарегистрированным пользователям. Все ставшие известными недостатки безопасности должны быть исправлены (без создания новых), а исправления изданы.

Управление конфигурацией (УК, класс ACM) - необходимый инструмент коллектива разработчиков. В этот класс входят три семейства, самое содержательное из которых - ACM_CAP, специфицирующее возможности УК. Кроме выполнения очевидных требований уникальной идентификации (маркировки) объекта оценки, его версий и элементов (с выделением частей, относящихся к функциям безопасности), необходимо предусмотреть меры защиты от несанкционированных изменений и меры поддержки генерации ОО.

Любопытно применение принципа разделения обязанностей: требуется, чтобы лицо, ответственное за включение элемента в УК, не являлось его разработчиком.

Семейство ACM_SCP специфицирует область действия управления конфигурацией. Она включает представление реализации объекта оценки, проектную и тестовую документацию, документацию пользователя и администратора, документацию УК, информацию о недостатках безопасности и инструментальные средства разработки.

Для уменьшения числа возможных ошибок управление конфигурацией следует максимально автоматизировать - в этом смысл требований семейства ACM_AUT. Автоматизация должна распространяться на защиту от несанкционированных изменений, генерацию объекта оценки, выявление различий между версиями и на нахождение элементов, подвергающихся воздействию определенной модификации.

В целом требования доверия к этапу разработки сформулированы на высоком уровне, в соответствии с современной технологией создания и сопровождения сложных систем.

Требования к этапу получения, представления и анализа результатов разработки

Мы переходим к рассмотрению трех следующих классов требований доверия безопасности: AGD (руководства), ATE (тестирование) и AVA (оценка уязвимостей).

Класс AGD состоит из двух однокомпонентных семейств, где сформулированы требования к руководствам администратора (AGD_ADM) и пользователя (AGD_USR).

Руководство администратора должно содержать:

- описание особенностей управления ОО безопасным способом;
- описание функций и интерфейсов администрирования;
- предупреждения относительно функций и привилегий, подлежащие контролю;
- описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО;
- описание всех параметров безопасности, контролируемых администратором, с указанием безопасных значений;
- описание событий, относящихся к безопасности;
- описание всех требований безопасности к среде ИТ, имеющих отношение к администратору.

В руководство пользователя необходимо включить:

- описание функций и интерфейсов объекта оценки, доступных пользователям;
- описание применения доступных пользователям функций безопасности;
- предупреждения относительно доступных пользователям функций и привилегий, которые следует контролировать;
- изложение всех обязанностей пользователя по безопасной эксплуатации ОО.

Класс ATE (тестирование) состоит из четырех семейств, содержащих требования к полноте, глубине, способам и результатам тестирования

функций безопасности на предмет их соответствия спецификациям.

Разработчик выполняет функциональное тестирование (семейство ATE_FUN), обосновывает достаточность глубины (семейство ATE_DPT) и покрытия (ATE_COV) тестов.

При функциональном тестировании необходимо проверить все функции безопасности, не ограничиваясь подтверждением наличия требуемых функций безопасности, но проверяя также, отсутствуют ли нежелательные режимы функционирования.

Анализ глубины должен показать достаточность тестов для демонстрации того, что функции безопасности выполняются в соответствии с проектами верхнего и нижнего уровней и представлением реализации.

Важно, чтобы анализ покрытия демонстрировал полное соответствие между представленными тестами и описанием функций безопасности в функциональной спецификации. Требуется полностью проверить все внешние интерфейсы функций безопасности.

Семейство ATE_IND (независимое тестирование) регламентирует действия оценщиков. Оценщику следует протестировать необходимое подмножество функций безопасности и подтвердить, что объект оценки функционирует в соответствии со спецификациями, а также выполнить некоторые или все тесты из тестовой документации, чтобы верифицировать результаты, полученные разработчиком.

Один из ключевых моментов оценки безопасности изделия ИТ - оценка уязвимостей (класс AVA), отправным пунктом которой является анализ уязвимостей (семейство AVA_VLA), выполняемый разработчиком и оценщиком. Четыре компонента этого семейства ранжированы по уровню строгости анализа и потенциалу предполагаемого нарушителя.

Анализ, проводимый разработчиком, направлен на поиск и идентификацию уязвимостей, обоснование невозможности их использования в предполагаемой среде и стойкости объекта оценки к явным нападениям.

Прежде всего оценщик обязан проверить, что ОО противостоит

нападениям нарушителя, соответственно, с низким (AVA_VLA.2), умеренным (AVA_VLA.3) или высоким (AVA_VLA.4) потенциалом. Для достижения этой цели в общем случае проводится независимый анализ уязвимостей, а затем оцениваются возможности использования идентифицированных разработчиком и дополнительно выявленных уязвимостей, посредством проведения тестовых атак.

Анализ стойкости функций безопасности объекта оценки (семейство AVA_SOF) проводится на уровне реализующих механизмов. По своей направленности он аналогичен анализу уязвимостей. Выше, в разделе "Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий", мы подробно рассматривали эту тему. Здесь же отметим, что требования единственного компонента семейства AVA_SOF носят формальный характер: для каждого механизма, имеющего утверждение относительно стойкости функции безопасности, анализ должен показать, что стойкость достигает или превышает уровень, определенный в профиле защиты или задании по безопасности.

Требования семейства AVA_MSU (неправильное применение) направлены на то, чтобы исключить возможность такого конфигурирования и/или применения объекта оценки, которое администратор или пользователь считают безопасным, в то время как оно таковым не является. Необходимо обеспечить отсутствие в руководствах вводящих в заблуждение, необоснованных и противоречивых указаний и наличие безопасных процедур для всех режимов функционирования. Опасные состояния должны легко выявляться.

Задача решается следующим образом: в представленных разработчиком руководствах идентифицируются все возможные режимы эксплуатации объекта оценки, включая действия после сбоя или ошибки в работе, их последствия и значение для безопасности эксплуатации. Прилагается список всех предположений относительно среды эксплуатации и требований к внешним мерам безопасности.

Оценщик должен повторить все процедуры конфигурирования и установки, а также выборочно другие процедуры для подтверждения того факта, что объект оценки можно безопасно конфигурировать и

использовать, применяя только представленные руководства. Кроме того, он обязан выполнить независимое тестирование и проверить, смогут ли администратор или пользователь выяснить, руководствуясь документацией, что ОО сконфигурирован или используется опасным образом.

Анализ скрытых каналов, регламентируемый семейством AVA_CCA, крайне сложен и концептуально, и технически (см., например, статью [8]). Здесь легко требовать, но трудно выполнять. Согласно "Общим критериям", разработчик проводит исчерпывающий поиск скрытых каналов для каждой политики управления информационными потоками и предоставляет документацию анализа, в которой идентифицированы скрытые каналы и оценена их пропускная способность, описаны наиболее опасные сценарии использования каждого идентифицированного скрытого канала.

Оценщик должен выборочно подтвердить правильность анализа скрытых каналов посредством тестирования.

Требования к поставке и эксплуатации, поддержка доверия

Класс ADO (поставка и эксплуатация) содержит требования к процедурам поставки, установки, генерации и запуска объекта оценки.

Требования к поставке сосредоточены в трехкомпонентном семействе ADO_DEL. Разработчик должен документировать и использовать процедуры поставки объекта оценки или его частей. Необходимо описать, каким образом различные процедуры и технические меры обеспечивают обнаружение (ADO_DEL.2) или предотвращение (ADO_DEL.3) модификаций либо иного расхождения между оригиналом разработчика и версией, полученной в месте применения, а также обнаружение попыток подмены от имени разработчика в тех случаях, когда последний ничего не поставлял.

Семейство ADO_IGS (установка, генерация и запуск) предназначено для безопасного перехода к этапу эксплуатации. Процедуры безопасной установки, генерации и запуска объекта оценки документируются разработчиком. Документация должна содержать описание процедур,

обеспечивающих протоколирование применявшихся опций генерации, для точного ответа на вопрос, как и когда был сгенерирован ОО.

Класс AMA (поддержка доверия) включает четыре семейства и содержит требования, к которым обращаются после сертификации объекта оценки. Они помогают (по возможности экономно, без полной повторной оценки) сохранить уверенность в том, что ОО продолжает отвечать своему заданию по безопасности после изменений в нем или в его среде. Речь идет о выявлении новых угроз или уязвимостей, изменении в требованиях пользователя, а также об исправлении ошибок.

Действия по поддержке доверия носят циклический характер. Каждая итерация цикла состоит из двух фаз:

- приемка объекта оценки для поддержки;
- мониторинг ОО.

Фаза приемки включает разработку плана поддержки доверия и категорирование компонентов объекта оценки по их влиянию на безопасность. Элементы фазы мониторинга - представление описания текущей версии ОО и выполнение анализа влияния изменений на безопасность. Возможно, в конце итерации выяснится, что план или категорирование нуждаются в уточнении или изменении; тогда новая итерация начнется с повторной приемки ОО.

Цикл поддержки доверия не может выполняться бесконечно. В конце концов, либо накопится много мелких изменений, либо потребуются крупные, и тогда переоценка станет неизбежной.

Семейство AMA_AMP (план поддержки доверия) регламентирует вход в цикл поддержки доверия. Оно идентифицирует процедуры, которые выполняет разработчик при изменении объекта оценки или его среды. План поддержки доверия должен содержать краткое описание ОО, включающее предоставляемые им функциональные возможности безопасности, идентифицировать сертифицированную версию ОО и ссылаться на результаты оценки, определять предусматриваемые пределы изменения ОО, содержать описание жизненного цикла ОО, текущие планы новых выпусков ОО, аудита и следующей переоценки, а

также включать в себя краткое описание любых запланированных изменений, которые, как ожидается, будут иметь заметное влияние на безопасность. План необходимо дополнить описанием процедур, которые предполагается применять для поддержки доверия и куда, как минимум, следует включить процедуры управления конфигурацией, поддержки свидетельства доверия, выполнения анализа влияния произведенных изменений на безопасность, устранения недостатков.

План поддержки доверия опирается на отчет о категорировании компонентов ОО для сертифицированной версии ОО, специфицируемый семейством AMA_CAT. Категорирование критически важно для анализа влияния на безопасность и переоценки ОО. Отчет должен распределить по категориям каждый компонент, который может быть идентифицирован в каждом представлении функций безопасности от наиболее до наименее абстрактного, согласно его отношению к безопасности. Как минимум, необходимо разделить компоненты ОО на осуществляющие и не осуществляющие политику безопасности. Следует описать примененную схему категорирования, чтобы сделать возможным распределение по категориям новых компонентов, а также перераспределение существующих вследствие изменений в ОО или в его задании по безопасности. Наконец, отчет должен идентифицировать средства разработки, модификация которых влияет на доверие.

Назначение семейства AMA_EVD (свидетельство поддержки доверия) состоит в том, чтобы в рамках фазы мониторинга убедиться в поддержке разработчиком доверия безопасности объекта оценки в соответствии с представленным планом. Семейство содержит требования к документации поддержки доверия для текущей версии ОО. Документация должна включать список текущей конфигурации ОО и список идентифицированных уязвимостей, подтверждать следование процедурам, описанным в плане поддержки доверия. Для каждой уязвимости в текущей версии требуется показать, что она не может быть использована в предполагаемой среде ОО.

Оценщик должен подтвердить, что все изменения, документированные при анализе влияния на безопасность для текущей версии ОО, находятся в пределах, установленных планом поддержки доверия, и что функциональное тестирование выполнялось на текущей версии ОО

соразмерно поддерживаемому уровню доверия.

Анализ влияния на безопасность (семейство AMA_SIA), проведенный разработчиком, позволит оценить последствия изменений, воздействующих на сертифицированный объект оценки. По его результатам готовится документ, идентифицирующий сертифицированный ОО, откуда была получена текущая версия, а также все новые и модифицированные компоненты. Для каждого изменения, воздействующего на задание по безопасности или на представления функций безопасности, следует описать все последствия, к которым оно приводит на более низких уровнях представления, идентифицировать все функции безопасности и компоненты, категорированные как осуществляющие политику безопасности и подверженные влиянию со стороны данного изменения.

Если изменение приводит к модификации представления реализации, следует идентифицировать тесты, подтверждающие правильность функционирования новой версии.

Наконец, необходимо проанализировать влияние изменений на оценку уязвимости, управление конфигурацией, руководства, поставку и эксплуатацию, поддержку жизненного цикла объекта оценки.

Оценщик должен удостовериться, что при анализе влияния на безопасность все изменения документированы на приемлемом уровне детализации вместе с соответствующим строгим обоснованием поддержки доверия в текущей версии ОО.

На этом мы завершаем рассмотрение семейств требований доверия безопасности.

Оценочные уровни доверия безопасности

В "Общих критериях" определено семь упорядоченных по возрастанию оценочных уровней доверия (ОУД) безопасности, содержащих рассчитанные на многократное применение комбинации требований доверия (не более одного компонента из каждого семейства). Наличие такой шкалы дает возможность сбалансировать получаемый уровень доверия со сложностью, сроками, стоимостью и самой возможностью

его достижения.

Предполагается, что в профилях защиты и заданиях по безопасности будут фигурировать или сами оценочные уровни, или их усиления, полученные путем расширения требований (за счет добавления к ОУД новых компонентов) либо увеличения строгости и/или глубины оценки (посредством замены компонентов более сильным вариантом из того же семейства). Таким образом, ОУД играют роль опорных точек в многомерном пространстве требований доверия.

Отметим, что в ОУД не включены требования классов APE (оценка профиля защиты), ASE (оценка задания по безопасности) и AMA (поддержка доверия), поскольку они находятся вне пределов основного цикла разработки изделий ИТ.

Оценочный уровень доверия 1 (ОУД1), предусматривающий функциональное тестирование, применим, когда требуется некоторая уверенность, что объект оценки работает безукоризненно, а угрозы безопасности не считаются серьезными. Его можно достичь без помощи разработчика и с минимальными затратами посредством анализа функциональной спецификации, спецификации интерфейсов, эксплуатационной документации в сочетании с независимым тестированием.

Оценочный уровень доверия 2 (ОУД2) предусматривает структурное тестирование и доступ к части проектной документации и результатам тестирования разработчиком. ОУД2 применим, когда разработчикам или пользователям требуется независимо получаемый умеренный уровень доверия при отсутствии доступа к полной документации по разработке.

В дополнение к ОУД1 предписывается анализ проекта верхнего уровня. Анализ должен быть поддержан независимым тестированием функций безопасности, актом разработчика об испытаниях, основанных на функциональной спецификации, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска явных уязвимостей. Требуется наличие списка конфигурации ОО с уникальной идентификацией элементов конфигурации и свидетельства безопасных процедур поставки.

Оценочный уровень доверия 3 (ОУД3), предусматривающий систематическое тестирование и проверку, позволяет достичь максимально возможного доверия при использовании обычных методов разработки. Он применим в тех случаях, когда разработчикам или пользователям требуется умеренный уровень доверия на основе всестороннего исследования объекта оценки и процесса его разработки.

По сравнению с ОУД2 сюда добавлено требование, которое предписывает разработчику создавать акт об испытаниях с учетом особенностей не только функциональной спецификации, но и проекта верхнего уровня. Кроме того, требуется контроль среды разработки и управление конфигурацией объекта оценки.

Оценочный уровень доверия 4 (ОУД4) предусматривает систематическое проектирование, тестирование и просмотр. Он позволяет достичь доверия, максимально возможного при следовании общепринятой практике коммерческой разработки. Это самый высокий уровень, на который, вероятно, экономически целесообразно ориентироваться для существующих типов продуктов.

ОУД4 характеризуется анализом функциональной спецификации, полной спецификации интерфейсов, эксплуатационной документации, проектов верхнего и нижнего уровней, а также подмножества реализации, применением неформальной модели политики безопасности ОО. Среди других дополнительных требований - независимый анализ уязвимостей, демонстрирующий устойчивость к попыткам проникновения нарушителей с низким потенциалом нападения, и автоматизация управления конфигурацией.

Отличительные особенности оценочного уровня доверия 5 (ОУД5) - полуформальное проектирование и тестирование. С его помощью достигается доверие, максимально возможное при следовании строгой практике коммерческой разработки, поддержанной умеренным применением специализированных методов обеспечения безопасности. ОУД5 востребован, когда нужен высокий уровень доверия и строгий подход к разработке, не влекущий излишних затрат.

Для достижения ОУД5 требуется формальная модель политики безопасности ОО и полуформальное представление функциональной спецификации и проекта верхнего уровня, полуформальная

демонстрация соответствия между ними, а также модульная структура проекта ОО. Акт об испытаниях должен быть основан еще и на проекте нижнего уровня. Необходима устойчивость к попыткам проникновения нарушителей с умеренным потенциалом нападения. Предусматривается проверка правильности анализа разработчиком скрытых каналов и всестороннее управление конфигурацией.

Оценочный уровень доверия 6 (ОУД6) характеризуется полуформальной верификацией проекта. Он позволяет получить высокое доверие путем применения специальных методов проектирования в строго контролируемой среде разработки при производстве высококачественных изделий ИТ и при защите ценных активов от значительных рисков.

Особенности ОУД6:

- структурированное представление реализации;
- полуформальное представление проекта нижнего уровня;
- иерархическая структура проекта ОО;
- устойчивость к попыткам проникновения нарушителей с высоким потенциалом нападения;
- проверка правильности систематического анализа разработчиком скрытых каналов;
- использование структурированного процесса разработки;
- полная автоматизация управления конфигурацией ОО.

Оценочный уровень доверия 7 (ОУД7), предусматривающий формальную верификацию проекта, применим к разработке изделий ИТ для использования в ситуациях чрезвычайно высокого риска или там, где высокая ценность активов оправдывает повышенные затраты.

На седьмом уровне дополнительно требуются:

- формальное представление функциональной спецификации и проекта верхнего уровня и формальная демонстрация соответствия между ними;
- модульная, иерархическая и простая структура проекта ОО;
- добавление представления реализации как основы акта об испытаниях;

- полное независимое подтверждение результатов тестирования разработчиком.

На наш взгляд, оценочные уровни доверия выбраны очень удачно; их усиление в профилях защиты и заданиях по безопасности в подавляющем большинстве случаев носит непринципиальный характер.

Дополнительную информацию по "Общим критериям" можно найти в книге [87].

Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности

Определяется роль профилей защиты, описывается их структура. Выделяются общие требования к сервисам безопасности.

Общие положения

Мы приступаем к анализу профилей защиты и их проектов, построенных на основе "Общих критериев" и описывающих сервисы безопасности, их комбинации и приложения. В первой части выделяются общие требования, которые могут войти в состав применимого ко всем сервисам функционального пакета, упрощающего разработку и понимание профилей для конкретных сервисов. Анализ профилей защиты позволяет оценить сильные и слабые стороны "Общих критериев", наметить возможные направления новых исследований.

"Общие критерии" в применении к оценке безопасности изделий информационных технологий (ИТ) являются, по сути, метасредствами, задающими систему понятий, в терминах которых должна производиться оценка, но не предоставляющих конкретных наборов требований и критериев, подлежащих обязательной проверке. Эти требования и критерии фигурируют в профилях защиты (ПЗ) и заданиях по безопасности (ЗБ) (см., например, [53], [20], [GTKRRPP]).

Профили защиты, в отличие от заданий по безопасности, носят универсальный характер: они характеризуют определенный класс изделий ИТ вне зависимости от специфики условий применения. Именно официально принятые профили защиты образуют построенную на основе "Общих критериев" (ОК) и используемую на практике нормативную базу в области информационной безопасности (ИБ).

В настоящее время такая база и в мире (см., например, [95],), и в России только создается. В нашей стране эту работу курирует ФСТЭК - Федеральная служба по техническому и экспортному контролю (ранее Государственная техническая комиссия при Президенте РФ -

Гостехкомиссия России).

Профили защиты могут характеризовать отдельные сервисы безопасности, комбинации подобных сервисов, реализованные, например, в операционной системе, а также прикладные изделия ИТ, для которых обеспечение информационной безопасности критически важно (пример - смарт-карты).

Нас в первую очередь будут интересовать профили защиты сервисов безопасности, поскольку последние являются универсальными строительными блоками, позволяющими формировать защитные рубежи информационных систем (ИС) различного назначения, разной степени критичности. В курсе [91] "Основы информационной безопасности" выделены следующие базовые сервисы безопасности:

- идентификация и аутентификация ;
- управление доступом ;
- протоколирование и аудит ;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

В силу разных причин не для всех перечисленных сервисов профили защиты разработаны или разрабатываются. Так, традиционные протоколирование и аудит, отказоустойчивость и безопасное восстановление адекватно описываются соответствующими классами функциональных требований "Общих критериев", поэтому формировать на их основе привычные классы защищенности относительно несложно (однако сделать это, разумеется, все же необходимо).

Выделение сервисов туннелирования и управления еще не вошло в общепринятую практику, поэтому пока они обойдены вниманием разработчиков ПЗ.

Наконец, криптография во многих странах (да и в самих "Общих критериях") является "особой точкой" безопасности, поэтому создание профилей защиты для сервисов шифрования и контроля целостности, а также для других сервисов, реализация которых опирается на криптографические механизмы, затруднено по законодательным и/или организационным причинам. (Заметим, что, хотя сложившееся вокруг компьютерной криптографии положение можно объяснить, его никак нельзя признать нормальным.)

Если придерживаться объектно-ориентированного подхода (см., например, курс [91], а также книгу [87]), то целесообразно выделить по крайней мере два уровня в иерархии наследования требований к сервисам безопасности:

- общие требования, применимые ко всем или многим сервисам;
- частные требования, специфичные для конкретного сервиса.

С точки зрения технологии программирования, "Общие критерии" построены по дообъектной, "библиотечной" методологии. Они предоставляют параметризованные функциональные требования, но не содержат необходимые для практического применения комбинации таких требований или универсальные интерфейсы, допускающие конкретизацию в контексте различных сервисов. Тем не менее, мы попытаемся выделить из разных профилей общие требования к сервисам безопасности, поскольку это упростит охват и понимание всей системы имеющихся профилей защиты.

При изложении общих и частных требований к сервисам безопасности, их комбинациям и приложениям мы будем следовать стандартной структуре профилей защиты (см. выше описание класса требований доверия APE), обращая особое внимание на интересующие нас аспекты:

- предположения безопасности ;
- угрозы безопасности;
- политика безопасности ;
- цели безопасности для объекта оценки;
- цели безопасности для среды;
- функциональные требования безопасности;
- требования доверия безопасности.

Общие предположения безопасности

Предположения безопасности - это часть описания среды, в которой функционирует объект оценки. Они выделяют объект оценки из общего контекста и задают границы рассмотрения. При проведении оценки истинность предположений принимается без доказательства.

Перечислим общие предположения:

- использование сервиса безопасности предусматривает наличие уполномоченного пользователя, который выполняет обязанности администратора, обладает достаточной квалификацией, отвечает за нормальное функционирование системы, осуществляет сопровождение сервиса и действует в соответствии с положениями политики безопасности;
- предусматривается возможность удаленного администрирования сервиса;
- политика управления данными аутентификации проводится в жизнь, и пользователи меняют эти данные должным образом и с требуемой регулярностью;
- после лишения пользователя прав доступа к сервису (например, в связи со сменой работы) его данные аутентификации и привилегии ликвидируются;
- предусматривается резервное копирование информации, ассоциированной с сервисом (такой, например, как значения конфигурационных параметров);
- аппаратно-программная среда сервиса безопасности является минимально достаточной для нормального функционирования (в частности, обычно отсутствуют средства разработки, а другие возможности модификации среды сведены к минимуму);
- предполагается физическая защищенность вычислительной установки, поддерживающей сервис безопасности ;
- не допускается возможность обхода узлов сети, на которых функционируют сервисы безопасности ;
- предполагается, что вредоносный код не может иметь подпись доверенной стороны;
- предполагается, что пользователи должным образом сообщают о случаях нарушения информационной безопасности ;

- предполагается, что пользователи и обслуживающий персонал способны противостоять методам морально-психологического воздействия.

Общие угрозы безопасности

Современные сервисы безопасности функционируют в распределенной среде, поэтому необходимо учитывать наличие как локальных, так и сетевых угроз. В качестве общих можно выделить следующие угрозы:

- обход злоумышленником защитных средств ;
- осуществление злоумышленником физического доступа к вычислительной установке, на которой функционирует сервисы безопасности ;
- ошибки администрирования, в частности, неправильная установка, ошибки при конфигурировании и т.п.;
- переход сервиса в небезопасное состояние в результате сбоя или отказа, при начальной загрузке, в процессе или после перезагрузки:
- маскарад пользователя (попытка злоумышленника выдать себя за уполномоченного пользователя, например, за администратора ; в распределенной среде возможны подмена исходного адреса или воспроизведение ранее перехваченных данных идентификации / аутентификации);
- маскарад сервера (попытка злоумышленника выдать свою систему за легальный сервер; следствием подобных действий может стать навязывание пользователю ложной информации или получение от него конфиденциальных сведений);
- использование злоумышленником чужого сетевого соединения или интерактивного сеанса (например, путем доступа к оставленному без присмотра терминалу);
- несанкционированное изменение злоумышленником конфигурации сервиса и/или конфигурационных данных;
- нарушение целостности программной конфигурации сервиса, в частности, внедрение троянских компонентов или получение контроля над сервисом;
- несанкционированный доступ к конфиденциальной (например, регистрационной) информации, в том числе

несанкционированное расшифрование закодированных данных;
- несанкционированное изменение данных (например, регистрационных), включая такие, целостность которых защищена криптографическими методами;
- несанкционированный доступ к данным (на чтение и/или изменение) в процессе их передачи по сети;
- анализ потоков данных с целью получения конфиденциальной информации;
- перенаправление потоков данных (в частности, на системы, контролируемые злоумышленником);
- блокирование потоков данных;
- повреждение или утрата регистрационной, конфигурационной или иной информации, влияющей на безопасность функционирования сервиса (например, из-за повреждения носителей или переполнения регистрационного журнала);
- агрессивное потребление злоумышленником ресурсов, в частности, ресурсов протоколирования и аудита, а также полосы пропускания;
- сохранение остаточной информации в многократно используемых объектах.

Общие элементы политики и цели безопасности

Сформулируем общие положения политики безопасности организации, относящиеся к защитным сервисам:

- идентификация и аутентификация всех субъектов доступа ;
- управление доступом к информационным ресурсам сервиса безопасности;
- подотчетность пользователей сервиса безопасности;
- протоколирование и аудит функционирования сервиса безопасности;
- обеспечение доступности коммуникационных каналов;
- обеспечение конфиденциальности и целостности управляющей информации (в частности, при удаленном администрировании);
- обеспечение целостности аппаратно-программной и информационной частей сервиса безопасности;
- обеспечение невозможности обхода защитных средств.

Переходя к изложению целей безопасности для объекта оценки, отметим, что их достижение должно способствовать противостоянию угрозам безопасности и реализации предписаний политики безопасности. Для различных сервисов безопасности общими являются нижеперечисленные цели:

- подотчетность субъектов и объектов, взаимодействующих с сервисом (необходимое условие достижения этой цели - идентификация и аутентификация взаимодействующих субъектов и объектов, а также протоколирование и аудит выполняемых действий);
- автоматизация административных действий, наличие средств проверки корректности конфигурации, как локальной, так и распределенной, наглядный интерфейс администрирования;
- обеспечение (прежде всего средствами пользовательского интерфейса) корректного использования функций безопасности;
- предоставление пользователям средств для проверки аутентичности серверов и других партнеров по общению, а также открытых криптографических ключей; реальное осуществление подобных проверок;
- выявление попыток нарушения политики безопасности, задание реакции на подобные попытки;
- обеспечение отсутствия вредоносного кода в составе сервиса, в том числе после ликвидации нарушений информационной безопасности;
- проверка программного кода на наличие подписи доверенной стороны перед его загрузкой в систему;
- выполнение резервного копирования информации, необходимой для восстановления нормальной работы сервиса;
- обеспечение безопасного восстановления после сбоев и отказов;
- обеспечение конфиденциальности и целостности информации при удаленном администрировании сервиса;
- обеспечение устойчивости средств идентификации и аутентификации к попыткам воспроизведения информации и другим способам реализации маскарада ; наличие средств разграничения доступа к компонентам и ресурсам сервиса безопасности;
- наличие средств контроля целостности компонентов и ресурсов сервиса;

- наличие средств контроля корректности функционирования сервиса;
- обеспечение безопасности многократного использования объектов.

Цели безопасности для среды дополняют цели безопасности объекта оценки и состоят в следующем:

- обеспечение минимальной достаточности аппаратной и программной конфигурации вычислительной установки, на которой функционирует сервис безопасности ;
- управление физическим доступом к компонентам и ресурсам сервиса;
- обеспечение невозможности обхода защитных средств;
- обеспечение достаточной подготовки уполномоченных пользователей сервиса безопасности;
- проведение в жизнь политики управления данными аутентификации: пользователи меняют эти данные должным образом и с требуемой регулярностью;
- ликвидация данных аутентификации и привилегий пользователей, лишенных доступа к сервису безопасности;
- разработка и реализация процедур и механизмов, предохраняющих от вторжения вредоносного программного обеспечения (ПО);
- разработка и реализация дисциплины доклада о нарушениях информационной безопасности;
- подготовка пользователей и обслуживающего персонала для противостояния методам морально-психологического воздействия;
- оперативная ликвидация выявленных уязвимостей.

Общие функциональные требования

Для различных сервисов безопасности общими являются функциональные требования, связанные с идентификацией и аутентификацией, управлением доступом, протоколированием и аудитом, а также обеспечением высокой доступности. Далее эти требования разбиты в соответствии с иерархией, принятой в "Общих

критериях".

Для сервисов безопасности предусмотрены общие требования по протоколированию и аудиту (класс FAU):

- автоматическая реакция аудита безопасности (FAU_ARP.1.1), включая генерацию записи в регистрационном журнале, а также локальную или удаленную сигнализацию об обнаружении вероятного нарушения безопасности, адресованную администратору ;
- генерация данных аудита безопасности (FAU_GEN.1). Обязательному протоколированию подлежат запуск и завершение регистрационных функций, а также все события для базового уровня аудита. В каждой регистрационной записи должны присутствовать дата и время события, тип события, идентификатор субъекта и результат (успех или неудача) события;
- анализ аудита безопасности (FAU_SAA.1.2). С целью выявления вероятных нарушений должны производиться по крайней мере накопление и/или объединение неуспешных результатов использования механизмов аутентификации, а также неуспешных результатов выполнения криптографических операций;
- просмотр аудита безопасности (FAU_SAR). Администратору предоставляется возможность читать всю регистрационную информацию. Прочим пользователям доступ к ней закрыт, за исключением явно специфицированных случаев;
- выбор событий аудита безопасности (FAU_SEL.1). Избирательность регистрации событий должна основываться хотя бы на минимально необходимом наборе атрибутов, состоящем из идентификатора объекта, идентификатора субъекта, адреса узла сети, типа события, даты и времени события;
- хранение данных аудита безопасности (FAU_STG.1.2). Регистрационную информацию следует защитить от несанкционированной модификации.

Многие сервисы безопасности прямо или косвенно нуждаются в криптографической поддержке, поэтому соответствующие требования класса FCS целесообразно трактовать как общие:

- управление криптографическими ключами (FCS_CKM). Должны

поддерживаться генерация криптографических ключей (FCS_CKM.1), распределение криптографических ключей (FCS_CKM.2), управление доступом к криптографическим ключам (FCS_CKM.3), уничтожение криптографических ключей (FCS_CKM.4);

- криптографические операции (FCS_COP.1). Всю информацию, передаваемую по доверенному каналу, необходимо шифровать и контролировать ее целостность согласно требованиям стандартов и других нормативных документов.

Любой сервис безопасности содержит данные пользователей (например, информацию для идентификации и аутентификации), поэтому общими являются и требования класса FDP (защита данных пользователя):

- политика управления доступом (FDP_ACC.1.1). Должно осуществляться разграничение доступа для пользователей, прямо или косвенно выполняющих операции с сервисом безопасности;
- функции управления доступом (FDP_ACF.1.1). Применение функций разграничения доступа основывается на следующих атрибутах безопасности: идентификаторы субъектов доступа, идентификаторы объектов доступа, адреса субъектов доступа, адреса объектов доступа, права доступа субъектов;
- базовая защита внутренней передачи (FDP_ITT.1). Следует осуществлять заданную политику управления доступом и/или информационными потоками, чтобы предотвратить раскрытие, модификацию и/или недоступность данных пользователя при их передаче между физически разделенными частями сервиса безопасности (FDP_ITT.1.1);
- защита остаточной информации (FDP_RIP.2.1). Для всех объектов должна обеспечиваться полная защита остаточной информации, то есть недоступность предыдущего состояния при освобождении ресурса.

Необходимость идентификации и аутентификации пользователей сервисов безопасности (класс FIA) стала следствием общего требования подотчетности:

- отказы аутентификации (FIA_AFL.1.2). При достижении определенного администратором числа неуспешных попыток аутентификации необходимо отказать субъекту в доступе, сгенерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности;
- определение атрибутов пользователя (FIA_ATD.1.1). Для каждого пользователя поддерживаются идентификатор, пароль и права доступа (роль). Кроме того, если используются криптографические операции, требуется поддержка открытых и секретных ключей;
- идентификация (FIA_UID) и аутентификация (FIA_UAU) пользователя. Каждый пользователь должен быть успешно идентифицирован (FIA_UID.2.1) и аутентифицирован (FIA_UAU.2.1) до разрешения любого действия, выполняемого сервисом безопасности от его имени. Необходимо предотвращать применение аутентификационных данных, которые были подделаны или скопированы у другого пользователя (FIA_UAU.3). Следует аутентифицировать любой представленный идентификатор пользователя (FIA_UAU.5.2) и повторно аутентифицировать пользователя по истечении определенного администратором интервала времени (FIA_UAU.6.1). Функции безопасности должны предоставлять пользователю только скрытую обратную связь во время выполнения аутентификации (FIA_UAU.7);
- связывание пользователь-субъект (FIA_USB.1.1). Соответствующие атрибуты безопасности пользователя нужно ассоциировать с субъектами, действующими от имени этого пользователя.

Управление - важнейший аспект информационной безопасности, а требования управления (класс FMT), несомненно, принадлежат к числу общих:

- управление отдельными функциями безопасности (FMT_MOF.1.1). Только администратору позволяется определять режим функционирования, отключения, подключения, модифицировать режимы идентификации и аутентификации, управлять правами доступа, протоколирования и аудита ;

- управление атрибутами безопасности (FMT_MSA). Только администратору предоставляется право изменения подразумеваемых значений, а также опроса, изменения, удаления, создания атрибутов безопасности и правил управления потоками информации (FMT_MSA.1.1). Следует обеспечить присваивание атрибутам безопасности исключительно безопасных значений (FMT_MSA.2.1);
- управление данными функций безопасности (FMT_MTD). Только администратор должен иметь возможность изменения подразумеваемых значений, опроса, изменения, удаления, очистки, определения типов регистрируемых событий, размеров регистрационных журналов, прав доступа субъектов, сроков действия учетных записей субъектов доступа, паролей, криптографических ключей (FMT_MTD.1.1). Только он определяет ограничения размеров регистрационных журналов, сроков действия учетных записей субъектов доступа, паролей, криптографических ключей, числа неудачных попыток аутентификации, интервалов бездействия пользователей (FMT_MTD.2.1). При выходе за допустимые границы должны выполняться установленные действия: передача уведомления администратору, блокирование или удаление учетной записи, запрос на смену пароля или ключа и т.д. (FMT_MTD.2.2). Следует обеспечить присваивание данным функциям лишь безопасных значений (FMT_MTD.3.1);
- отмена (FMT_REV.1). Только уполномоченным администраторам разрешено выполнять отмену атрибутов безопасности, ассоциированных с пользователями. Важные для безопасности полномочия должны отменяться немедленно (FMT_REV.1.2);
- роли управления безопасностью (FMT_SMR). Поддерживаются следующие роли: уполномоченный пользователь, удаленный пользователь, администратор (FMT_SMR.1.1). Получение ролей удаленного пользователя и администратора может производиться только по явному запросу (FMT_SMR.3.1).

Приватность (класс FPR) - специфический аспект информационной безопасности, однако требование открытости для уполномоченного пользователя носит общий характер:

- скрытность (FPR_UNO). Администратору необходимо иметь

возможность наблюдать за использованием ресурсов сервиса безопасности (FPR_UNO.4.1).

Собственная защищенность (класс FPT) - важная характеристика любого сервиса безопасности. В число общих входят следующие требования:

- тестирование абстрактной машины (FPT_AMT.1). Для демонстрации выполнения предположений безопасности, обеспечиваемых абстрактной машиной, положенной в основу сервиса безопасности, при запуске и/или по запросу администратора выполняется пакет тестовых программ (FPT_AMT.1.1);
- безопасность при сбое (FPT_FLS). Сервис должен сохранять безопасное состояние при аппаратных сбоях (вызванных, например, перебоями электропитания) (FPT_FLS.1.1);
- целостность экспортируемых данных (FPT_ITI). Сервис предоставляет возможность верифицировать целостность всех данных в момент их передачи между ним и удаленным доверенным изделием ИТ, выполняет повторную передачу информации, а также генерирует запись регистрационного журнала, если модификации обнаружены (FPT_ITI.1.2);
- надежное восстановление (FPT_RCV). Когда автоматическое восстановление после сбоя или прерывания обслуживания невозможно, следует обеспечить переход сервиса в режим аварийной поддержки, позволяющий вернуться к безопасному состоянию (FPT_RCV.2.1). После аппаратных сбоев требуется возврат к безопасному состоянию с использованием автоматических процедур (FPT_RCV.2.2);
- обнаружение повторного использования (FPT_RPL). Сервис должен обнаруживать повторное использование аутентификационных данных (FPT_RPL.1.1), отказывать в доступе, генерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности (FPT_RPL.1.2);
- посредничество при обращениях (FPT_RVM). Функции, осуществляющие политику безопасности сервиса, вызываются и успешно выполняются прежде, чем разрешается выполнение любой другой функции сервиса (FPT_RVM.1.1). Компонент

FPT_RVM.1 направлен на обеспечение невозможности обхода защитных средств;

- разделение доменов (FPT_SEP). Функции безопасности должны поддерживать отдельный домен для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами (FPT_SEP.1.1);
- метки времени (FPT_STM). Функциям безопасности нужно предоставлять надежные метки времени (FPT_STM.1.1);
- согласованность данных между функциями безопасности (FPT_TDC). Необходима согласованная интерпретация регистрационной информации, а также параметров используемых криптографических операций (FPT_TDC.1.1);
- согласованность перечисленных функций безопасности при дублировании в пределах объекта оценки (FPT_TRC). Должна обеспечиваться согласованность функций безопасности при дублировании их в различных частях объекта оценки (FPT_TRC.1.1). Когда части, содержащие дублируемые данные, разъединены, она выполняется после восстановления соединения перед обработкой любых запросов к заданным функциям безопасности (FPT_TRC.1.2);
- самотестирование функций безопасности (FPT_TST). Для демонстрации правильности работы функций безопасности в процессе нормального функционирования и/или по запросу администратора при запуске периодически должен выполняться пакет программ самотестирования (FPT_TST.1.1), а администратор верифицирует целостность данных (FPT_TST.1.2) и выполняемого кода функций безопасности (FPT_TST.1.3).

Требования класса FTA (доступ к объекту оценки) направлены на обеспечение защищенности от агрессивного потребления ресурсов:

- ограничение на параллельные сеансы (FTA_MCS). Ограничение максимального числа параллельных сеансов, предоставляемых одному пользователю (FTA_MCS.1.1). У этой величины должно быть подразумеваемое значение, устанавливаемое администратором (FTA_MCS.1.2);
- блокирование сеанса (FTA_SSL). По истечении установленного администратором значения длительности бездействия пользователя сеанс работы принудительно завершается

(FTA_SSL.3.1);

- открытие сеанса с объектом оценки (FTA_TSE). Сервис должен быть способен отказать в открытии сеанса, основываясь на идентификаторе субъекта, пароле субъекта, правах доступа субъекта (FTA_TSE.1.1).

Обеспечение защищенного взаимодействия сервисов безопасности в распределенной среде (класс FTP (доверенный маршрут / канал)) - одно из важнейших общих требований:

- доверенный канал передачи между функциями безопасности (FTP_ITC). Для связи с удаленным доверенным изделием ИТ функции безопасности должны предоставлять канал, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия (FTP_ITC.1.1). Обеим сторонам необходимо иметь возможность инициирования связи через доверенный канал (FTP_ITC.1.2, FTP_ITC.1.3);
- доверенный маршрут (FTP_TRP). Для связи с удаленным пользователем функции безопасности предоставляют маршрут, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия (FTP_TRP.1.1). Пользователю позволяется инициировать связь через доверенный маршрут (FTP_TRP.1.2). Для начальной аутентификации удаленного пользователя и удаленного управления использование доверенного маршрута является обязательным (FTP_TRP.1.3).

Общие требования доверия безопасности

Требования доверия безопасности, по сравнению с функциональными, представляются более проработанными, поскольку для них определены оценочные уровни доверия (ОУД).

Для большинства областей применения достаточно третьего уровня доверия, но поскольку он достижим при разумных затратах на разработку, его можно считать типовым.

В число требований доверия третьего оценочного уровня входят:

- анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации;
- независимое тестирование ;
- наличие проекта верхнего уровня ;
- анализ стойкости функций безопасности ;
- поиск разработчиком явных уязвимостей ;
- контроль среды разработки;
- управление конфигурацией.

В принципе реален и четвертый оценочный уровень, который можно рекомендовать для конфигураций повышенной защищенности. К числу дополнительных требований этого уровня относятся:

- полная спецификация интерфейсов;
- наличие проекта нижнего уровня ;
- анализ подмножества реализации;
- применение неформальной модели политики безопасности ;
- независимый анализ уязвимостей ;
- автоматизация управления конфигурацией.

Вероятно, это самый высокий уровень, который можно достичь при существующей технологии программирования и разумных затратах материальных и временных ресурсов.

Мы завершаем изложение общих требований к сервисам безопасности. На наш взгляд, знакомство с ними необходимо для усвоения и последующего практического использования "Общих критериев".

Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности

Описываются предположения и цели безопасности, функциональные требования и требования доверия, специфичные для конкретных сервисов безопасности. Основное внимание уделено функциональным требованиям, как наиболее важным для обеспечения безопасности.

Биометрическая идентификация и аутентификация

Системы биометрической идентификации и аутентификации, общие сведения о которых можно найти в курсе [91] "Основы информационной безопасности", весьма актуальны и интересны с точки зрения оценки их безопасности. В данном разделе рассматривается профиль защиты [27], разработанный специалистами Министерства обороны США для оценки коммерческих продуктов, применяемых в среде со средними требованиями к безопасности.

Наиболее интересная (и самая большая по объему) часть в этом профиле - описание угроз, которым подвержены системы биометрической идентификации и аутентификации, что наводит на определенные размышления.

Первой упомянута угроза случайного прохождения злоумышленником чисто биометрической процедуры идентификации и аутентификации. Если база биометрических шаблонов велика, то уже этот метод атаки, не требующий ничего, кроме нахальства, может принести успех. Вообще говоря, биометрические системы подвержены ошибкам первого (успешная идентификация и аутентификация лица, не являющегося уполномоченным пользователем) и второго (неправомерный отказ в доступе уполномоченному пользователю) рода. Величины допустимых расхождений эталонного и представленного биометрических шаблонов входят в число параметров безопасности. Неквалифицированный администратор, желая уменьшить число отказов уполномоченным пользователям, способен чрезмерно повысить вероятность ошибки первого рода.

Вторая угроза - мимикрия под атакуемого субъекта (подражание его голосу, попытки воспроизвести подпись и т.п.). Биометрические данные трудно скрыть, поэтому лучше изначально предполагать, что они общеизвестны, и строить защиту, исходя из этого предположения.

Для компрометации биометрических систем могут применяться искусственные средства идентификации (например, желатиновые муляжи глаз). В контролируемой среде подобным артефактом воспользоваться трудно, однако контроль возможен не всегда.

В биометрической базе данных некоторые элементы могут быть "слабее" остальных, т. е. их легче атаковать. Нередко причина заключается в низком качестве биометрического шаблона в сочетании с высокой вероятностью ошибки первого рода. Например, можно использовать как эталонные несколько образцов подписи, имеющих существенные различия. Другой пример - слишком тихая, с паузами речь при запоминании голоса пользователя. "Зашумление" биометрических шаблонов - косвенная угроза, способствующая появлению слабых элементов. Для защиты рекомендуется выявление и удаление (замена) подобных шаблонов.

Злоумышленник с помощью технических средств способен зашумлять каналы связи между частями биометрической системы, чтобы заставить администратора увеличить вероятность ошибок первого рода.

"Атака на близнеца" - угроза, реализуемая в том случае, если в биометрической базе оказываются данные о людях с похожими характеристиками (это могут быть и настоящие близнецы, один из которых - злоумышленник).

Возможно использование "остаточных" биометрических данных от предыдущего пользователя, а также воспроизведение подобных данных.

Неквалифицированные действия штатного администратора и злоумышленные - уполномоченного пользователя, не являющегося администратором, могут привести к изменению значений разного рода параметров безопасности и ослаблению защиты, в частности, изменению или порче базы биометрических данных.

Возможные недостатки в протоколировании и аудите биометрической

системы повышают ее уязвимость, поскольку некоторые атаки длительное время остаются незамеченными.

Выделим ряд специфических функциональных требований:

- мониторинг целостности данных функций безопасности (FPT_ITT.3). Требуется обнаружение модификации данных, передаваемых между разделенными частями объекта оценки; при обнаружении ошибки целостности следует уведомить администратора и запротоколировать это событие;
- противодействие физическому нападению (FPT_PHP.3). Функции безопасности должны противодействовать нарушению физической целостности объекта оценки, а также применению электромагнитных и иных зашумляющих устройств.
- Для мер доверия выбран четвертый оценочный уровень, что можно считать стандартным (общим) решением.

Требования к произвольному (дискреционному) управлению доступом

Дальнейшее изложение основано на первой редакции проекта [1] Руководящего документа Гостехкомиссии России "Безопасность информационных технологий. Контролируемый доступ. Профиль защиты" (ПЗ КД), подготовленной в Центре безопасности информации. Его прототип [35], базирующийся на версии 2.0 "Общих критериев", был разработан в 1999 году в Агентстве национальной безопасности США.

В принципе, ПЗ КД соответствует классу безопасности С2 "Оранжевой книги" [38] или пятому классу защищенности по классификации Гостехкомиссии России для средств вычислительной техники [17], однако применение методологии и обширного набора требования безопасности из "Общих критериев" позволило сделать профиль, по сравнению с упомянутыми документами, существенно более детальным и обоснованным.

Из соответствия классу безопасности С2 следует, что в ПЗ КД рассматривается только дискреционное (произвольное) управление

доступом. Требования, включенные в профиль, направлены на достижение базового уровня безопасности в условиях невраждебного и хорошо управляемого сообщества пользователей при наличии лишь непреднамеренных угроз.

Из числа частных функциональных требований ПЗ КД выделим наиболее важные:

- ассоциация идентификатора пользователя (FAU_GEN.2). Функции безопасности должны ассоциировать каждое потенциально протоколируемое событие с идентификатором пользователя - инициатора этого события (на первый взгляд кажется, что из данного требования есть очевидные исключения, например, неудачные попытки идентификации / аутентификации, однако на этой стадии средства контролируемого доступа еще не используются, а за идентификацию и аутентификацию отвечает другой сервис безопасности);
- выборочный просмотр аудита (FAU_SAR.3). Необходимо предоставить возможность поиска, сортировки, упорядочения регистрационных данных, основываясь на идентификаторах пользователей и, быть может, других специфицированных атрибутах;
- управление доступом, основанное на атрибутах безопасности (FDP_ACF.1). Проводимая политика дискреционного управления доступом должна основываться на таких атрибутах, как идентификатор пользователя и принадлежность к группе (группам), а также атрибутах, ассоциированных с объектами. Последние дают возможность сопоставления разрешенных и запрещенных операций с идентификаторами одного или более пользователей и/или групп, задания разрешенных или запрещенных по умолчанию операций;
- определение атрибутов пользователя (FIA_ATD.1). Для каждого пользователя должен поддерживаться следующий список атрибутов безопасности: идентификатор пользователя, принадлежность к группе, данные аутентификации, допустимые роли;
- верификация секретов (FIA_SOS.1). При однократной попытке использования механизма аутентификации или при неоднократных попытках в течение одной минуты вероятность

случайного доступа должна быть меньше 1:1000000. Любая обратная связь при попытках использования механизма аутентификации не должна приводить к превышению указанного уровня вероятности;

- связывание пользователь-субъект (FIA_USB.1). Функции безопасности должны ассоциировать следующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя: идентификатор пользователя, который ассоциируется с событиями аудита; идентификаторы пользователя, применяемые для осуществления политики дискреционного управления доступом; принадлежность к группам, используемая для осуществления политики дискреционного управления доступом;
- инициализация статических атрибутов (FMT_MSA.3). Должны обеспечиваться ограничительные подразумеваемые значения для атрибутов безопасности, при помощи которых осуществляется политика дискреционного управления доступом (FMT_MSA.3.1). Должна предоставляться возможность определения альтернативных начальных значений для отмены подразумеваемых значений при создании объектов (FMT_MSA.3.2);
- отмена (FMT_REV.1). Право отмены атрибутов безопасности, ассоциированных с объектами, необходимо предоставлять только пользователям, уполномоченным на это политикой дискреционного управления доступом (FMT_REV.1.1).

Рассмотренный проект профиля показывает, что выделение общих требований к сервисам безопасности значительно сокращает специфическую часть, облегчает ее изучение и верификацию.

Требования к принудительному (мандатному) управлению доступом

В данном разделе рассматривается первая редакция проекта [2] Руководящего документа Гостехкомиссии России "Безопасность информационных технологий. Меточная защита. Профиль защиты" (ПЗ МЗ), подготовленная в Центре безопасности информации (см. также [62]). ПЗ МЗ соответствует классу безопасности В1 "Оранжевой книги"

[38] или четвертому классу защищенности по классификации Гостехкомиссии России для средств вычислительной техники [17].

Профиль защиты для мандатного (принудительного) управления доступом имеет много общего с рассмотренным в предыдущем разделе профилем ПЗ КД. Некоторые отличия носят очевидный характер; например, включение меток безопасности в записи регистрационного журнала (семейство функциональных требований FAU_GEN), выборочный просмотр аудита на основании меток безопасности (FAU_SAR) или включение данных о допуске (FIA_ATD) в число атрибутов безопасности пользователя. Ни на общих свойствах этих двух профилей, ни на рутинных отличиях мы останавливаться не будем.

Перечислим специфичные для ПЗ МЗ функциональные требования:

- экспорт данных пользователя (FDP_ETC). При экспорте назначенных данных пользователя должна осуществляться политика мандатного управления доступом (FDP_ETC.1.1, FDP_ETC.2.1). Непомеченные данные экспортируются без атрибутов безопасности (FDP_ETC.1.2), помеченные - с однозначно ассоциированными атрибутами (FDP_ETC.2.2, FDP_ETC.2.3). Устройства, используемые для экспорта данных без атрибутов безопасности, не могут употребляться для экспорта с атрибутами за исключением ситуации, когда изменение в состоянии устройства выполнено вручную и может быть запротоколировано (FDP_ETC.2.4). Отметим, что в ОК в компоненте FDP_ETC.1 отсутствует элемент, необходимый для назначения правил управления экспортом непомеченных данных;
- ограниченное управление информационными потоками (FDP_IFC.1). Для назначенных субъектов и объектов и всех операций над этими субъектами и объектами осуществляется политика мандатного управления доступом (FDP_IFC.1.1);
- иерархические атрибуты безопасности (FDP_IFF.2). Политика мандатного управления доступом должна основываться на метках безопасности субъектов и объектов (FDP_IFF.2.1). Метка безопасности составляется из иерархического уровня и набора неиерархических категорий. На множестве допустимых меток безопасности должно быть определено отношение частичного порядка с указанными далее свойствами (FDP_IFF.2.7). Метки

равны, если совпадают их уровни и наборы категорий. Метка A больше метки B, если уровень A больше уровня B и набор категорий B является подмножеством набора A; если уровень A равен уровню B и набор категорий B является собственным подмножеством набора A. Метки несравнимы, если они не равны и ни одна из меток не больше другой. Для любых двух допустимых меток существует наименьшая верхняя грань, которая больше или равна этим меткам, а также наибольшая нижняя грань, которая не больше обеих меток. Должно поддерживаться по крайней мере 16 уровней и 64 категории. Информационный поток между управляемыми субъектами и объектами посредством управляемой операции разрешен, если метка источника больше или равна метке целевого субъекта или объекта (FDP_IFF.2.2);

- импорт данных пользователя (FDP_ITC). Это семейство требований симметрично экспортным требованиям FDP_ETC;
- управление атрибутами безопасности (FMT_MSA.1). Функции безопасности должны осуществлять политику мандатного управления доступом, чтобы ограничить право модификации меток безопасности, ассоциированных с объектами;
- роли безопасности (FMT_SMR.1). В число поддерживаемых должна входить роль, дающая право изменять атрибуты безопасности объектов.

Для требований доверия безопасности рассматриваемый профиль предписывает оценочный уровень 3, усиленный компонентом ADV_SPM.1 (неформальная модель политики безопасности объекта оценки).

Ролевое управление доступом

Ролевое управление доступом (Role-Based Access Control, RBAC) представляет собой универсальный каркас, нейтральный по отношению к конкретной дисциплине разграничения доступа и предназначенный в первую очередь для упрощения администрирования ИС с большим числом пользователей и различных ресурсов.

Ниже рассматриваются специфические требования для профиля RBAC [74], [72], основанного на версии 2.0 "Общих критериев".

Разделение обязанностей - существенная и специфичная для ролевого управления доступом цель безопасности. Возможность ее достижения - важное достоинство ролевого доступа.

Еще одна особая и методологически важная цель безопасности - организация иерархии ролей с наследованием прав доступа. Применение идей и методов объектно-ориентированного подхода необходимо для успешной работы с большими системами.

Для ролевого управления доступом характерны следующие функции:

- создание и удаление ролей; создание, удаление и модификация атрибутов ролей и отношений между ролями;
- формирование и поддержка ассоциаций между пользователями и ролями;
- формирование и поддержка ассоциаций между правами доступа и ролями.

Эти функции обслуживаются тремя классами функциональных требований, на которых мы и остановимся:

- ограниченное управление доступом (FDP_ACC.1.1). По крайней мере для части операций субъектов над объектами должно действовать ролевое управление доступом, которое в общем случае может существовать с другими дисциплинами разграничения доступа;
- управление доступом, основанное на атрибутах безопасности (FDP_ACF.1.1). В число учитываемых атрибутов безопасности следует включить, помимо прочих, присвоенные субъекту роли и права доступа этих ролей;
- управление данными функций безопасности (FMT_MTD). Только администратор должен иметь возможность определения и изменения ролей, их атрибутов, связей между ними и ограничений на подобные связи (FMT_MTD.1.1). Необходимы и другие требования класса FMT, но они в данном случае носят прямолинейный характер и рассматриваться не будут.

Требования безопасности при сбое (семейство FPT_FLS) имеют технический характер. Должно сохраняться безопасное состояние в

ситуациях, когда база данных ролей недоступна или повреждена (FPT_FLS.1.1). Как и в случае управления безопасностью, другие требования этого класса необходимы, но не нуждаются в детальном рассмотрении.

Можно видеть, что функциональные требования "Общих критериев" полезны для достижения тактических целей безопасности. Стратегические цели, носящие концептуальный или архитектурный характер, - организация иерархии ролей с небольшим числом сущностей на каждом уровне или следование принципу разделения обязанностей - приходится формулировать отдельно, без стандартизованной понятийной базы.

Межсетевое экранирование

Для межсетевых экранов (МЭ) разработан целый ряд профилей защиты и проектов подобных профилей (см. [40], [57], [56], [23], [24]). Отметим, что экранирование - это, видимо, единственный сервис безопасности, для которого Гостехкомиссия России одной из первых в мире разработала и ввела в действие Руководящий документ [18], его основные идеи получили международное признание и фигурируют в профилях защиты, имеющих официальный статус в таких странах, как США.

Межсетевые экраны классифицируются на основании уровней эталонной семиуровневой модели, на которых осуществляется фильтрация потоков данных. Далее рассматриваются специфические требования двух видов профилей, соответствующих фильтрации на уровнях вплоть до транспортного (пакетная фильтрация) и на всех уровнях, включая прикладной (комплексное экранирование).

Изложение вопросов пакетной фильтрации основывается на профиле [40], наиболее представительном среди документов аналогичного назначения.

В общем случае рассматривается многокомпонентный межсетевой экран. Политика безопасности МЭ базируется на принципе "все, что не разрешено, запрещено".

Информация, поступающая в МЭ, может предназначаться для фильтрации или для изменения параметров самого МЭ. В первом случае идентификация / аутентификация не требуется, во втором она обязательна, причем используются одноразовые пароли (идентифицироваться и аутентифицироваться должны как операторы, осуществляющие удаленное администрирование, так и устройства, в частности маршрутизаторы, посылающие информацию для МЭ, например, измененные таблицы маршрутизации). Для формального описания перечисленных требований применяются компоненты FMT_MSA.1 (управление атрибутами безопасности), FMT_MSA.3 (статическая инициализация атрибутов) и FIA_UAU.5 (сочетание механизмов аутентификации).

Поскольку "Общие критерии" не предназначены для оценки специфических качеств криптографических алгоритмов, рассматриваемый профиль ссылается на федеральный стандарт США FIPS PUB 140-1, требуя согласованности с ним для средств аутентификации, шифрования и контроля целостности. Формальной оболочкой для данного требования является компонент OK FCS_COP.1.

Решения по фильтрации потоков данных принимаются на основе набора правил, в которых могут фигурировать исходный и целевой сетевые адреса, протокол транспортного уровня, исходный и целевой порты, а также входной и выходной сетевой интерфейс. Формально ограниченное управление информационными потоками между неаутентифицируемыми сущностями описывается компонентом FDP_IFC.1, а используемые при этом простые атрибуты безопасности - компонентом FDP_IFF.1. Выборочный просмотр регистрационной информации (FAU_SAR.3.1) может основываться на адресах, диапазонах адресов, номерах портов, диапазонах дат и времени.

В плане требований доверия безопасности рассматриваемый профиль ограничивается оценочным уровнем 2. На наш взгляд, этого недостаточно для защиты критически важных систем, функционирующих в среде со средним уровнем риска.

Отметим, что за пределами рассмотрения в профиле остались такие технологические аспекты, как согласованность базы правил фильтрации для многокомпонентных конфигураций, удобство административного

интерфейса (необходимое условие уменьшения числа ошибок администрирования), защита от атак на доступность.

Переходя к вопросам комплексного экранирования, отметим, что современные комплексные межсетевые экраны, осуществляющие фильтрацию на всех уровнях, включая прикладной, по сравнению с пакетными фильтрами обеспечивают более надежную защиту, что нашло отражение в дополнительных требованиях безопасности, включенных в профили [56] и [23], [24].

В состав комплексных межсетевых экранов могут входить серверы-посредники, они требуют от пользователей соответствующих сетевых услуг (таких, например, как FTP или Telnet) идентификации и аутентификации (с помощью механизмов, основанных на данных одноразового использования и соответствующих компоненту FIA_UAU.4).

В правилах фильтрации могут фигурировать команды протоколов прикладного уровня и параметры команд.

В проекте профиля [23] предписывается организация полного управления межсетевым доступом (компонент FDP_ACC.2), а также предотвращение угроз доступности (FDP_IFC.2.1).

Важным моментом проекта [23] являются требования анонимности (FPR_ANO.1.1), псевдонимности (FPR_PSE.1) и невозможности ассоциации (FPR_UNL.1.1) межсетевого доступа для сущностей, ассоциированных с защищаемой сетью или самим межсетевым экраном. Эти требования могут быть выполнены на основе использования механизма трансляции адресов и применения серверов-посредников.

Пример проекта [23] показывает, что в российских условиях можно обойти формальные, но не содержательные, проблемы, связанные с криптографией. В любом случае криптографические аппаратные и программные модули необходимо разрабатывать и/или оценивать, даже если само слово "криптография" в профиле защиты отсутствует.

Шифрование и контроль целостности необходимы для организации доверенного канала с целью обеспечения безопасности удаленного

администрирования (соответствующие требования были рассмотрены ранее в числе общих для различных сервисов). Для них существуют российские ГОСТы, которыми можно воспользоваться при построении аналогов профилей [40] и [56]. Аутентификация, устойчивая к сетевым угрозам, также обязательна, однако национальный криптографический ГОСТ для нее не принят. Приходится, как это сделано в [23], ограничиваться общими требованиями верификации секретов (FIA_SOS.1) и защищенности от подделки (FIA_UAU.3). Впрочем, в любом случае привлечение национальных (а не международных) стандартов создает проблемы взаимодействия с иностранными партнерами и осложняет взаимное признание сертификатов разными странами.

Системы активного аудита

В работе [6] приведен набросок семейства профилей защиты для классификации систем активного аудита, а также соображения по расширению набора функциональных требований "Общих критериев". Проекты ПЗ для важнейших компонентов подобных систем - анализатора и сенсора - представлены в [54], [55].

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы - злоумышленное (в соответствии с заранее определенной политикой безопасности) или нетипичное (согласно принятым критериям).

Назначение активного аудита - оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

По целому ряду причин, из числа которых мы выделим обеспечение масштабируемости, средства активного аудита строятся в архитектуре менеджер / агент. Основными агентскими компонентами являются компоненты извлечения регистрационной информации (сенсоры). Анализ, принятие решений - функции менеджеров. Очевидно, между менеджерами и агентами должны быть сформированы доверенные каналы.

В число функций безопасности, специфичных для средств активного

аудита, входят генерация и извлечение регистрационной информации, ее анализ и реагирование на подозрительную активность.

Отметим, что такой универсальный аспект, как безопасное администрирование, для средств активного аудита приобретает особое значение, если включить в него автоматическую коррекцию (в первую очередь - пополнение) базы сигнатур атак. Тем не менее, соответствующие требования целесообразно отнести к числу общих, поскольку аналогичная возможность нужна, например, другому сервису безопасности - анализу защищенности.

Из существенных для активного аудита компонентов класса FAU "Аудит безопасности" в "Общих критериях" отсутствуют анализ на соответствие политике безопасности (пороговый, статистический и сигнатурный анализы в семействе FAU_SAA предусмотрены), хранилища для описаний контролируемых объектов и для анализируемой информации, а также все интерфейсные компоненты. Слабо отражена возможность выбора рассматриваемых событий как сенсорами (агентами), так и анализаторами (менеджерами).

С целью адекватного отражения специфики средств активного аудита в [6] предложен ряд добавлений к стандартному набору функциональных требований.

В семейство FAU_GEN (генерация данных аудита безопасности) предлагается включить два новых компонента. FAU_GEN.3 - ассоциирование вызвавшего событие объекта с включением в регистрационные записи имени (идентификатора) этого объекта. На минимальном уровне должны протоколироваться открытие/закрытие объекта (установление/разрыв соединения и т.п.), на базовом - все промежуточные операции. На детальном уровне в регистрационные записи должны входить все операнды операции с объектом.

Компонент FAU_GEN.3 добавлен по двум причинам. Во-первых, должна соблюдаться симметрия между субъектами и объектами. Во-вторых, статистические профили целесообразно строить не для субъектов, а для объектов, но для этого нужно располагать соответствующей информацией.

Еще один предлагаемый компонент - FAU_GEN.4 - предназначен для

обеспечения неотказуемости сервиса, пользующегося услугами семейства FAU_GEN, от регистрации события. Вообще говоря, неотказуемость реализуется, даже если не были востребованы коммуникации, поэтому здесь нельзя прибегнуть к классу FCO.

Стандартный компонент FAU_SAR.3 дает возможность осуществлять поиск и сортировку регистрационной информации, задавая в качестве критериев логические выражения. Подобные выражения полезны также для задания фильтров, управляющих работой сенсоров.

Автоматический анализ регистрационной информации с целью выявления подозрительной активности представлен в "Общих критериях" четырьмя компонентами семейства FAU_SAA.

FAU_SAA.1 ориентирован на обнаружение превышения порогов, заданных фиксированным набором правил.

FAU_SAA.2 служит для выявления нетипичной активности путем анализа профилей поведения. В "Общих критериях" предлагаются профили для субъектов, хотя профили объектов могут оказаться предпочтительными.

"Общие критерии" допускают анализ и в реальном времени, и постфактум; поддержку анализа в реальном времени следует рассматривать как важнейшую отличительную особенность средств активного аудита.

FAU_SAA.3 направлен на обнаружение простых атак путем проведения сигнатурного анализа.

FAU_SAA.4 позволяет выявлять сложные, многоэтапные атаки, осуществляемые группой злоумышленников.

Предусматривается возможность настройки всех четырех компонентов путем добавления, модификации или удаления правил, отслеживаемых субъектов и сигнатур.

В [6] вводится еще один компонент, FAU_SAA.5, фиксирующий нарушения политики безопасности. Задавать политики предлагается с помощью предикатов первого порядка.

Что касается автоматического реагирования на подозрительную активность, то "Общие критерии", по сути, ограничились констатацией подобной возможности. В [6] рассматривается более сложная сущность - решатель, который, получив рекомендации от компонентов анализа, определяет, действительно ли имеет место подозрительная активность, и, при необходимости, надлежащим образом реагирует (выбирая форму реакции в зависимости от серьезности выявленных нарушений).

Это значит, что решатель должен уметь:

- ранжировать подозрительную активность ;
- реагировать в соответствии с рангом нарушения.

Управление обоими аспектами поручено администратору безопасности.

В качестве отдельной возможности, присущей системам высокого класса, фигурирует проведение корреляционного анализа информации.

Описание контролируемых объектов и хранение соответствующей информации - важнейшая составная часть средств активного аудита, придающая им свойства расширяемости и настраиваемости. К этому компоненту предъявляются главным образом технологические требования.

Мониторы, организующие оболочки для менеджеров средств активного аудита, должны обладать двумя группами свойств:

- обеспечивать защиту процессов, составляющих менеджер, от злоумышленных воздействий;
- обеспечивать высокую доступность этих процессов.

Первая группа обслуживается семейством FPT_SEP.

Вторая группа свойств поддерживается такими техническими решениями, как программное обеспечение (ПО) промежуточного слоя, кластерные конфигурации и т.д. В плане безопасности целесообразно следовать требованиям FPT_FLS.1 (невозможность перехода в небезопасное состояние в случае сбоя или отказа), а также FPT_RCV.2, FPT_RCV.3, FPT_RCV.4 (надежное восстановление в автоматическом

режиме, без потери данных, с точностью до функции безопасности).

Безопасность интерфейсов монитора (с другими мониторами, сенсорами, администратором безопасности) может обеспечиваться компонентами FPT_ITI.1, FPT_ITI.2 (обнаружение и исправление модификации экспортируемых данных), FPT_ITC.1 (конфиденциальность экспортируемых данных), FPT_ITA.1 (доступность экспортируемых данных).

На рабочем месте администратора безопасности необходимо иметь стандартные для средств управления функции: графический интерфейс, возможность настройки способа визуализации, уровня детализации и отбора отображаемых событий.

Специфичной для средств активного аудита является возможность получения объяснений от анализаторов и решателей по поводу обнаруженной подозрительной активности. Такие объяснения помогают выбрать адекватный способ реагирования.

При формировании классификационной схемы средств активного аудита в [23] предлагается выделить базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Профили защиты, соответствующие классам защищенности, строятся на основе базового ПЗ и соответствующих комбинаций ФП.

В [23] предлагается зафиксировать профили для следующих разновидностей средств активного аудита:

- класс 5 - защита одного информационного сервиса с отслеживанием фиксированного набора характеристик и пороговым анализом (базовый ПЗ);
- класс 4 - защита однохостовой конфигурации с произвольным набором информационных сервисов, отслеживанием сетевого трафика, системных и прикладных событий, пороговым и простым сигнатурным анализом в реальном масштабе времени;
- класс 3 - защита сегмента локальной сети от многоэтапных атак при сохранении остальных предположений класса 4;
- класс 2 - защита произвольной конфигурации с выявлением нетипичного поведения при сохранении остальных

предположений класса 3;

- класс 1 - наложение всех требований с возможностью обеспечения заданного соотношения между ошибками первого и второго рода.

В контексте "Общих критериев" важным и сложным является поднятый в [23] вопрос о целесообразности разработки и применения жестких классификационных схем для сервисов безопасности. С одной стороны, гибкость требований ОК такова, что на их основе можно разработать множество профилей защиты с минимальными требованиями, учитывающими специфику информационных систем и их окружения и позволяющими добиться необходимого уровня безопасности с минимальными затратами. С другой стороны, едва ли не все ИС имеют тенденцию к частым и многочисленным изменениям, способным нарушить истинность сделанных в ПЗ предположений безопасности. Слишком точная подгонка профилей защиты (равно как и характеристик ИС) опасна, у них должен быть запас прочности. В приведенной выше классификации предусмотрено изменение защищаемой конфигурации, поэтому заказчик может выбрать класс "на вырост".

Классификационная схема показывает способы усиления функций безопасности (для средств активного аудита это в первую очередь расширение спектра отслеживаемых параметров, повышение оперативности и усложнение методов анализа регистрационной информации), что важно при выборе подходящей реализации сервиса безопасности из большого числа доступных вариантов.

Наконец, наличие большого числа несравнимых между собой минимальных профилей создает проблемы и для производителей сервисов безопасности, поскольку вовлекает их в многочисленные процедуры сертификации. Конечно, при этом могут быть использованы результаты предыдущих испытаний, но у каждой процедуры все равно остается существенная постоянная часть (финансовая и временная).

Можно сделать вывод, что для совокупности профилей защиты целесообразно с самого начала планировать построение иерархии наследования с применением соответствующих функциональных пакетов. Часть узлов в этой иерархии (например, общие требования к сервисам безопасности) могут быть фиктивными в том смысле, что им

не соответствуют профили для законченных изделий ИТ, однако они столь же необходимы, как и (обобщенные) интерфейсы в объектно-ориентированных системах.

Анонимизаторы

Анонимизаторы предназначены для выполнения функциональных требований приватности (класс FPR "Общих критериев"). В данном разделе, основываясь на статье [71] и профиле защиты [45], мы рассмотрим одну из разновидностей анонимизаторов - сеть серверов пересылки, обеспечивающую приватность пользователей электронной почты.

Вероятно, приватность - это единственный класс функциональных требований ОК, направленных не на обеспечение безопасности иерархически организованных, жестко администрируемых систем, а на защиту специфических интересов пользователей информационных сервисов. В "Оранжевой книге" Министерства обороны США и Руководящих документах Гостехкомиссии России подобных требований не было, поэтому необходимо накапливать опыт по их применению, что придает работам [71] и [45] особую ценность. Происходит становление так называемой многоаспектной информационной безопасности, когда делается попытка учесть весь спектр интересов (порой конфликтующих между собой) всех субъектов информационных отношений, а также все виды конфигураций ИС, в том числе децентрализованные, не имеющие единого центра управления.

Напомним, что класс FPR содержит четыре семейства: FPR_ANO (анонимность - возможность совершать действия, не раскрывая идентификационных данных пользователя), FPR_PSE (псевдонимность - анонимность с сохранением подотчетности), FPR_UNL (невозможность ассоциации - анонимность с сокрытием связи между действиями одного пользователя), FPR_UNO (скрытность, или ненаблюдаемость - сокрытие самого факта использования ресурса или услуги). Псевдонимность полезна, например, когда за многократное обращение к каким-то специфическим платным услугам полагаются скидки. Невозможность ассоциации позволяет защититься от раскрытия личности пользователя путем анализа профиля его поведения. Назначение семейств FPR_ANO и FPR_UNO очевидно.

Сеть серверов пересылки почты состоит из независимо администрируемых узлов. Отправитель определяет в ней путь сообщения, которое шифруется таким образом, что каждому серверу известны только предыдущий и следующий узлы. В результате достигается невозможность установления ассоциации между отправителем и получателем. Если в сообщении отсутствуют идентификационные данные отправителя, то обеспечиваются анонимность, невозможность ассоциации и, отчасти, скрытность. Псевдонимность может быть реализована путем применения особым образом заданных обратных адресов. Отметим, что на тех же принципах организуется работа анонимизаторов для других информационных сервисов, в частности, для Web-доступа. Существуют свободно распространяемые (Mixmaster) и коммерческие (компании Zero Knowledge Systems) реализации сетей серверов пересылки.

Сеть серверов пересылки можно рассматривать двояко: изнутри и извне. Традиционный взгляд изнутри, с точки зрения гипотетического администратора сети, обязанного обеспечить ее безопасность и высокую доступность, ведет к традиционному же профилю защиты, требования которого противоречат приватности. Действительно, для защиты сети от атак на доступность необходимо выявлять подозрительную активность путем накопления и анализа регистрационной информации, уметь прослеживать пользователей и т.п. В силу указанных причин в данном разделе мы будем придерживаться взгляда извне, с точки зрения пользователя сервиса анонимизации; с этих позиций и разработан профиль [45].

Для сети серверов пересылки сообщений выделяются следующие специфические угрозы безопасности:

- возможность установления ассоциации между отправителем и получателем, если путь сообщения проходит только через один сервер пересылки;
- установление контроля над несколькими серверами пересылки и проведение совместного анализа их регистрационной информации.

Отметим также, что многие общие угрозы (маскарад сервера с целью распространения поддельных криптографических ключей, установление

контроля над одним из серверов пересылки для извлечения необходимой конфиденциальной информации, перенаправление потоков данных с целью подмены части сети пересылки, анализ потоков данных между пользовательской системой и сетью пересылки и т.п.) приобретают в указанном контексте специфический характер, так как направлены на нарушение приватности пользователей.

Формулируются два специфических положения политики безопасности:

- обеспечение анонимности сообщений, т. е. получатель не может узнать идентификационных данных отправителя, если последний сам не поместил их в сообщение в явном виде;
- обеспечение невозможности прослеживать сообщения, т. е. в результате перехвата нельзя одновременно узнать отправителя и получателя.

Перечислим специфические цели безопасности:

- серверы пересылки должны принимать и обрабатывать сообщения, не опираясь на какую-либо информацию об отправителе;
- содержание сообщений на всем пути следования скрыто от сторонних наблюдателей;
- сеть серверов пересылки необходимо построить таким образом, чтобы успешно противостоять попыткам анализа потоков данных, в частности, потоков между пользовательской системой и сетью;
- сеть серверов пересылки следует построить с учетом того, чтобы пользователь мог (и, более того, был обязан) корректно распределять между узлами сети данные, существенные для невозможности прослеживания адресатов сообщения, а также выбирать узлы, участвующие в обработке сообщения. Сеть пересылки обязана реализовать пользовательский выбор;
- пользователи и узлы сети пересылки должны однозначно идентифицироваться, а сообщения - доставляться в нужные узлы с сохранением конфиденциальности соответствующих данных;
- сеть серверов пересылки должна быть построена так, чтобы использование, распространение и интервал времени доступности данных, влияющих на возможность ассоциации пользователей, были минимальными;

- ни одному субъекту (пользователю, администратору, злоумышленнику) нельзя предоставлять возможность получения информации, достаточной для прослеживания отправителей сообщений.

Специфические цели безопасности для среды:

- узлы сети пересылки должны администрироваться независимо и, более того, антагонистично;
- сеть пересылки должна быть топологически распределенной.

Чтобы лучше понять приведенные ниже специфические функциональные требования, целесообразно помнить, что рассматриваемый профиль защиты сформирован с позиций пользователя, так что в объект оценки (ОО) входят как серверы пересылки, так и клиентские системы. Все потоки данных контролируются функциями безопасности ОО; экспорта или импорта данных не происходит.

В пределах области действия функций безопасности имеют место следующие виды операций:

- передача сообщения клиентской системой серверу пересылки;
- пересылка сообщений, а также управляющей информации (в том числе ключевой), между серверами;
- доставка сообщения с сервера на клиентскую систему;
- обработка сервером пересылки (транзитных) сообщений;
- операции, выполняемые сервером с криптографическими ключами: генерация, распространение, хранение, доступ, использование, уничтожение;
- порождение сервером пересылки фиктивных сообщений.

Для отправки сообщения пользователь должен задать целевой адрес и цепочку серверов пересылки. При получении почты требуется аутентификация, так как входящие сообщения нуждаются в расшифровании.

В пределах объекта оценки действует специфическая форма политики принудительного управления доступом, состоящая в том, что каждый

элемент пользовательских данных приписывается определенному субъекту, и только этот субъект получает право на доступ к приписанным ему данным. Далее провозглашается политика борьбы со скрытыми каналами, чтобы противостоять попыткам анализа потоков данных.

Специфические функциональные требования состоят в следующем.

- полное управление доступом (FDP_ACC.2). Политика принудительного управления доступом должна распространяться на всех субъектов (серверы пересылки, клиентское ПО, пользователи, администраторы), все объекты (в том числе на содержание и маршрутную информацию сообщений) и все операции;
- ограниченное управление информационными потоками (FDP_IFC.1). Должна проводиться в жизнь политика борьбы со скрытыми каналами применительно к серверам пересылки, клиентскому ПО, сообщениям, передаче и приему сообщений (FDP_IFC.1.1);
- частичное устранение неразрешенных информационных потоков (FDP_IFF.4). Политику борьбы со скрытыми каналами необходимо внедрять, чтобы уменьшить до заданных пределов утечку информации о работе пользователей с сетью пересылки, возникающую за счет анализа периферийных потоков данных (FDP_IFF.4.1). Получение профилей поведения компонентов сети пересылки путем анализа периферийных потоков данных должно быть невозможным (FDP_IFF.4.2);
- полное управление временем хранения данных (FDP_IRC.2). Все объекты, нужные для нормальной работы сети пересылки, удаляются сразу после завершения операций с ними. Отметим, что это не просто специфическое, но новое функциональное требование, предложенное автором профиля защиты;
- управление атрибутами безопасности (FMT_MSA.1). Согласно политике принудительного управления доступом, только пользователь, сгенерировавший данные, может выполнять операции над их атрибутами безопасности, в число которых входят маршрут сообщения и его рандомизация, минимальное число пересылок, число отправляемых избыточных сообщений, параметры потоков данных и криптографических алгоритмов и

т.п. (FMT_MSA.1.1);

- анонимность без запроса информации (FPR_ANO.2). Должны обеспечиваться невозможность определения подлинного имени отправителя сообщения, обрабатываемого сетью серверов пересылки (FPR_ANO.2.1), а также невозможность отслеживания и анонимность пересылки сообщений для всех пользователей без запроса какой-либо ссылки на подлинное имя пользователя (FPR_ANO.2.2);
- размещение информационных ресурсов (FPR_TRD.2). Сеть пересылки должна состоять из отдельных взаимодействующих частей, в каждой из которых реализуются свои правила аутентификации и управления доступом (FPR_TRD.2.1). Доступ к данным другой части предоставляется только по явному запросу (FPR_TRD.2.2). Данные, критичные для невозможности ассоциации (маршрут, время и т.п.), должны храниться в виде, исключающем их полное чтение одной частью сети, чтобы обеспечить невозможность прослеживания всей цепочки между отправителем и получателем сообщения (FPR_TRD.2.3). Этот и два последующих компонента предложены автором профиля защиты;
- распределение обработки сообщений (FPR_TRD.3). По своей сути этот компонент аналогичен предыдущему с точностью до замены слова "храниться" на "обрабатываться";
- невозможность ассоциации пользователей (FPR_UNL.2). Должна обеспечиваться невозможность установления факта отправки сообщений одним и тем же пользователем.

Для мер доверия безопасности предлагается оценочный уровень 5. Напомним, что его характерными особенностями являются применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними, а также проведение анализа скрытых каналов разработчиками и оценщиками. Это очень высокий уровень, но в данном случае его выбор представляется оправданным, поскольку, с одной стороны, объект оценки относительно прост, с легко формализуемой политикой безопасности, а с другой, в функциональных требованиях предусмотрен анализ скрытых каналов.

Рассмотренный профиль защиты, на наш взгляд, весьма поучителен. Он

демонстрирует как достоинства, так и недостатки "Общих критериев". К числу достоинств можно отнести богатый набор современных функциональных требований, особо выделив требования приватности. К сожалению, как мы уже отмечали, они носят "точечный", а не концептуальный или архитектурный характер. Для требования распределенности архитектуры пришлось вводить новое семейство - FPR_TRD. Отметим, в свою очередь, что отнесение его к классу приватности не кажется нам оправданным. Распределенность принципиально важна для целого ряда систем, но если в системах электронных платежей, как и в сети серверов пересылки, это необходимое условие приватности (в профиле новое семейство получило наименование "распределения доверия"), то во многих других случаях она играет инфраструктурную роль, обеспечивая живучесть (устойчивость к отказам) и/или масштабируемость (в сочетании с архитектурой менеджер / агент). Очевидно, архитектурные требования заслуживают отдельного класса.

Требования безопасности повторного использования, безусловно, должны быть дополнены требованиями минимизации времени хранения объектов, что и сделано в рассмотренном профиле. Это важно, помимо приватности, практически для всех приложений криптографии, в ситуациях, когда образуются временные файлы с информацией ограниченного доступа и т.п.

Авторы работ [71], [45] справедливо замечают, что введение новых функциональных требований имеет свои оборотные стороны. Конкретные профили получаются проще, естественнее, однако их сравнение с нестандартными компонентами усложняется. Возможный выход подсказывает технология программирования, предусматривающая проблемно-ориентированные расширения базовых интерфейсов, как это выполнено, например, в Java-системах. Подобные расширения можно разработать и стандартизовать быстрее, чем полный набор требований, поскольку они затрагивают более узкий круг специалистов, объединенных к тому же общностью интересов.

Выпуск и управление сертификатами

В документе [63] предлагается упорядоченное семейство из четырех

профилей защиты для аппаратно-программных компонентов, реализующих выпуск, аннулирование и управление сертификатами открытых ключей (удовлетворяющими, например, спецификациям X.509) (Certificate Issuing and Management Components, CIMC).

Таким образом, перед нами жесткая классификационная схема, рассчитанная на применение в разнообразных средах. Каждый заказчик, учитывая степень критичности ИС и реальные риски, сам выбирает необходимый уровень защищенности и соответствующий ему профиль. На нижнем (первом) уровне потенциал злоумышленников и риски предполагаются низкими, прежде всего обеспечивается защита от случайных ошибок авторизованных пользователей (например, за счет использования принципа разделения обязанностей). При переходе на более высокие уровни угрозы нарастают, а требования ужесточаются. На верхнем (четвертом) уровне злоумышленниками могут быть и авторизованные пользователи, а требования безопасности оказываются настолько жесткими, что удовлетворить им могут только перспективные изделия ИТ. Это разумный подход, снабжающий ориентирами и заказчиков, и разработчиков.

Объект оценки в профилях из [63] является элементом инфраструктуры открытых ключей и в общем случае включает нижеследующие функциональные компоненты:

- центр выпуска и аннулирования сертификатов (именуемый также удостоверяющим центром, УЦ). Это - ядро ОО. Сгенерированная информация помещается в хранилище (см. далее). Между различными УЦ могут существовать отношения доверия;
- центры приема пользовательских запросов на создание сертификатов или изменение их статуса. Обязательные компоненты объекта оценки, которые верифицируют представленные пользователем данные;
- серверы, обслуживающие протокол оперативной выдачи статуса сертификатов. Этот компонент может отсутствовать или находиться за пределами ОО;
- серверы восстановления и/или распространения секретного ключевого материала - дополнительная функция.

Отметим, что хранилище сертификатов и информации об их статусе,

обслуживающее запросы приложений, находится вне рамок ОО.

Помимо функциональных, в объект оценки входят инфраструктурные компоненты:

- криптографический модуль. Он подписывает сертификаты и списки их аннулирования, при необходимости генерирует криптографические ключи. Требования безопасности, предъявляемые к криптографическим модулям, изложены в федеральном стандарте США FIPS PUB 140-2 [41], дополнившем FIPS PUB 140-1 (см. [36]);
- модуль администрирования;
- модуль идентификации и аутентификации ;
- модуль ролевого управления доступом;
- модуль протоколирования и аудита.

Представленная выше логическая компонентная архитектура не обязательно совпадает с физической структурой объекта оценки. В принципе возможна монолитная реализация ОО, объединение/ расщепление компонентов и т.д.

Переходя к специфическим функциональным требованиям безопасности для среды, отметим выделение в [63] четырех ролей:

- администратор (отвечает за установку, конфигурирование, обслуживание нужд пользователей и т.п.);
- оператор (выполняет резервное копирование и восстановление);
- инспектор (ведает запросами и утверждением сертификатов и их статуса);
- аудитор (анализирует регистрационную информацию).

В соответствии с компонентом FMT_SMR.2 (ограничения на роли безопасности), один пользователь не может выступать более чем в одной из перечисленных выше ролей (FMT_SMR.2.3).

Среда должна обеспечить защиту конфиденциальности данных пользователя при передаче между функциями безопасности (FDP_UCT). Более точно, надо обеспечить базовую конфиденциальность обмена данными (FDP_UCT.1). Аналогичная защита необходима для

конфиденциальных данных самой среды (FPT_ITC.1, FPT_ITT.1). Кроме того, требуется контроль целостности данных.

Криптографическими методами контролируется целостность (в частности, аутентичность) программного кода, присутствующего в системе, и кода, который в принципе может быть загружен (дополнительные требования профиля FPT_TST_CIMC.2 и FPT_TST_CIMC.3).

Среди специфических (более того, дополнительных, по сравнению с "Общими критериями") функциональных требований безопасности для объекта оценки выделим наиболее значимые:

- инициирование и обработка события подписывания регистрационного журнала (FPT_CIMC_TSP.1), выполняемого с конфигурируемой периодичностью. Подпись должна контролировать целостность по крайней мере тех регистрационных записей, которые появились после предыдущего подписывания. В регистрационной записи о самом событии подписывания присутствуют электронная цифровая подпись, значение хэш-функции или имитовставка аналогичного назначения;
- инициирование и обработка события постановки третьей стороной подписанных меток времени (FPT_CIMC_TSP.2). Этот компонент аналогичен предыдущему и обеспечивает дополнительный контроль целостности регистрационных данных (например, на случай компрометации объекта оценки);
- резервное копирование и восстановление (FDP_CIMC_BKP.1), с дополнительными (криптографическими) мерами контроля целостности и обеспечения конфиденциальности (FDP_CIMC_BKP.2), с точностью до последней завершенной транзакции (FDP_CIMC_BKP.3). Названные компоненты направлены на безопасное (в том числе свободное от внедрения вредоносного кода) восстановление. Отметим, что подобные требования полезны также для СУБД и других систем с транзакциями;
- принудительные доказательство и верификация подлинности источника данных о статусе сертификатов и других данных, критичных для безопасности (FCO_NRO_CIMC.3). Аналогично

должны контролироваться заявки на регистрацию сертификатов. Предпочтительный способ доказательства подлинности - цифровые подписи (FCO_NRO_CIMC.4).;

- экспортируемая информация об изменении статуса сертификатов должна иметь формат, описанный в спецификациях X.509 для списков аннулирования или RFC 2560 для протокола оперативной выдачи статуса сертификатов (FDP_CIMC_CSE.1);
- защита конфиденциальности секретных ключей пользователей (FDP_ACF_CIMC.2) и функций безопасности (FMT_MTD_CIMC.4). Секретные ключи обслуживающего персонала и функций безопасности объекта оценки должны храниться в стандартном криптографическом модуле или шифроваться стандартными методами. Секретные ключи пользователей шифруются с помощью долговременных ключей защиты. Аналогичные требования предъявляются к хранению секретных ключей симметричных методов шифрования (FDP_ACF_CIMC.3 и FMT_MTD_CIMC.5);
- секретные ключи должны экспортироваться либо в зашифрованном виде, либо с использованием процедур разделения знаний (FDP_ETC_CIMC.4, FDP_ETC_CIMC.5, FMT_MTD_CIMC.6, FMT_MTD_CIMC.7);
- контроль целостности хранимых открытых ключей (FDP_DSI_CIMC.3). Открытые ключи, хранимые в объекте оценки вне криптографического модуля, нужно защитить от несанкционированного изменения стандартными криптографическими методами. Проверку целостности требуется производить при каждом доступе к ключу;
- обнуление секретных ключей (FCS_CKM_CIMC.5). Функции безопасности должны обеспечить обнуление открытого представления секретных ключей в криптографическом модуле ;
- контроль допустимости значений полей сертификатов (FMT_MOF_CIMC.3). Функции безопасности контролируют значения полей сертификатов в соответствии с правилами, заданными администратором. Аналогичные проверки необходимо производить для списков аннулированных сертификатов (FMT_MOF_CIMC.5) и сообщений протокола оперативной выдачи статуса сертификатов (FMT_MOF_CIMC.6);
- генерация сертификатов (FDP_CIMC_CER.1). Генерируются только корректные сертификаты, удовлетворяющие требованиям

стандарта (X.509) и правилам, заданным администратором. Такие же требования должны выполняться для списков аннулированных сертификатов (FDP_CIMC_CRL.1) и сообщений протокола оперативной выдачи статуса сертификатов (FDP_CIMC_OCSP.1). До выпуска сертификата необходимо убедиться, что его предполагаемый владелец обладает секретным ключом, ассоциированным с открытым ключом из сертификата.

Требования доверия безопасности усиливаются параллельно с возрастанием выбранного уровня профиля защиты. Для верхнего, четвертого уровня используются в основном требования ОУД4 и, частично, ОУД5, а также требование ALC_FLR.3 (систематическое устранение недостатков), не входящее ни в один ОУД.

На наш взгляд, рассмотренное семейство профилей может служить примером при построении классификационных схем в Руководящих документах Гостехкомиссии России.

Анализ защищенности

Анализ защищенности - сравнительно новый, но весьма популярный сервис безопасности, помогающий реализовать профилактический подход к обеспечению защиты информационных систем. Суть его весьма проста, но "Общими критериями" он поддержан крайне слабо. Посмотрим, как можно изменить это положение.

Предлагается ввести новый класс функциональных требований - FPA: анализ защищенности. В нем может быть три семейства:

- FPA_HLP: описание уязвимости, выдача рекомендаций по ее устранению;
- FPA_RAD: автообнаружение контролируемых объектов;
- FPA_SPA: анализ характеристик защищенности.

Семейство FPA_HLP может состоять из одного компонента:

- FPA_HLP.1 - описание, выдача (возможно, с заданным уровнем детализации) сведений об уязвимостях, информация о которых

содержится в базе данных системы анализа защищенности (эта база данных аналогична базе правил в компоненте анализа регистрационной информации FAU_SAA.1).

Для семейства FPA_HLP предусмотрено многократное использование (например, для выдачи сведений об атаках средствами активного аудита). Его роль сравнима с ролью комментариев в языках программирования; отсутствие подобного семейства, на наш взгляд, является методологической недоработкой авторов "Общих критериев". Выдача пояснений полезна не только для анализа защищенности, но и для выбора реакции на обнаруженную атаку. (Почему система анализа решила, что атака имеет место? Какие правила при этом сработали? Насколько серьезна обнаруженная атака? На все эти вопросы администратор безопасности должен получить оперативные, информативные ответы.)

Семейство FPA_RAD может располагать одним компонентом:

- FPA_RAD.1 - автообнаружение компонентов анализируемой ИС, описание которых содержится в базе данных системы анализа защищенности.

В семействе FPA_SPA возможно присутствие трех компонентов:

- FPA_SPA.1 - проверка наличия в системе и/или сети сущностей, указанных в базе данных системы анализа защищенности (имеются в виду небезопасные сервисы, такие, например, как TFTP);
- FPA_SPA.2 - анализ характеристик выявленных сущностей (номеров версий, конфигурационных параметров, атрибутов доступа, слабых паролей - и здесь анализируется то, что перечислено в базе данных). Правила для анализа могут быть сложными, охватывающими несколько характеристик;
- FPA_SPA.3 - проверка реакции объекта на выполнение определенных действий (имитация атак, перечисленных в базе).

Надеемся, что предлагаемый класс функциональных требований безопасности поможет в разработке профиля защиты для систем

анализа защищенности.

Профили защиты, разработанные на основе "Общих критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности

Описываются предположения и цели безопасности, функциональные требования и требования доверия, специфичные для конкретных комбинаций и приложений сервисов безопасности. Наиболее подробно рассматриваются частные функциональные требования.

Операционные системы

Операционные системы (ОС) - классический объект оценки по требованиям безопасности еще со времен "Оранжевой книги". Более того, до сих пор остается весьма распространенным мнение о том, что это важнейшее, едва ли не единственное защитное средство. С современных позиций ОС можно рассматривать как комбинацию сервисов идентификации и аутентификации, управления доступом и протоколирования/аудита. Кроме того, операционные системы обеспечивают базовые, инфраструктурные свойства безопасности, в том числе разделение доменов и посредничество при обращениях.

Для операционных систем разработан целый ряд профилей защиты (см. [69], [70], [80], [81], [3], [4]). К этой же группе документов можно отнести руководство по разработке профилей для перспективных коммерческих продуктов ИТ [79], поскольку оно, как и [70], [80], [81], [4]), ориентировано на класс безопасности С2 "Оранжевой книги".

Мы, однако, рассмотрим проект [3] (адаптированный вариант профиля [69]) , в целом соответствующий четвертому классу защищенности по классификации Гостехкомиссии России для средств вычислительной техники, поскольку он более представителен с точки зрения требований безопасности.

Операционные системы, удовлетворяющие проекту ПЗ, должны обеспечивать дискреционное и мандатное управление доступом, мандатное управление целостностью и предоставлять криптографические сервисы . Всем пользователям необходим ассоциированный уровень допуска, определяющий максимальный

уровень чувствительности данных, к которым они могут обращаться (см. выше раздел "Требования к принудительному (мандатному) управлению доступом").

Вероятно, единственная специфическая угроза для рассматриваемого класса ОС заключается в неадекватной классификации данных на основе их меток, что способствует осуществлению несанкционированного доступа к (помеченным) данным. В качестве контрмеры провозглашается специфическая цель безопасности: " Операционная система должна предоставлять возможность расставлять точные метки чувствительности и целостности".

Еще одна очевидная цель состоит в том, что операционная система обязана поддерживать домен для своего собственного выполнения, это защитит ее и принадлежащие ей ресурсы от внешнего вмешательства, искажения или несанкционированного раскрытия.

Для борьбы с маскарадом сервера операционная система должна выделять средства, предотвращающие связь пользователя с некоторой сущностью, выдающей себя за операционную систему, но не являющейся таковой.

Из числа специфических функциональных требований наибольший интерес представляют криптографические компоненты. Остановимся на них подробнее:

- генерация криптографических ключей (FCS_CKM.1). Симметричные криптографические ключи должны генерироваться в соответствии с согласованным с ФАПСИ алгоритмом, реализуемым аппаратным или программным генератором случайных чисел (см. далее компонент FCS_COP_EXP.2) и/или схемой генерации ключей, которая основана на криптографии с открытым ключом, использует программный и/или аппаратный генератор случайных чисел, определенный в FCS_COP_EXP.2, и хэш-функцию по ГОСТ Р 34.11-94. Асимметричные криптографические ключи должны генерироваться, согласуясь с параметрами криптографического преобразования, применяя генератор случайного числа и/или генератор простых чисел и удовлетворяя ГОСТ Р 34.10-2001 в

части генерации простых чисел, ГОСТ Р 34.10-2001 для реализации процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма, ГОСТ 28147-89 для реализации процедур зашифрования и расшифрования данных, а также требованиям из этого проекта ПЗ: FPT_CTST_EXP, FCS_COP_EXP.2 и документации разработчика. Дополнительное требование упомянутого проекта ПЗ состоит в том, что к каждому сгенерированному симметричному ключу должна добавляться имитовставка алгоритма ГОСТ 28147-89 или контрольная сумма другого аттестованного алгоритма (FCS_CKM_EXP.1);

- распределение криптографических ключей (FCS_CKM.2). Согласно проекту профиля [3], ключи должны распределяться (вручную или автоматически) в соответствии с требованиями ФАПСИ и действующих нормативных документов. Не предусматривается автоматическое распределение секретных ключей асимметричных криптосистем;
- доступ к криптографическим ключам (FCS_CKM.3). Ключи должны храниться только в зашифрованном виде в соответствии с требованиями ФАПСИ и действующих нормативных документов (FCS_CKM.3.1). Дополнительное требование: информацию, позволяющую однозначно идентифицировать ключ (FCS_CKM_EXP.3.1), хранить нельзя;
- уничтожение криптографических ключей (FCS_CKM.4). Криптографические ключи должны уничтожаться в соответствии с требованиями ФАПСИ и действующих нормативных документов. Удалять ключи и другие критичные параметры необходимо немедленно, полностью и таким образом, чтобы поверх ключа/критичной области памяти записывались три или более различных шаблонов (FCS_CKM.4.1);
- криптографические операции (FCS_COP.1). Операции зашифрования/расшифрования данных должны выполняться в соответствии с алгоритмом криптографического преобразования по ГОСТ 28147-89 или другим аттестованным алгоритмом, а операции вычисления цифровой подписи - в соответствии с алгоритмом выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма по ГОСТ Р 34.10-2001 или другим аттестованным алгоритмом. Операции хэширования выполняются согласно определенному

ГОСТ Р 34.11-94 или другому аттестованному алгоритму, операции обмена криптографическими ключами - в соответствии с требованиями ФАПСИ и действующих нормативных документов. (FCS_COP.1.1);

- генерация случайных чисел (FCS_COP_EXP.2 - дополнительный компонент, предложенный в данном проекте ПЗ). Генерация случайных чисел должна выполняться множеством независимых аппаратных и/или программных датчиков, выходы которых объединяются с использованием хэш-функции по ГОСТ Р 34.11-94 или другого аттестованного алгоритма (FCS_COP_EXP.2.1). Датчики случайных/псевдослучайных чисел необходимо защитить от нарушения алгоритмов (режимов) их функционирования (FCS_COP_EXP.2.2);
- защита остаточной информации криптографического ключа (FDP_RIP_EXP.2 - дополнительный компонент). Любой ресурс, содержащий критичные параметры безопасности, при освобождении этого ресурса должен быть очищен от всей информации путем перезаписи поверх его содержимого, как определено процедурой уничтожения ключа;
- отделение домена функций безопасности (FPT_SEP_EXP.1 - дополнительный компонент). Поддерживается криптографический домен, отделенный от остальных функций безопасности, защищенный от вмешательства и искажения недоверенными субъектами (FPT_SEP_EXP.1.1);
- тестирование криптографического модуля (FPT_CTST_EXP - дополнительное семейство). Для проверки правильности функционирования криптографического модуля необходимо реализовывать возможность его тестирования путем выполнения набора встроенных тестов при начальном запуске, по запросу администратора по криптографии и периодически (FPT_CTST_EXP.1.1). Тесты должны обеспечивать проверку и документирование статистических характеристик генераторов случайных/псевдослучайных чисел и отображение результатов тестирования (FPT_CTST_EXP.1.2). Предписывается выполнение тестов обнаружения ошибок в ключе при начальном запуске и по запросу администратора по криптографии (FPT_CTST_EXP.1.3), а также немедленное (сразу после генерации ключа) самотестирование каждого участвующего в генерации ключей компонента для верификации его функционирования в

соответствии с FCS_CKM.1.1 и FCS_COP_EXP.2 (FPT_CTST_EXP.1.4). Сгенерированный ключ не должен использоваться, если самотестирование какого-либо компонента завершилось неудачей (FPT_CTST_EXP.1.5);

- доверенный маршрут (FTP_TRP_EXP.1 - дополнительный компонент). Криптографический модуль должен обеспечивать маршрут связи между собой и локальными пользователями, который логически отличим от других маршрутов и предоставляет уверенную идентификацию самого себя (FTP_TRP_EXP.1.1).

Для обслуживания криптографических средств в рассматриваемом проекте ПЗ предусмотрен дополнительный компонент требований доверия безопасности:

- анализ скрытых каналов криптографического модуля (AVA_CCA_EXP.1). Для криптографического модуля разработчику следует провести поиск скрытых каналов утечки критичных параметров безопасности (AVA_CCA_EXP.1.1D) и представить документацию анализа скрытых каналов (AVA_CCA_EXP.1.2D), которая идентифицирует скрытые каналы в криптографическом модуле и содержит оценку их пропускной способности (AVA_CCA_EXP.1.1C). Документация должна содержать описание процедур, используемых для заключения о существовании скрытых каналов в криптографическом модуле, и информацию, необходимую для проведения анализа скрытых каналов (AVA_CCA_EXP.1.2C). Кроме того, в ней описываются все предположения, сделанные в процессе анализа (AVA_CCA_EXP.1.3C), метод, применяемый для оценки пропускной способности канала в случае наиболее опасного сценария (AVA_CCA_EXP.1.4C), и сам наиболее опасный сценарий использования каждого идентифицированного скрытого канала (AVA_CCA_EXP.1.5C). Оценщик обязан подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств (AVA_CCA_EXP.1.1E), а результаты анализа скрытых каналов показывают, что криптографический модуль удовлетворяет функциональным требованиям (AVA_CCA_EXP.1.2E). Наконец, произведя тестирование, он выборочно подтверждает правильность результатов анализа скрытых каналов

(AVA_CCA_EXP.1.3E).

Можно видеть, что в проекте профиля [3] вопросы криптографии изложены весьма пространно, однако смысл всех требований предельно прост: соответствие национальным стандартам (их три). Многократно упоминаемое соответствие требованиям ФАПСИ и действующих нормативных документов - условие туманное, допускающее неоднозначное толкование. (Заметим, что ссылка на требования определенного ведомства - вещь рискованная, так как последнее может прекратить свое существование.) Небесспорно и введение дополнительных, по сравнению с "Общими критериями", требований (функциональных и доверия).

Напомним, что в рассмотренном выше ПЗ для межсетевых экранов [40] криптография используется, помимо шифрования и контроля целостности, также и для аутентификации, однако ссылки на национальный стандарт и привлечения стандартных требований оказалось достаточно. Не ясно, почему следует особо оговаривать отделение криптографического домена или проведение анализа скрытых каналов криптографического модуля - другие функции безопасности не менее критичны и должны обладать не меньшей собственной защищенностью. Целесообразно выделить требования к криптографическим модулям в отдельный документ, как это сделано в федеральном стандарте США FIPS PUB 140-2 [41], а не перегружать ими профиль защиты ОС.

Далее, в рассматриваемом проекте ПЗ предусмотрена возможность удаленного администрирования, но отсутствует упоминание об аутентификации с использованием криптографических методов, а также о защите от подделки и/или воспроизведения аутентификационных данных (компоненты FIA_UAU.3 и FIA_UAU.4 "Общих критериев"). В результате остаются без противодействия стандартные сетевые угрозы.

Еще одна специфическая особенность ОС - возможность управления использованием ресурсов, их распределением между пользователями. Для этого уместно применить механизм квотирования.

- максимальные квоты (FRU_RSA.1). Пользователям должны выделяться квоты долговременной и оперативной памяти, а

также процессорного времени (FRU_RSA.1.1).

Рассмотренный проект профиля защиты для операционных систем показывает, как важно соблюдать определенный уровень формализации изложения, а также единый уровень детализации. Неоднородность ПЗ чревата несистематичностью, завышением или занижением требований. К сожалению, "Общие критерии" не регламентируют этот аспект разработки профилей защиты, заданий по безопасности и функциональных пакетов.

Отдельного рассмотрения заслуживают специфические функциональные требования, присутствующие в проекте [80]. Выше, в разделе "Системы активного аудита", мы отмечали важность требований к интерфейсам и их безопасности. В [80] предложен дополнительный элемент FAU_GEN.1-CSPP.3, предписывающий предоставление прикладного программного интерфейса для добавления собственных данных к общему регистрационному журналу и/или для ведения приложениями собственных журналов.

Для управления экспортом данных пользователя в соответствии с политикой безопасности введен элемент FDP_ETC.1-CSPP.3, предусматривающий выделение отдельного пула выходных каналов (например, путем резервирования номеров TCP-портов), недоступных обычным приложениям.

Поддержка распределенных конфигураций регламентируется целым рядом дополнительных требований, направленных на обеспечение конфиденциальности (FPT_ITC.1.1-CSPP), целостности (FPT_ITI.1.1-CSPP), согласованности (FPT_SYN-CSPP.1.1) критичных данных функций безопасности.

В заключение раздела следует отметить, что в Центре безопасности информации создан проект базового профиля защиты для ОС и разрабатывается профиль защиты ОС в средах, нуждающихся в высокой робастности (защищенности), с тем чтобы иметь завершенное семейство профилей защиты операционных систем.

Системы управления базами данных

Системы управления базами данных (СУБД), как и операционные системы, содержат комбинацию сервисов безопасности, однако, в отличие от ОС, не являются самодостаточными. СУБД используют механизмы и функции ОС. Такая двухуровневость ведет к появлению специфических угроз и требует привлечения соответствующих средств противодействия. Например, базы данных располагаются в файлах или на дисках, управляемых ОС; следовательно, к объектам БД можно обратиться как штатными средствами СУБД, так и с помощью механизмов ОС, получив доступ к файлу или устройству. Подобные возможности должны учитываться в профиле защиты для СУБД.

Дальнейшее изложение основано на проекте ПЗ [5] (его прототип [78] соответствует классу безопасности С2 "Оранжевой книги").

Здесь вводится понятие аутентификационного пакета, который предоставляет для СУБД механизм подтверждения подлинности заявляемого идентификатора пользователя. В рассматриваемом проекте профиля защиты для этого необходим хотя бы один из двух механизмов: внешний (аутентификация средствами ОС) или внутренний (аутентификация средствами СУБД).

Еще одно проявление упомянутой выше двухуровневости - предположение безопасности базовой конфигурации, состоящее в том, что базовая система (операционная система, и/или сетевые сервисы безопасности, и/или специальное программное обеспечение) установлены, сконфигурированы и управляются безопасным образом. Аналогичную направленность имеют цели безопасности для среды, предусматривающие, что базовая система должна обеспечить механизмы управления доступом, которые позволят защитить от несанкционированного доступа все связанные с СУБД файлы; кроме того, ОС предоставит средства для изоляции функций безопасности и защиты процессов СУБД.

Отметим, что в распределенной среде управление доступом и изоляция могут поддерживаться не только средствами базовой ОС, но и архитектурно, путем разнесения компонентов СУБД по узлам сети и использования межсетевых экранов. Эта возможность в проекте [5] не рассматривается.

Переходя к функциональным требованиям безопасности, укажем на

важность требований согласованности данных между функциями безопасности (FPT_TDC), а также согласованности данных функций безопасности при дублировании в пределах распределенного объекта оценки (FPT_TRC). Согласованность достигается с помощью некоторой формы обработки распределенных транзакций или путем обновления дублируемых данных с применением какого-либо протокола синхронизации. К сожалению, требования этих семейств в проекте [5] не представлены, равно как и требования распределенности хранения и обработки для повышения устойчивости к отказам. Конечно, в "Оранжевой книге" ничего подобного не было, однако в наше время, как показывает профиль [45], следование определенным архитектурным принципам является обязательным.

Для защиты от атак на доступность в рассматриваемом проекте предусмотрены реализация квот, выделяемых пользователям (FRU_RSA.1), а также базовые ограничения на параллельные сеансы (FTA_MCS.1).

В целом, на наш взгляд, проект [5] нуждается в доработке. Необходимо учесть специфику современных СУБД, в частности, требования обеспечения динамической целостности данных, реализуемые механизмом транзакций. Требования безопасного восстановления носят слишком общий характер. Защита от стандартных угроз, существующих в сетевой среде, целиком переложена на базовую систему. Не учтены специфические для СУБД угрозы, описанные, например, в главе "Информационная безопасность систем управления базами данных" книги [83].

Виртуальные частные сети

Туннелирование и шифрование (наряду с необходимой криптографической инфраструктурой) на выделенных шлюзах в комбинации с экранированием на маршрутизаторах поставщиков сетевых услуг (для разделения пространств "своих" и "чужих" сетевых адресов в духе виртуальных локальных сетей) позволяют реализовать такое важное в нынешних условиях защитное средство, как виртуальные частные сети. Подобные сети, наложенные обычно поверх Internet, существенно дешевле и гораздо безопаснее, чем действительно собственные сети организации, построенные на выделенных каналах.

Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об уязвимости и соответствующим образом обеспечивать защиту. Современные протоколы, поддерживающие спецификации IPsec (см., например, [9]), позволяют сделать это.

На концах туннелей, реализующих виртуальные частные сети, целесообразно установить межсетевые экраны, обслуживающие подключение организаций к внешним сетям. В таком случае туннелирование и шифрование становятся дополнительными преобразованиями, выполняемыми в процессе фильтрации потоков данных наряду с трансляцией адресов. Помимо корпоративных межсетевых экранов, в роли конечных устройств могут выступать мобильные компьютеры сотрудников (точнее, их персональные МЭ). Далее соответствующие узлы сети мы будем называть опорными.

В качестве основы последующего изложения выбран проект профиля защиты [29], где объект оценки - совокупность опорных узлов. Требования к перспективным средствам аналогичного назначения представлены в документе [76].

Поскольку реализация виртуальных частных сетей в значительной степени основывается на криптографических механизмах, в число специфических угроз входят применение злоумышленником методов и средств криптографического анализа, а также компрометация криптографических ключей. Упомянем и угрозы доступности каналов связи.

Для нейтрализации угроз должны быть выполнены функциональные требования безопасности, относящиеся к криптографии. Необходимо осуществление контроля доступа к криптографическим ключам (FCS_CKM.3.1), шифрование (FCS_COP.1.1) и применение механизмов контроля целостности (FCS_COP.1.1) информации, передаваемой в рамках доверенного канала.

В виртуальной частной сети управление информационными потоками ограничивается (FDP_IFC.1.1). Вообще говоря, через опорные узлы проходят не только потоки данных, предназначенные для виртуальной частной сети, но и данные для внешних адресатов. Эти потоки должны различаться и обрабатываться по-разному (например, первые

необходимо шифровать, а вторые - нет). По сути, должно быть реализовано межсетевое экранирование, только одна из сетей является виртуальной.

От виртуальных частных сетей требуется реализация некоторых аспектов приватности. Они не должны допустить, чтобы извне можно было определить подлинное имя пользователя, связанного с передаваемой в рамках доверенного канала информацией (FPR_ANO.1.1). В то же время, администратору необходимо предоставить возможность наблюдения за использованием ресурсов и функционированием процессов (FPR_UNO.4.1).

Опорные узлы должны обладать определенной отказоустойчивостью, обеспечивая возврат к безопасному состоянию, генерацию записи журнала аудита, сигнализацию администратору, когда происходит сбой в системе электропитания или нарушение безопасности (FRU_FLT.1.1).

Таковы специфические функциональные требования безопасности для виртуальных частных сетей. В "Общих критериях" в явном виде не представлены требования к туннелированию ; нет их и в рассмотренном проекте. Возможно, туннелирование трактуется лишь как механизм обеспечения анонимности.

Виртуальные локальные сети

Под виртуальной локальной сетью в проекте профиля защиты [26] понимается такое логическое объединение узлов локальной сети, при котором обмен данными на канальном уровне эталонной семиуровневой модели возможен только между этими узлами.

Использование виртуальных локальных сетей позволяет:

- повысить производительность (и доступность) сети за счет локализации потоков данных ;
- обеспечить защиту передаваемых данных посредством логического разделения среды передачи ;
- реализовать управление доступом пользователей к сетевым ресурсам.

Разграничение потоков данных обеспечивается путем фильтрации кадров данных. Таким образом, объект оценки оказывается межсетевым экраном канального уровня.

В проекте [26] рассматриваются два способа построения виртуальных локальных сетей:

- группировка портов объекта оценки. В этом случае каждый порт поддерживает только одну виртуальную сеть;
- использование специальной метрики для определения принадлежности к конкретной виртуальной локальной сети.

Впрочем, предлагаемые в проекте требования безопасности в равной степени применимы к обоим вариантам.

От рассмотренных ранее межсетевых экранов объект оценки отличается ограниченностью ресурсов и меньшей функциональностью. В частности, вся работа с регистрационной информацией (начиная с хранения) возлагается на среду, точнее, на так называемое средство анализа событий. Это освобождает объект оценки от ряда стандартных требований протоколирования и аудита, но ведет к необходимости организации доверенного канала.

Смарт-карты

Профиль защиты для смарт-карт [77] интересен необычностью объекта оценки. Он позволяет оценить гибкость и разнообразие требований "Общих критериев".

Эта необычность заключается в следующем:

- минимум аппаратных ресурсов (интегральная схема, включающая процессор; оперативная и постоянная память относительно небольшого объема; порты ввода/вывода) в сочетании с программным обеспечением ограниченной функциональности (в профиле [77] рассматривается базовое ПО);
- принадлежность неконтролируемой среде, когда карта может оказаться в руках злоумышленника, располагающего специальным

оборудованием.

В защите (обеспечении конфиденциальности и целостности) нуждаются хранящиеся на карте пользовательские данные, программное обеспечение (прикладное и базовое), а также аппаратные компоненты.

Отметим, что приемное устройство, снабжающее смарт-карту электропитанием и связью с внешним миром, не входит в объект оценки.

Учитывая ограниченность ресурсов и потенциально враждебную среду, сервисы безопасности для смарт-карт должны быть отобраны и реализованы с особой тщательностью.

Сформулируем предположения безопасности для среды:

- после установления доверенного канала с приемным устройством последнее предполагается достаточно безопасным, чтобы поддерживать доверенные коммуникации;
- предполагается, что обеспечена конфиденциальность и целостность информации, хранящейся вне карты и существенной для ее безопасности. Имеются в виду как пользовательские данные, так и криптографические ключи, загружаемые приложения и т.п.

С большинством возможных угроз смарт-карта должна справляться самостоятельно, без помощи среды. Выделим специфические (а также специфически реализуемые и отражаемые) угрозы:

- осуществление доступа к смарт-карте с помощью специального оборудования, когда преследуется цель выяснить определенные аппаратные и/или программные характеристики (применяемые криптографические механизмы, используемые ключи, хранимые данные и программы и т.п.). Не исключены попытки изменить аппаратно-программную конфигурацию и/или данные, а также перевести смарт-карту в небезопасное состояние, поместив ее в стрессовые условия (например, температурные или электромагнитные);
- логические атаки: отслеживание зависимостей между входными

данными операций, выполняемых смарт-картой, и результатами; попытки перевести карту в небезопасное состояние искусственно инициированным сбросом или загрузить вредоносные программы; использование некорректных входных данных; воспроизведение данных аутентификации; переборные атаки (на криптографические компоненты). К этой же категории угроз можно отнести попытки организовать нештатное взаимодействие прикладных функций и выполнить действия (например, отладочные), предусмотренные для особых этапов жизненного цикла смарт-карты. Одновременное проведение нескольких атак;

- несанкционированный доступ: попытки злоупотребления полномочиями при доступе к пользовательским данным или данным функций безопасности, а также использования новой, не до конца оформленной смарт-карты ;
- попытки выявления и анализа утечек информации во время нормальной работы смарт-карты, совместный анализ результатов многих наблюдений.
- попытки изготовления копий (клонирование) компонентов смарт-карты для детального изучения их поведения.

Специфической угрозой для среды является замена интегральной схемы, установленной в смарт-карте, с целью несанкционированного доступа к данным пользователя или функций безопасности.

Из специфических положений политики безопасности прежде всего отметим наличие уникальных идентификационных данных для каждого объекта оценки, а также (как ни странно) накопление регистрационной информации, которое необходимо производить, несмотря на ограниченность ресурсов. Аудит может выполняться во время сервисного обслуживания смарт-карты.

Цели безопасности формулируются таким образом, чтобы обеспечить нейтрализацию угроз и выполнить положения политики безопасности: интегральная схема должна работать в любых, в том числе стрессовых, условиях; осуществляется защита от многократного использования ресурсов при переборных атаках; изучение передаваемых данных не должно давать дополнительной информации по сравнению с анализом содержимого памяти; нормальное (безопасное) состояние устанавливается сразу после подачи питания или сброса; при замене

интегральной схемы на карте обязательно должны оставаться следы и т.п.

Перейдем к рассмотрению специфических функциональных требований:

- автоматическая реакция аудита безопасности (FAU_ARP) при обнаружении возможного нарушения безопасности. Предписываются минимальные необратимые последствия реакции. Подчеркнем, что в силу специфики объекта оценки оперативное информирование администратора безопасности в общем случае невозможно; с опасностью приходится бороться самостоятельно;
- генерация списка регистрационных данных (FAU_LST - дополнительное семейство). На интегральной схеме, устанавливаемой в смарт-карте, нет часов; время указывает только приемное устройство, которое не считается доверенным. Следовательно, события можно лишь упорядочить по мере их появления, но с ними нельзя ассоциировать дату и время. В регистрационную информацию должны включаться идентификационные данные аппаратных и программных компонентов;
- противодействие физическому нападению (FPT_PHP.3). Функции безопасности обязаны противодействовать попыткам эксплуатации в стрессовых условиях, отслеживанию информации, другим физическим атакам, автоматически реагируя таким образом, чтобы предотвратить нарушение политики безопасности (FPT_PHP.3.1);
- надежное восстановление (FPT_RCV). Автоматическое восстановление без недопустимой потери (FPT_RCV.3), восстановление функции (FPT_RCV.4).

Для требований доверия безопасности в [77] используется усиленный оценочный уровень 4. Усиление обеспечивают компоненты AVA_VLA.3 (систематический поиск уязвимостей, обеспечение стойкости к нападениям, выполняемым нарушителем с умеренным потенциалом) и ADV_INT.1 (модульность).

Важным достоинством работы [77] является выделение двух

функциональных пакетов: для интегральной схемы и базового ПО. Эти части могут разрабатываться независимыми производителями, поэтому целесообразно, чтобы они проводили такую же независимую сертификацию, а интегратор (производитель смарт-карт) выбирал поставщиков и осуществлял интегральную сертификацию. В части функциональных требований пакет для базового ПО аналогичен рассмотренному профилю ; к аппаратуре предъявляется меньшее число требований. Например, в функциональном пакете для интегральной схемы отсутствуют компоненты FAU_SAA.1 (анализ потенциального нарушения) и FPT_RPL.1 (обнаружение повторного использования), что представляется вполне естественным.

Некоторые выводы

"Общие критерии" - исключительно мощное, гибкое средство разработки требований безопасности для изделий информационных технологий. В частности, могут быть выделены общие требования к сервисам безопасности, а также учтена специфика конкретных сервисов, фигурирующих по отдельности или в различных комбинациях.

В то же время, сама гибкость "Общих критериев" - источник сложных проблем, в первую очередь относящихся к методологии разработки профилей защиты. Можно провести аналогию с языками и технологией программирования, когда владение передовым языком программирования вовсе не означает умения проектировать и создавать большие программные комплексы.

Вопросы технологии "программирования" профилей защиты носят разнообразный характер и затрагивают все этапы жизненного цикла ПЗ. Какой подход выбрать при разработке ПЗ: "снизу вверх" или "сверху вниз"? Сами "Общие критерии", имеющие библиотечную (не объектную) структуру, подталкивают к применению подхода "снизу вверх", от отдельных требований к общей функциональности. Однако, как показывает опыт разработчиков профиля [45] (равно как и технология программирования), наиболее предпочтителен подход "сверху вниз", от требуемой функциональности объекта оценки к базовым механизмам безопасности.

Еще один технологический аспект - модульность ПЗ. Выделение функциональных пакетов для составных частей объекта оценки, реализованное в [77], дает больше свободы и разработчикам, и интеграторам, способствует раннему выявлению и устранению проблем, облегчает деятельность оценщиков.

Следующий вопрос касается технологии сопровождения множества профилей защиты. Как соотносить между собой отдельные ПЗ? Как группировать их, выстраивать иерархии и т.п.? Пока зарегистрированных профилей относительно немного (что само по себе является проблемой, но, можно надеяться, временной), и все-таки очевидно, что их число будет расти, они станут поступать из различных источников, из разных стран, так что поддержание международного статуса "Общих критериев", несомненно, потребует специальных усилий, которые целесообразно планировать заранее (см. соглашение "О признании сертификатов по Общим критериям в области безопасности информационных технологий").

Очень серьезная проблема - неполнота функциональных требований "Общих критериев". Как показывают рассмотренные профили, авторам ПЗ приходится добавлять собственные нестандартные классы, семейства, компоненты и элементы, что ведет к несопоставимости разрабатываемых профилей, к усложнению процедур сертификации и взаимного признания сертификатов.

Принципиальный недостаток - отсутствие в "Общих критериях" архитектурных и технологических требований. Такие свойства, как распределенность архитектуры, следование подходу менеджер/агент и т.п., необходимы для успешной реализации функций объекта оценки, они критичны для его безопасности.

Таким образом, проведенный анализ позволяет наметить следующие направления дальнейших исследований и разработок:

- создание новых профилей защиты, охватывающих все сервисы безопасности;
- разработка методологии и соответствующих инструментальных средств создания ПЗ;
- разработка дисциплины и инструментальных средств для

использования множества профилей защиты ;

- развитие "Общих критериев", разработка новых стандартных требований безопасности, как "точечных", так и концептуальных, архитектурных;
- разработка дисциплины введения новых нестандартных требований с минимизацией проблем несопоставимости получающихся профилей защиты.

Для решения сформулированных проблем необходимо взаимодействие специалистов, независимо от их национальной и, тем более, ведомственной принадлежности.

Рекомендации семейства X.500

Данные рекомендации очень важны в концептуальном плане. Служба директорий, формат сертификатов открытых ключей и атрибутов - это базовые элементы инфраструктуры программно-технического уровня информационной безопасности.

Основные понятия и идеи рекомендаций семейства X.500

Рекомендации семейства X.500 описывают службу директорий. Среди возможностей, предоставляемых этой службой, обычно выделяют дружественное именование (обращение к объектам по именам, удобным с точки зрения человека) и отображение имен в адреса (динамическое связывание объекта и его расположения - необходимое условие поддержки "самоконфигурируемости" сетевых систем).

Основные понятия службы директорий зафиксированы в рекомендациях X.501 " Служба директорий: модели" [47] и X.511 " Служба директорий: абстрактное определение сервиса" [49].

Множество систем, обеспечивающих функционирование службы директорий, вместе с содержащейся в них информацией можно представлять как единое целое - Директорию с большой буквы.

Информация, доступ к которой возможен посредством Директории, называется Информационной Базой Директории . Она обычно используется для облегчения взаимодействия таких сущностей, как объекты прикладного уровня, люди, списки рассылки и т.д., а также для получения сведений о них.

Предполагается, что Информационная База имеет древовидную структуру, называемую Информационным Деревом Директории . Вершины этого дерева, отличные от корня, составляют элементы Директории, в которых хранится информация об объектах .

У каждого элемента есть однозначно идентифицирующее его различительное имя. В пределах поддеревьев Информационного Дерева могут использоваться относительные различительные имена.

Природа объектов, информация о которых хранится в Директории, произвольна. Единственное требование к ним состоит в идентифицируемости (возможности именования).

Объекты объединяются в классы. Каждый объект должен принадлежать по крайней мере одному классу.

Элементы Директории могут быть составными, объединять подэлементы, содержащие информацию об отдельных аспектах объектов.

Каждый элемент состоит из атрибутов, имеющих тип и одно или несколько значений. Набор атрибутов зависит от класса объекта.

Некоторые из концевых узлов (листьев) Информационного Дерева могут представлять собой синонимы, содержащие альтернативное имя и указатель на элемент с информацией об объекте.

Служба директорий предоставляет две группы операций:

- опрос;
- модификацию.

В число операций опроса входят:

- чтение значений атрибутов элемента Директории ;
- сравнение значения атрибута элемента Директории с заданной величиной (полезно, например, для проверки пароля без предоставления доступа к хранимому паролю);
- выдача списка (перечисление) непосредственных преемников заданного узла Информационного Дерева ;
- поиск и чтение элементов, удовлетворяющих заданным фильтрам (условиям), в заданных частях Информационного Дерева ;
- отказ от незавершенной операции опроса (например, если она выполняется слишком долго).

В группу операций модификации входят:

- добавление нового (концевого) узла Информационного Дерева ;

- удаление концевого узла Информационного Дерева ;
- модификация элемента Директории с возможным добавлением и/или удалением атрибутов и их значений;
- модификация относительного различительного имени элемента или перемещение узла Информационного Дерева к другому предшественнику.

Рекомендации X.501 описывают три возможные схемы управления доступом к Директории: базовую, упрощенную и основанную на правилах; последняя может реализовывать принудительное (мандатное) управление доступом с использованием меток безопасности. Решения о предоставлении доступа принимаются с учетом существующей политики безопасности.

Разумеется, предусмотрена аутентификация системных агентов и пользователей, а также источников данных Директории.

Таковы основные понятия и идеи службы директорий, зафиксированные в семействе рекомендаций X.500 и необходимые нам для последующего изложения.

Каркас сертификатов открытых ключей

Мы приступаем к изучению четвертой редакции рекомендаций X.509 [48], которая регламентирует следующие аспекты:

- сертификаты открытых ключей ;
- сертификаты атрибутов ;
- сервисы аутентификации.

Идейной основой рекомендаций X.509 являются сертификаты открытых ключей, обслуживающие такие грани информационной безопасности, как конфиденциальность и целостность, и такие сервисы, как аутентификация и неотказуемость.

В курсе "Основы информационной безопасности" [91] приведены необходимые сведения о криптографии с открытыми ключами и механизме электронной цифровой подписи (ЭЦП); далее

предполагается, что они уже известны.

Сертификат открытого ключа - это структура данных, обеспечивающая ассоциирование открытого ключа и его владельца. Надежность ассоциации, подлинность сертификата подтверждаются подписью удостоверяющего центра (УЦ).

Сертификаты имеют конечный срок годности. Поддерживать актуальность информации об их статусе помогают списки отзыва, подписываемые удостоверяющими центрами и содержащими перечни сертификатов, переставших быть годными. Последнее может случиться как в результате естественного окончания срока, так и досрочно, например, из-за компрометации секретного ключа владельца.

Формат сертификата описан в курсе [91]. В простейшем случае он выглядит так:

$$CA\ \langle\langle A \rangle\rangle = CA\ \{V, SN, AI, CA, A, A_p, TA\}$$

Здесь:

- A - имя владельца сертификата;
- CA - имя удостоверяющего центра ;
- $CA\ \langle\langle A \rangle\rangle$ - сертификат, выданный A центром CA ;
- $CA\ \{I\}$ - данные I, снабженные подписью CA ;
- V - версия сертификата (в настоящее время - версия 3);
- SN - порядковый номер сертификата;
- AI - идентификатор алгоритма, использованного при подписании сертификата;
- A_p - информация об открытом ключе A ;
- TA - даты начала и конца срока годности сертификата.

Отметим, что в общем случае формат может быть существенно сложнее. С помощью механизма расширений его можно приспособить для нужд различных приложений и сообществ пользователей. В X.509 предусмотрены полезные расширения, носящие универсальный характер.

Каждое расширение включает имя, флаг критичности и значение. Если

при обработке (проверке) сертификата встречается неизвестное расширение с флагом критичности FALSE, оно может быть проигнорировано; если же у подобного расширения флаг равен TRUE, сертификат приходится считать некорректным.

Сертификаты открытых ключей подразделяются на два основных вида:

- сертификаты оконечных сущностей;
- сертификаты удостоверяющих центров.

Оконечные сущности не имеют права выпускать сертификаты. Удостоверяющие центры ведают выпуском и аннулированием сертификатов, которые относятся к одному из двух классов:

- "самовыпущенные" сертификаты (изготовленные для себя самим удостоверяющим центром). Они полезны, например, при смене ключей УЦ, чтобы обеспечить доверие новым ключам на основании доверия старым. Важным подклассом данного класса являются "самоподписанные" сертификаты, в которых секретный ключ, использованный для генерации ЭЦП, соответствует заверяемому открытому ключу. Таким способом УЦ может афишировать свой открытый ключ или иную информацию о собственном функционировании;
- кросс-сертификаты (выдаются одним УЦ другому). Они применяются и в иерархической структуре для авторизации нижестоящего УЦ вышестоящим, и в произвольной структуре "распределенного доверия" как факт признания одним УЦ существования другого.

Рассмотрим процесс получения и проверки пользователем A открытого ключа пользователя B. Элемент Директории, представляющий A, содержит один или несколько сертификатов открытых ключей A, заверенных удостоверяющим центром, который мы обозначим CA (A) (а сертификат A - как CA (A) <<A>>) и которому, разумеется, соответствует свой узел в Информационном Дереве. Предполагается, что пользователь доверяет своему УЦ, поэтому, если существует сертификат CA (A) <<B>>, процесс выяснения открытого ключа B можно считать завершенным. В противном случае приходится строить

так называемый сертификационный маршрут от A к B (обозначается A -> B), начинающийся сертификатом CA (A) <<X1>>, который CA (A) выдал некоторому другому УЦ, X_1, ставшему вследствие этого доверенным для A. Маршрут продолжается сертификатом вида X_1 <<X_2>>, содержит промежуточные звенья вида X_i <<X_{i+1}>> и завершается сертификатом X_n <<B>>.

Элемент Директории, соответствующий удостоверяющему центру, содержит сертификаты двух типов: прямые (сгенерированные данным УЦ для других) и обратные (выданные данному УЦ другими). Если, кроме того, удостоверяющие центры образуют иерархию, соответствующую Информационному Дереву, то сертификационный маршрут можно построить без привлечения дополнительной информации, только на основе различительных имен A и B. Действительно, с помощью обратных сертификатов выполняется подъем от CA (A) до корня поддерева, общего для A и B, а затем, с помощью прямых сертификатов осуществляется спуск до CA (B). В рассмотренном выше процессе A - пользователь сертификата, B - его владелец (субъект), CA (B) - удостоверяющий центр. Все три стороны несут друг перед другом определенные обязательства и, в свою очередь, пользуются предоставляемыми гарантиями. Обязательства и гарантии могут быть зафиксированы в политике сертификата, ссылка на которую хранится в одном из полей расширений. Обычно политика - это общепринятый текст, но в ней могут присутствовать и формальные условия, допускающие автоматическую проверку.

При построении и использовании сертификационного маршрута проверяется согласованность политик, присутствующих в кросс-сертификатах. Еще один пример употребления данного поля расширения - наложение и проверка ограничений на длину сертификационного маршрута (вообще говоря, чем длиннее маршрут, тем меньше доверия он вызывает).

Другая группа дополнительных полей сертификатов обслуживает способы и срок действия ключей. Для шифрования и цифровой подписи применяют разные ключи; следовательно, у одного субъекта может быть несколько пар ключей и, соответственно, несколько сертификатов. Чтобы выбрать среди них нужный, необходимо иметь возможность

выяснить назначение представленного в сертификате открытого ключа. Аналогично, может потребоваться знание срока годности секретного ключа, посредством которого формируют ЭЦП, поскольку этот срок обычно меньше, чем у открытого ключа, проверяющего подпись.

Значительная часть рекомендаций X.509 посвящена спискам отзыва сертификатов; мы, однако, не будем останавливаться на этом сугубо техническом вопросе.

Каркас сертификатов атрибутов

Вероятно, развитие механизма расширений натолкнуло авторов рекомендаций X.509 на мысль о том, что в заверенных сертификатах можно хранить не только открытые ключи, но и произвольные атрибуты субъектов - держателей (владельцев) сертификатов.

Сертификат атрибутов - это структура данных, снабженная цифровой подписью соответствующего удостоверяющего центра и связывающая значения некоторых атрибутов с идентификационной информацией держателя сертификата.

Вообще говоря, сертификаты атрибутов имеют универсальный характер, но в рекомендациях X.509 внимание акцентируется на их применении в качестве основы инфраструктуры управления привилегиями.

У каркасов сертификатов открытых ключей и сертификатов атрибутов немало общего. Это и система удостоверяющих центров, и списки отзыва, и многое другое. Мы, однако, сосредоточимся на специфике управления привилегиями.

Отметим в первую очередь, что жизненные циклы открытых ключей и привилегий устроены по-разному, имеют разную длительность. Привилегии могут делегироваться вспомогательным сущностям на короткие промежутки времени (порядка минуты). Для управления привилегиями используются свои понятия и механизмы, например роли. Следовательно, хотя с синтаксической точки зрения для цели управления привилегиями можно использовать снабженные соответствующими расширениями сертификаты открытых ключей, идейная и практическая сторона вопроса подразумевает разделение

каркасов открытых ключей и управления привилегиями, что и сделано в рекомендациях X.509.

В контексте управления привилегиями удостоверяющий центр называется центром авторизации. Выделяется главный центр авторизации, который может делегировать другим центрам права наделения привилегиями и их дальнейшего делегирования.

На протяжении маршрута делегирования должно действовать правило доминирования: промежуточный центр авторизации не вправе делегировать больше привилегий, чем сам имеет (для каждой привилегии должно быть определено, что значит "не больше").

Вообще говоря, известны две схемы выделения и проверки привилегий:

- удостоверяющий центр по собственной инициативе наделяет некоторую сущность привилегиями, создав сертификат атрибутов и поместив его в Директорию с предоставлением свободного доступа. В дальнейшем верификатору привилегий разрешается использовать этот сертификат при принятии решения о предоставлении определенного вида доступа. Перечисленные действия могут происходить без ведома и участия субъекта - держателя сертификата;
- субъект запрашивает центр авторизации на предмет получения определенной привилегии. При положительном решении созданный сертификат атрибутов возвращается держателю и явным образом предъявляется последним при доступе к защищенным ресурсам.

Независимо от принятой схемы выделяются три основных понятия инфраструктуры управления привилегиями:

- объект (точнее, метод объекта), к которому осуществляется доступ и который может быть снабжен такими атрибутами, как метка безопасности.
- предъявитель привилегий ;
- верификатор привилегий, принимающий решения (с учетом действующей политики безопасности и существующего окружения) о достаточности предъявленных привилегий для

предоставления доступа.

Верификатор привилегий - это какая-либо экранирующая сущность, логически располагающаяся между вызывающим и вызываемым методами объектов ; рекомендации X.509 не налагают ограничений на правила экранирования.

Ролевое управление доступом может быть реализовано за счет введения дополнительного уровня косвенности, а также трактовки допустимых ролей как атрибутов субъектов и ассоциирования привилегий с ролями путем выпуска соответствующих сертификатов.

Отметим, что каркас сертификатов атрибутов может быть использован не только для управления доступом, но и в контексте обеспечения неотказуемости. При этом предъявитель привилегий выступает в качестве субъекта свидетельства, верификатор привилегий оказывается пользователем свидетельства, а метод объекта трактуется как целевая сущность.

Можно видеть, что каркас сертификатов атрибутов обладает достаточной гибкостью и выразительной силой, чтобы служить основой инфраструктуры управления привилегиями, поддерживать контроль доступа и неотказуемость.

Простая и сильная аутентификация

Каркасы сертификатов открытых ключей и атрибутов - основа целого ряда сервисов безопасности, в число которых входят аутентификация, контроль целостности, управление доступом. Они могут использоваться как самой Директорией, так и произвольными приложениями. В этом разделе мы рассмотрим простую и сильную аутентификации, включенные в рекомендации X.509.

Простая аутентификация предназначена только для локального использования. Данные для нее могут вырабатываться и передаваться тремя способами:

- имя и пароль пользователя передаются в открытом виде;
- имя, пароль, случайное число и, возможно, временной штамп

(метка) подвергаются воздействию односторонней функции, результат которой передается получателю для проверки;

- к описанному выше результату добавляется случайное число и/или временной штамп и еще раз применяется односторонняя функция (возможно, та же самая).

Рассмотрим более подробно реализацию разновидности 2 простой аутентификации. Пользователь A сначала генерирует токен безопасности PT1:

PT1 = h1 (t1A, r1A, A, passwdA)

Токен PT1 используется для создания аутентификационного токена AT1:

AT1 = t1A, r1A, A, PT1

(т. е. токен AT1 состоит из четырех компонентов). Пользователь A пересылает пользователю B токен AT1. Цель B - своими средствами создать аналог токена безопасности PT1 (реконструировать PT1) и сравнить его с оригиналом. Он запрашивает у службы директорий или извлекает самостоятельно локальную копию пароля passwdA (обозначим ее passwdA-B) и реконструирует PT1:

PT1-B = h1 (t1A, r1A, A, passwdA-B)

Если PT1 и PT1-B совпадут, подлинность пользователя A считается установленной.

Сильная аутентификация основана на применении асимметричных методов шифрования, пригодных для генерации электронной подписи. Подлинность пользователя A считается установленной, если он продемонстрирует владение секретным ключом, ассоциированным с хранящимся в сертификате на имя A открытым ключом.

Рекомендации X.509 описывают три возможные процедуры сильной аутентификации:

- односторонний обмен. От пользователя A пользователю B

передается один токен. При этом подтверждается подлинность A и B, а также то, что токен сгенерирован A, предназначен B, не был изменен и является "оригинальным" (т. е. не посылается повторно);

- двусторонний обмен. Дополнительно от B к A направляется ответ, допускающий проверку того, что он был сгенерирован B, предназначен A, не был изменен и является "оригинальным";
- трехсторонний обмен. От A к B передается еще один токен. Обеспечивает те же свойства, что и двусторонний, без использования временных штампов.

Предполагается, что независимо от выбранной процедуры и до выполнения обменов пользователь A выясняет открытый ключ B и обратный сертификационный маршрут B -> A.

Рассмотрим более подробно процедуру одностороннего обмена.

В качестве первого шага пользователь A генерирует "уникальное" число rA, предназначенное для защиты от воспроизведения и подделки аутентификационного токена.

После этого A направляет B сообщение следующей структуры:

B -> A, A {tA, rA, B}

где tA - временной штамп, в общем случае представляющий собой пару (время генерации токена и срок его годности). (Напомним, что конструкция вида A {I} обозначает информацию I, подписанную открытым ключом A.)

Получив это сообщение, B предпринимает следующие действия:

- по обратному сертификационному пути B -> A выясняет открытый ключ A (A_p), попутно проверяя статус сертификата A ;
- проверяет подпись и, тем самым, целостность присланной информации;
- проверяет, что в качестве получателя указан B ;
- удостоверяется, что временной штамп "свежий", а число rA ранее

не использовалось.

Двусторонний и трехсторонний обмены являются довольно очевидным развитием одностороннего.

На этом мы завершаем рассмотрение рекомендаций семейства X.500.

Спецификации Internet-сообщества IPsec

Данные спецификации имеют фундаментальное значение, описывая полный набор средств обеспечения конфиденциальности и целостности на сетевом уровне.

Архитектура средств безопасности IP-уровня

В курсе "Основы информационной безопасности" [91] указывалось, что практически все механизмы сетевой безопасности могут быть реализованы на третьем уровне эталонной модели ISO/OSI. Более того, IP-уровень можно считать оптимальным для размещения защитных средств, поскольку при этом достигается удачный компромисс между защищенностью, эффективностью функционирования и прозрачностью для приложений.

Стандартизованными механизмами IP-безопасности могут (и должны)пользоваться протоколы более высоких уровней и, в частности, управляющие протоколы, протоколы конфигурирования и маршрутизации.

Средства безопасности для IP описываются семейством спецификаций IPsec, разработанных рабочей группой IP Security.

Протоколы IPsec обеспечивают управление доступом, целостность вне соединения, аутентификацию источника данных, защиту от воспроизведения, конфиденциальность и частичную защиту от анализа трафика.

Архитектура средств безопасности для IP-уровня специфицирована в документе [60]. Ее основные составляющие представлены на рис. 9.1. Это прежде всего протоколы обеспечения аутентичности (протокол аутентифицирующего заголовка - Authentication Header, AH) и конфиденциальности (протокол инкапсулирующей защиты содержимого - Encapsulating Security payload, ESp), а также механизмы управления криптографическими ключами. На более низком архитектурном уровне располагаются конкретные алгоритмы шифрования, контроля целостности и аутентичности. Наконец, роль фундамента выполняет так называемый домен интерпретации (Domain

of Interpretation, DOI), являющийся, по сути, базой данных, хранящей сведения об алгоритмах, их параметрах, протокольных идентификаторах и т.п.

Рис. 9.1. Основные элементы архитектуры средств безопасности IP-уровня

Деление на уровни важно для всех аспектов информационных технологий. Там же, где участвует еще и криптография, важность возрастает вдвойне, поскольку приходится считаться не только с чисто техническими факторами, но и с особенностями законодательства различных стран, с ограничениями на экспорт и/или импорт криптосредств (см. курс "Основы информационной безопасности" [91]).

Протоколы обеспечения аутентичности и конфиденциальности в IPsec не зависят от конкретных криптографических алгоритмов. (Более того, само деление на аутентичность и конфиденциальность предоставляет и разработчикам, и пользователям дополнительную степень свободы в ситуации, когда к криптографическим относят только шифровальные средства.) В каждой стране могут применяться свои алгоритмы, соответствующие национальным стандартам, но для этого, как минимум, нужно позаботиться об их регистрации в домене интерпретации.

Алгоритмическая независимость протоколов, к сожалению, имеет и оборотную сторону, состоящую в необходимости предварительного согласования набора применяемых алгоритмов и их параметров, поддерживаемых общающимися сторонами. Иными словами, стороны

должны выработать общий контекст безопасности (Security Association, SA) и затем использовать такие его элементы, как алгоритмы и их ключи. За формирование контекстов безопасности в IPsec отвечает особое семейство протоколов, которое будет рассмотрено в последующих разделах.

Протоколы обеспечения аутентичности и конфиденциальности могут применяться в двух режимах: транспортном и туннельном. В первом случае защищается только содержимое пакетов и, быть может, некоторые поля заголовков. Как правило, транспортный режим используется хостами. В туннельном режиме защищается весь пакет - он инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуют на специально выделенных защитных шлюзах (в роли которых могут выступать маршрутизаторы или межсетевые экраны, см. курс "Основы информационной безопасности" [91]).

В последующих разделах мы подробно рассмотрим основные элементы IPsec.

Контексты безопасности и управление ключами

Формирование контекстов безопасности в IPsec разделено на две фазы. Сначала создается управляющий контекст, назначение которого - предоставить доверенный канал (в терминологии "Общих критериев", см., например, [84]), т. е. аутентифицированный, защищенный канал для выработки (в рамках второй фазы) протокольных контекстов и, в частности, для формирования криптографических ключей, используемых протоколами AH и ESp.

В принципе, для функционирования механизмов IPsec необходимы только протокольные контексты ; управляющий играет вспомогательную роль. Более того, явное выделение двух фаз утяжеляет и усложняет формирование ключей, если рассматривать последнее как однократное действие. Тем не менее, из архитектурных соображений управляющие контексты не только могут, но и должны существовать, поскольку обслуживают все протокольные уровни стека TCp/IP, концентрируя в одном месте необходимую функциональность. Первая фаза начинается в ситуации, когда взаимодействующие стороны не имеют общих секретов (общих ключей) и не уверены в аутентичности

друг друга. Если с самого начала не создать доверенный канал, то для выполнения каждого управляющего действия с ключами (их модификация, выдача диагностических сообщений и т.п.) в каждом протоколе (AH, ESp, TLS и т.д.) этот канал придется формировать заново.

Общие вопросы формирования контекстов безопасности и управления ключами освещаются в спецификации [67] - " Контексты безопасности и управление ключами в Internet" (Internet Security Association and Key Management protocol, ISAKMp). Здесь вводятся две фазы выработки протокольных ключей, определяются виды управляющих информационных обменов и используемые форматы заголовков и данных. Иными словами, в [67] строится протокольно-независимый каркас.

Существует несколько способов формирования управляющего контекста. Они различаются двумя показателями:

- используемым механизмом выработки общего секретного ключа;
- степенью защиты идентификаторов общающихся сторон.

В простейшем случае секретные ключи задаются заранее (ручной метод распределения ключей). Для небольших сетей такой подход вполне работоспособен, но он не является масштабируемым. Последнее свойство может быть обеспечено при автоматической выработке и распределении секретных ключей в рамках протоколов, основанных на алгоритме Диффи-Хелмана (см. [91]). Пример тому - "Протокол для обмена ключами в Internet " (The Internet Key Exchange, IKE, [43]).

При формировании управляющего контекста идентификаторы общающихся сторон (например, IP-адреса) могут передаваться в открытом виде или шифроваться. Поскольку ISAKMp предусматривает функционирование в режиме клиент/сервер (т. е. ISAKMp-сервер может формировать контекст для клиента), сокрытие идентификаторов в определенной степени повышает защищенность от пассивного прослушивания сети.

Последовательность передаваемых сообщений, позволяющих сформировать управляющий контекст и обеспечивающих защиту

идентификаторов, выглядит следующим образом (см. рис. 9.2).

Рис. 9.2. Формирование управляющего контекста.

В первом сообщении (1) инициатор направляет предложения по набору защитных алгоритмов и конкретных механизмов их реализации. Предложения упорядочиваются по степени предпочтительности (для инициатора). В ответном сообщении (2) партнер информирует о сделанном выборе - какие алгоритмы и механизмы его устраивают. Для каждого класса защитных средств (генерация ключей, аутентификация, шифрование) выбирается только один элемент.

В сообщениях (3) и (4) инициатор и партнер отправляют свои части ключевого материала, необходимые для выработки общего секретного ключа (мы опускаем детали, специфичные для алгоритма Диффи-Хелмана). Одноразовые номера (nonce) представляют собой псевдослучайные величины, служащие для защиты от воспроизведения сообщений.

Посредством сообщений (5) и (6) происходит обмен идентификационной информацией, подписанной (с целью

аутентификации) секретным ключом отправителя и зашифрованной выработанным на предыдущих шагах общим секретным ключом. Для аутентификации предполагается использование сертификатов открытых ключей. Отметим, что в число подписываемых данных входят одноразовые номера.

В представленном виде протокол формирования управляющего контекста защищает от атак, производимых нелегальным посредником, а также от нелегального перехвата соединений. Для защиты от атак на доступность, для которых характерно прежде всего навязывание интенсивных вычислений, присущих криптографии с открытым ключом, применяются так называемые идентифицирующие цепочки (cookies). Эти цепочки, формируемые инициатором и его партнером с использованием текущего времени (для защиты от воспроизведения), на самом деле присутствуют во всех ISAKMp-сообщениях и в совокупности идентифицируют управляющий контекст (в первом сообщении, по понятным причинам, фигурирует только цепочка инициатора). Согласно спецификациям [67], заголовок ISAKMp-сообщения имеет вид, изображенный на рис. 9.3. Если злоумышленник пытается "завалить" кого-либо запросами на создание управляющего контекста, подделывая при этом свой IP-адрес, то в сообщении (3) (см. выше рис. 9.2) он не сможет предъявить идентифицирующую цепочку партнера, поэтому до выработки общего секретного ключа и, тем более, электронной подписи и полномасштабной проверки аутентичности дело попросту не дойдет.

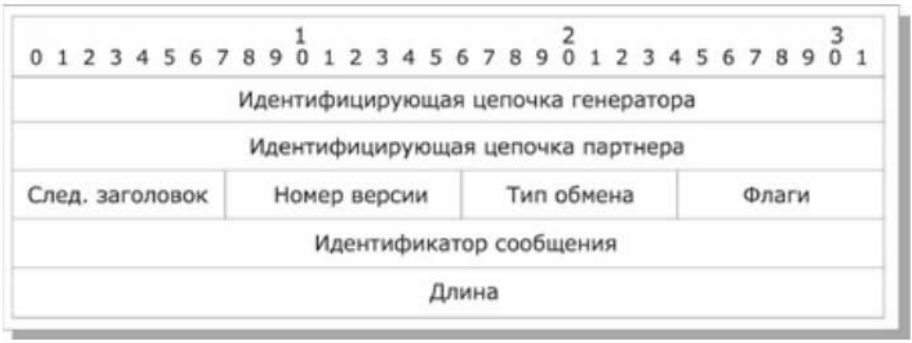

Рис. 9.3. Формат заголовка ISAKMp-сообщения.

Управляющие контексты являются двунаправленными в том смысле, что любая из общающихся сторон может инициировать с их помощью

выработку новых протокольных контекстов или иные действия. Для передачи ISAKMp-сообщений используется любой протокол, однако в качестве стандартного принят UDp с номером порта 500.

Протокольные контексты и политика безопасности

Системы, реализующие IPsec, должны поддерживать две базы данных:

- базу данных политики безопасности (Security policy Database, SpD);
- базу данных протокольных контекстов безопасности (Security Association Database, SAD).

Все IP-пакеты (входящие и исходящие) сопоставляются с упорядоченным набором правил политики безопасности. При сопоставлении используется фигурирующий в каждом правиле селектор - совокупность анализируемых полей сетевого уровня и более высоких протокольных уровней. Первое подходящее правило определяет дальнейшую судьбу пакета:

- пакет может быть ликвидирован;
- пакет может быть обработан без участия средств IPsec;
- пакет должен быть обработан средствами IPsec с учетом набора протокольных контекстов, ассоциированных с правилом.

Таким образом, системы, реализующие IPsec, функционируют как межсетевые экраны, фильтруя и преобразуя потоки данных на основе предварительно заданной политики безопасности.

Далее мы детально рассмотрим контексты и политику безопасности, а также порядок обработки сетевых пакетов.

Протокольный контекст безопасности в IPsec - это однонаправленное "соединение" (от источника к получателю), предоставляющее обслуживаемым потокам данных набор защитных сервисов в рамках какого-то одного протокола (AH или ESp). В случае симметричного взаимодействия партнерам придется организовать два контекста (по одному в каждом направлении). Если используются и AH, и ESp, потребуется четыре контекста.

Элементы базы данных протокольных контекстов содержат следующие поля (в каждом конкретном случае некоторые значения полей будут пустыми):

- используемый в протоколе AH алгоритм аутентификации, его ключи и т.п.;
- используемый в протоколе ESp алгоритм шифрования, его ключи, начальный вектор и т.п.;
- используемый в протоколе ESp алгоритм аутентификации, его ключи и т.п.;
- время жизни контекста;
- режим работы IPsec: транспортный или туннельный ;
- максимальный размер пакетов;
- группа полей (счетчик, окно, флаги) для защиты от воспроизведения пакетов.

Пользователями протокольных контекстов, как правило, являются прикладные процессы. Вообще говоря, между двумя узлами сети может существовать произвольное число протокольных контекстов, так как число приложений в узлах произвольно. Отметим, что в качестве пользователей управляющих контекстов обычно выступают узлы сети (поскольку в этих контекстах желательно сосредоточить общую функциональность, необходимую сервисам безопасности всех протокольных уровней эталонной модели для управления криптографическими ключами).

Управляющие контексты - двусторонние, т. е. любой из партнеров может инициировать новый ключевой обмен. Пара узлов может одновременно поддерживать несколько активных управляющих контекстов, если имеются приложения с существенно разными криптографическими требованиями. Например, допустима выработка части ключей на основе предварительно распределенного материала, в то время как другая часть порождается по алгоритму Диффи-Хелмана.

Протокольный контекст для IPsec идентифицируется целевым IP-адресом, протоколом (AH или ESp), а также дополнительной величиной - индексом параметров безопасности (Security parameter Index, SpI). Последняя величина необходима, поскольку могут существовать несколько контекстов с одинаковыми IP-адресами и протоколами. Далее

будет показано, как используются индексы SpI при обработке входящих пакетов.

IPsec обязывает поддерживать ручное и автоматическое управление контекстами безопасности и криптографическими ключами. В первом случае все системы заранее снабжаются ключевым материалом и иными данными, необходимыми для защищенного взаимодействия с другими системами. Во втором - материал и данные вырабатываются динамически, на основе определенного протокола - IKE [43], поддержка которого обязательна.

Протокольный контекст создается на базе управляющего с использованием ключевого материала и средств аутентификации и шифрования последнего. В простейшем случае, когда протокольные ключи генерируются на основе существующих, последовательность передаваемых сообщений выглядит так, как показано на рис. 9.4.

Рис. 9.4. Формирование протокольного контекста.

Когда вырабатывался управляющий контекст, для него было создано три вида ключей:

- SKEYID_d - ключевой материал, используемый для генерации протокольных ключей;
- SKEYID_a - ключевой материал для аутентификации;
- SKEYID_e - ключевой материал для шифрования.

Все перечисленные виды ключей задействованы в обмене, показанном на рис. 9.4. Ключом SKEYID_e шифруются сообщения. Ключ SKEYID_a служит аргументом хэш-функций и тем самым аутентифицирует сообщения. Наконец, протокольные ключи - результат применения псевдослучайной (хэш) функции к SKEYID_d с дополнительными параметрами, в число которых входят одноразовые номера инициатора и партнера. В результате создание протокольного контекста оказывается аутентифицированным, защищенным от несанкционированного ознакомления, от воспроизведения сообщений и от перехвата соединения.

Сообщения (1) и (2) могут нести дополнительную нагрузку, например, данные для выработки "совсем новых" секретных ключей или идентификаторы клиентов, от имени которых ISAKMp-серверы формируют протокольный контекст. В соответствии с протоколом IKE, за один обмен (состоящий из трех показанных на рис. 9.4 сообщений) формируется два однонаправленных контекста - по одному в каждом направлении. Получатель контекста задает для него индекс параметров безопасности (SpI), помогающий находить контекст для обработки принимаемых пакетов IPsec.

Строго говоря, протокольные контексты играют вспомогательную роль, будучи лишь средством проведения в жизнь политики безопасности; она должна быть задана для каждого сетевого интерфейса с задействованными средствами IPsec и для каждого направления потоков данных (входящие/исходящие). Согласно спецификациям IPsec [60], политика рассчитывается на бесконтекстную (независимую) обработку IP-пакетов, в духе современных фильтрующих маршрутизаторов. Разумеется, должны существовать средства администрирования базы данных SpD, так же, как и средства администрирования базы правил межсетевого экрана, однако этот аспект не входит в число стандартизуемых.

С внешней точки зрения, база данных политики безопасности (SpD) представляет собой упорядоченный набор правил. Каждое правило задается как пара:

- совокупность селекторов ;
- совокупность протокольных контекстов безопасности.

Селекторы служат для отбора пакетов, контексты задают требуемую обработку. Если правило ссылается на несуществующий контекст, оно должно содержать достаточную информацию для его (контекста) динамического создания. Очевидно, в этом случае требуется поддержка автоматического управления контекстами и ключами. В принципе, функционирование системы может начинаться с задания базы SpD при пустой базе контекстов (SAD); последняя будет наполняться по мере необходимости.

Дифференцированность политики безопасности определяется селекторами, употребленными в правилах. Например, пара взаимодействующих хостов может использовать единственный набор контекстов, если в селекторах фигурируют только IP-адреса; с другой стороны, набор может быть своим для каждого приложения, если анализируются номера TCp- и UDp-портов. Аналогично, два защитных шлюза способны организовать единый туннель для всех обслуживаемых хостов или же расщепить его (путем организации разных контекстов) по парам хостов или даже приложений.

Все реализации IPsec должны поддерживать селекцию следующих элементов:

- исходный и целевой IP-адреса (адреса могут быть индивидуальными и групповыми, в правилах допускаются диапазоны адресов и метасимволы "любой");
- имя пользователя или узла в формате DNS или X.500;
- транспортный протокол;
- номера исходного и целевого портов (здесь также могут использоваться диапазоны и метасимволы).

Обработка исходящего и входящего трафика, согласно [60], не является симметричной. Для исходящих пакетов просматривается база SpD, находится подходящее правило, извлекаются ассоциированные с ним протокольные контексты и применяются соответствующие механизмы безопасности. Во входящих пакетах для каждого защитного протокола уже проставлено значение SpI, однозначно определяющее контекст. Просмотр базы SpD в таком случае не требуется; можно считать, что политика безопасности учитывалась при формировании соответствующего контекста. (Практически это означает, что ISAKMp-

пакеты нуждаются в особой трактовке, а правила с соответствующими селекторами должны быть включены в SpD.)

Отмеченная асимметрия, на наш взгляд, отражает определенную незавершенность архитектуры IPsec. В более раннем, по сравнению с [60], документе RFC 1825 понятия базы данных политики безопасности и селекторов отсутствовали. В новой редакции сделано полшага вперед - специфицирован просмотр базы SpD как обязательный для каждого исходящего пакета, но не изменена обработка входящих пакетов. Конечно, извлечение контекста по индексу SpI эффективнее, чем просмотр набора правил, но при таком подходе, по меньшей мере, затрудняется оперативное изменение политики безопасности. Что касается эффективности просмотра правил, то ее можно повысить методами кэширования, широко используемыми при реализации IP.

Возможно, еще более серьезным недостатком является невозможность обобщения предложенных процедур формирования контекстов (управляющих и протокольных) на многоадресный случай. В текущих спецификациях IPsec смешиваются две разные вещи - область действия контекста (сейчас это односторонний или двусторонний поток данных) и способ его идентификации (по индексу SpI или паре идентифицирующих цепочек). Получается, что способ идентификации (именования) навязывает трактовку области действия, что представляется неверным. На наш взгляд, вопросы именования могут решаться локально, а область действия контекста потенциально должна распространяться на произвольное число партнеров.

Обеспечение аутентичности IP-пакетов

Протокол аутентифицирующего заголовка (Authentication Header, AH, см. [58]) служит в IPsec для обеспечения целостности пакетов и аутентификации источника данных, а также для защиты от воспроизведения ранее посланных пакетов. AH защищает данные протоколов более высоких уровней и те поля IP-заголовков, которые не меняются на маршруте доставки или меняются предсказуемым образом. (Отметим, что число "непредсказуемых" полей невелико - это prio. (Traffic Class), Flow Label и Hop Limit. Предсказуемо меняется целевой адрес при наличии дополнительного заголовка исходящей маршрутизации.)

Формат заголовка АН показан на рис. 9.5.

Рис. 9.5. Формат заголовка АН.

Поясним смысл полей, специфичных для АН:

- индекс параметров безопасности (SpI) - 32-битное значение, выбираемое получателем пакетов с АН-заголовками в качестве идентификатора протокольного контекста (см. выше раздел "Протокольные контексты и политика безопасности");
- порядковый номер - беззнаковое 32-битное целое, наращиваемое от пакета к пакету. Отправитель обязан поддерживать этот счетчик, в то время как получатель может (но не обязан) использовать его для защиты от воспроизведения. При формировании протокольного контекста обе взаимодействующие стороны делают свои счетчики нулевыми, а потом согласованным образом увеличивают их. Когда значение порядкового номера становится максимально возможным, должен быть сформирован новый контекст безопасности ;
- аутентификационные данные - поле переменной длины, содержащее имитовставку (криптографическую контрольную сумму, Integrity Check Value, ICV) пакета; способ его вычисления определяется алгоритмом аутентификации.

Для вычисления аутентифицированных имитовставок могут применяться различные алгоритмы. Спецификациями [58] предписывается обязательная поддержка двух алгоритмов, основанных на применении хэш-функций с секретными ключами:

- HMAC-MD5 (Hashed Message Authentication Code - Message Digest version 5, см. [65]);
- HMAC-SHA-1 (Hashed Message Authentication Code - Secure Hash Algorithm version 1, см. [66]).

Мы не будем описывать процесс вычисления хэш-функций, лишь еще раз обратим внимание на необходимость приведения национальных криптографических стандартов, нормативно-правовой базы и практических работ в соответствие со сложившейся международной практикой.

Обеспечение конфиденциальности сетевого трафика

Протокол инкапсулирующей защиты содержимого (Encapsulating Security payload, ESp, см. [59]) предоставляет три вида сервисов безопасности:

- обеспечение конфиденциальности (шифрование содержимого IP-пакетов, а также частичная защита от анализа трафика путем применения туннельного режима);
- обеспечение целостности IP-пакетов и аутентификации источника данных;
- обеспечение защиты от воспроизведения IP-пакетов.

Можно видеть, что функциональность ESp шире, чем у AH (добавляется шифрование); взаимодействие этих протоколов мы подробнее рассмотрим позже. Здесь же отметим, что ESp не обязательно предоставляет все сервисы, но либо конфиденциальность, либо аутентификация должны быть задействованы. Формат заголовка ESp выглядит несколько необычно (см. рис. 9.6). Причина в том, что это не столько заголовок, сколько обертка (инкапсулирующая оболочка) для зашифрованного содержимого. Например, ссылку на следующий заголовок нельзя выносить в начало, в незашифрованную часть, так как она лишится конфиденциальности.

Рис. 9.6. Формат заголовка ESp.

Поля "Индекс параметров безопасности (SpI)", "Порядковый номер" и "Аутентификационные данные" (последнее присутствует только при включенной аутентификации) имеют тот же смысл, что и для AH. Правда, ESp аутентифицирует лишь зашифрованную часть пакета (плюс два первых поля заголовка).

Применение протокола ESp к исходящим пакетам можно представлять себе следующим образом. Назовем остатком пакета ту его часть, которая помещается после предполагаемого места вставки заголовка ESp. При этом не важно, какой режим используется - транспортный или туннельный. Шаги протокола таковы:

- остаток пакета копируется в буфер;
- к остатку приписываются дополняющие байты, их число и номер (тип) первого заголовка остатка, с тем чтобы номер был прижат к границе 32-битного слова, а размер буфера удовлетворял требованиям алгоритма шифрования;
- текущее содержимое буфера шифруется;
- в начало буфера приписываются поля "Индекс параметров безопасности (SpI)" и "Порядковый номер" с соответствующими значениями;
- пополненное содержимое буфера аутентифицируется, в его конец помещается поле "Аутентификационные данные";
- в новый пакет переписываются начальные заголовки старого пакета и конечное содержимое буфера.

Таким образом, если в ESp включены и шифрование, и аутентификация, то аутентифицируется зашифрованный пакет. Для входящих пакетов действия выполняются в обратном порядке, т. е. сначала производится аутентификация. Это позволяет не тратить ресурсы на расшифровку поддельных пакетов, что в какой-то степени защищает от атак на доступность.

Два защитных протокола - AH и ESp - могут комбинироваться разными способами. При выборе транспортного режима AH должен использоваться после ESp (аналогично тому, как в рамках ESp аутентификация идет следом за шифрованием). В туннельном режиме AH и ESp применяются, строго говоря, к разным (вложенным) пакетам, число допустимых комбинаций здесь больше (хотя бы потому, что возможна многократная вложенность туннелей с различными начальными и/или конечными точками).

Совокупность механизмов, предлагаемая в рамках IPsec, является весьма мощной и гибкой. IPsec - это основа, на которой может строиться реализация виртуальных частных сетей, обеспечиваться защищенное взаимодействие мобильных систем с корпоративной сетью, защита прикладных потоков данных и т.п.

Спецификация Internet-сообщества TLS

Спецификация TLS развивает и уточняет популярный протокол Secure Socket Layer (SSL), используемый в большом числе программных продуктов. Она может служить основой обеспечения безопасности протоколов прикладного уровня.

Основные идеи и понятия протокола TLS

Мы приступаем к рассмотрению протокола безопасности транспортного уровня (Transport Layer Security, TLS) (см. [39]), в котором получили дальнейшее развитие понятия, изложенные в версии 3.0 популярного протокола Secure Socket Layer (SSL) корпорации Netscape.

Посредством протокола TLS приложения, построенные в архитектуре клиент/сервер, могут защититься от пассивного и активного прослушивания сети и подделки сообщений.

TLS имеет двухуровневую организацию. На первом (нижнем) уровне, опирающемся на надежный транспортный сервис, каковой предоставляет, например, TCP, располагается протокол передачи записей (TLS Record Protocol), на втором (верхнем) - протокол установления соединений (TLS Handshake Protocol). Строго говоря, протокол безопасности транспортного уровня располагается между транспортным и прикладным уровнями. Его можно отнести к сеансовому уровню эталонной модели ISO/OSI.

Протокол передачи записей обеспечивает конфиденциальность и целостность передаваемых данных. Обеспечение конфиденциальности достигается путем применения методов симметричного шифрования (см. [91]), причем для каждого соединения генерируется свой секретный ключ. Контроль целостности (и, в частности, аутентичности) сообщений основан на использовании хэш-функций с секретными ключами.

Протокол установления соединений позволяет серверу и клиенту провести взаимную аутентификацию, согласованно выбрать алгоритм шифрования и криптографические ключи перед тем, как прикладной протокол начнет передачу данных. Для аутентификации сторон

применяются методы криптографии с открытым ключом (см. [91]), при выработке совместных секретов обеспечивается конфиденциальность и целостность, в том числе защита от нелегального посредника.

В соответствии с уровневой организацией сетевых протоколов, TLS не зависит от протоколов прикладного уровня. Кроме того, он обеспечивает интероперабельность использующих его независимо написанных приложений или компонентов приложений; последние могут успешно согласовывать криптографические параметры в динамике, не располагая информацией о кодах друг друга.

По отношению к алгоритмам симметричного и асимметричного шифрования TLS представляет собой алгоритмически независимый, расширяемый каркас, допускающий добавление новых криптографических методов и их реализаций.

В спецификациях TLS фигурируют четыре криптографические операции: цифровая подпись, потоковое шифрование, блочное шифрование и шифрование открытым ключом. Все они, особенно асимметричное шифрование, способны поглотить много процессорного времени. Для решения этой проблемы определенное внимание уделено вопросам эффективности, минимизации нагрузки на процессор и сеть: предлагаемая схема кэширования в рамках сеанса уменьшает число соединений, устанавливаемых "с нуля".

В последующих разделах подробно рассматриваются составляющие протокола TLS и их использование.

Протокол передачи записей

В общем виде функционирование протокола передачи записей можно представлять себе следующим образом. Сообщение, поступившее для передачи с более высокого протокольного уровня, включает длину, тип и содержимое. Оно разбивается на блоки (записи), допускающие эффективную обработку (или, наоборот, в один блок объединяется несколько небольших однотипных сообщений), сжимается, снабжается имитовставкой, шифруется, затем результат передается. На стороне получателя принятые данные расшифровываются, верифицируются, подвергаются декомпрессии и сборке, и затем сообщение доставляется

клиенту на вышележащем протокольном уровне.

Спецификациями TLS предусмотрено четыре вышележащих клиента протокола передачи записей:

- протокол установления соединений;
- протокол оповещения (alert protocol);
- протокол смены параметров шифрования (change cipher spec protocol);
- протокол передачи прикладных данных (application data protocol).

Функции этих протоколов будут рассмотрены в следующем разделе.

С точки зрения протокола передачи записей, каждое соединение является двунаправленным и может находиться в одном из двух состояний: обработки (т. е. быть текущим) и ожидания (быть отложенным). Кроме того, состояние соединения характеризуется применяемыми алгоритмами (сжатия, шифрования, вычисления имитовставки) и их параметрами (секретными ключами и начальными векторами. Наконец, каждому соединению соответствуют четыре экземпляра состояния: по два на клиентской и серверной сторонах (любая из них может передавать и принимать данные).

Перечислим и другие элементы состояния соединения:

- мастер-секрет - 48-байтное значение, разделяемое партнерами по общению и служащее для выработки других общих секретов (ключей шифрования и т.п.);
- два 32-байтных случайных значения, одно из которых предоставляется сервером, а другое - клиентом, но оба участвуют в выработке ключей и начальных векторов;
- два 64-битных порядковых номера передаваемой записи (по одному на сторонах отправителя и получателя) с нулевым начальным значением.

Первоначальное состояние - ожидания - создает протокол установления соединений ; он же ведает переводом отложенных соединений в текущие и наоборот.

Формально процесс обработки данных протоколом передачи записей можно описать как последовательность преобразований структур (в спецификациях [39] для этой цели используется интуитивно понятный C-подобный язык).

На первом шаге выполняется фрагментация (или объединение однотипных) сообщений, предназначенных для передачи, в структуры TLSPlaintext размером не более 16384 байт (см. листинг 10.1).

```
enum {
  change_cipher_spec(20), alert(21),
  handshake(22), application_data(23), (255)
} ContentType;

struct {
  ContentType type;
  ProtocolVersion version;
  uint16 length;
  opaque fragment [TLSPlaintext.length];
} TLSPlaintext;
```

Листинг 10.1. Начальная структура блока протокола передачи записей.

Типы сообщений, поступающих с вышележащих уровней протоколу передачи записей, могут чередоваться, а сами сообщения - создавать очереди. В таком случае прикладные данные имеют наименьший приоритет.

На втором шаге выполняется сжатие данных (естественно, без потери информации). Оно приводит к появлению следующей структуры (см. листинг 10.2).

```
struct {
  ContentType type;
  /* Тот же, что и TLSPlaintext.type */

  ProtocolVersion version;
  /* Та же, что и TLSPlaintext.version */
```

```
  uint16 length;
  opaque fragment [TLSCompressed.length];
} TLSCompressed;
```

Листинг 10.2. Структура блока протокола передачи записей после сжатия.

Далее следуют криптографические операции. К этому моменту на основе мастер-секрета и случайных значений, предоставленных сервером и клиентом, должен быть сгенерирован ключевой блок достаточной длины (см. листинг 10.3).

```
key_block = PRF
    (SecurityParameters.master_secret,
     "key expansion",
     SecurityParameters.server_random +
     SecurityParameters.client_random);

/* PRF - псевдослучайная функция */
/* "+" обозначает операцию конкатенации */
```

Листинг 10.3. Вычисление ключевого блока в протоколе передачи записей.

Затем ключевой блок делится на порции, служащие клиенту и серверу ключами хэш-функций и шифрования, а также начальным вектором (см. листинг 10.4).

```
client_write_MAC_secret
    [SecurityParameters.hash_size]
server_write_MAC_secret
    [SecurityParameters.hash_size]
client_write_key
    [SecurityParameters.key_material_length]
server_write_key
    [SecurityParameters.key_material_length]

client_write_IV [SecurityParameters.IV_size]
server_write_IV [SecurityParameters.IV_size]

/* MAC - Message Authentication Code, */
```

```
/* аутентификационный код сообщения */
/* IV - Initialization Vector, */
/* начальный вектор */
```

Листинг 10.4. Параметры криптографических операций протокола передачи записей.

С помощью сформированных параметров криптографических операций выполняется третий шаг протокола передачи записи, состоящий в вычислении имитовставки (см. листинг 10.5).

```
HMAC_hash (MAC_write_secret, seq_num +
  TLSCompressed.type +
  TLSCompressed.version +
  TLSCompressed.length +
  TLSCompressed.fragment));
```

Листинг 10.5. Вычисление имитовставки в протоколе передачи записей.

Обратим внимание, что в состав аргумента хэш-функции входит порядковый номер записи для защиты от кражи, дублирования и переупорядочения сообщений.

На четвертом шаге выполняется шифрование блока вместе с имитовставкой (см. листинг 10.6).

```
stream-ciphered struct {
  opaque content [TLSCompressed.length];
  opaque MAC [CipherSpec.hash_size];
} GenericStreamCipher;

block-ciphered struct {
  opaque content [TLSCompressed.length];
  opaque MAC [CipherSpec.hash_size];
  uint8 padding
    [GenericBlockCipher.padding_length];
  uint8 padding_length;
} GenericBlockCipher;

struct {
```

```
  ContentType type;
  ProtocolVersion version;
  uint16 length;
  select (CipherSpec.cipher_type) {
   case stream: GenericStreamCipher;
   case block: GenericBlockCipher;
  } fragment;
 } TLSCiphertext;
```

Листинг 10.6. Шифрование блока вместе с имитовставкой в протоколе передачи записей.

На стороне получателя действия выполняются в обратном порядке:

- расшифрование;
- контроль целостности;
- декомпрессия;
- сборка сообщений.

Разумеется, и здесь должны быть сформированы параметры криптографических операций.

Протокол установления соединений и ассоциированные протоколы

Назначение протокола установления соединений - организовать сеанс взаимодействия клиента и сервера (произвести аутентификацию сторон, согласовать применяемые алгоритмы - сжатия, выработки ключей, шифрования и вычисления имитовставки - и их параметры). Позднее, в рамках того же сеанса (при наличии флага возобновляемости), опираясь на согласованные параметры, новые соединения могут формироваться более экономным образом.

На рис. 10.1 показан процесс формирования сеанса. Звездочками помечены необязательные сообщения, в квадратные скобки заключено сообщение протокола смены параметров шифрования.

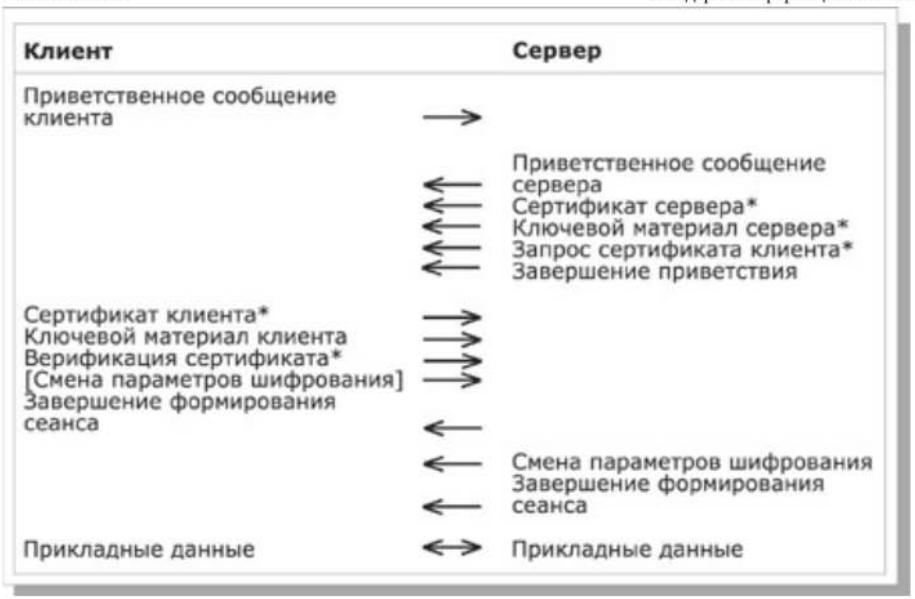

Рис. 10.1. Процесс формирования сеанса

Процесс формирования нового сеанса происходит с помощью транспортных услуг протокола передачи записей по некоторому существующему соединению, возможно, с пустыми алгоритмами сжатия и криптографии.

Новое соединение на основе существующего сеанса формируется более экономным образом (см. рис. 10.2).

Рис. 10.2. Формирование нового соединения на основе существующего

сеанса

Обычно новые сеансы и соединения формируются по инициативе клиента (например, при подсоединении к серверу), но и сервер может "намекнуть" клиенту на желательность подобного действия (если, например, пришло время смены криптографических параметров), послав запрос приветственного сообщения (HelloRequest).

Поясним структуру и назначение сообщений, приведенных на рисунках.

Приветственное сообщение клиента, открывающее процесс формирования сеанса или соединения, выглядит следующим образом (см. листинг 10.7).

```
struct {
  uint32 gmt_unix_time;
  opaque random_bytes [28];
} Random;

struct {
  ProtocolVersion client_version;
  Random random;
  SessionID session_id;
  CipherSuite cipher_suites<2..2^16-1>;
  CompressionMethod
    compression_methods<1..2^8-1>;
} ClientHello;
```

Листинг 10.7. Структура приветственного сообщения клиента в протоколе установления соединений.

Если идентификатор сеанса (session_id) пуст, имеется в виду формирование нового сеанса; в противном случае устанавливается новое соединение в рамках существующего сеанса. Поля compression_methods и cipher_suites содержат списки предлагаемых клиентом алгоритмов сжатия и криптографии (в порядке убывания приоритетов). Они должны быть построены так, чтобы согласие между клиентом и сервером было заведомо возможным. В частности, в списке алгоритмов сжатия должен фигурировать пустой метод.

Сервер отвечает клиенту собственным приветствием, главное в котором - выбранные алгоритмы сжатия и криптографии (см. листинг 10.8).

```
struct {
  ProtocolVersion server_version;
  Random random;
  SessionID session_id;
  CipherSuite cipher_suite;
  CompressionMethod compression_method;
} ServerHello;
```

Листинг 10.8. Структура приветственного сообщения сервера в протоколе установления соединений.

Если клиент представил непустой идентификатор сеанса, сервер ищет его в своем кэше и при возможности и желании возобновляет сеанс, формируя на его основе (по сокращенному варианту, показанному на рис. 10.2) новое соединение. В противном случае организуется еще один сеанс, быть может, анонимный (с пустым идентификатором) и, следовательно, невозобновляемый.

На следующем шаге формирования нового сеанса сервер направляет клиенту свой сертификат (точнее, сертификационный маршрут), назначение которого - предоставить материал для выработки совместных ключей и аутентифицировать сервер. В принципе, возможен, хотя и не рекомендуется, анонимный сеанс, без обмена сертификатами, однако нужно помнить, что он уязвим для атак нелегального посредника.

Если сертификат сервера не посылался или содержащихся в нем данных недостаточно, сервер должен отправить свой ключевой материал в отдельном сообщении. При желании сервер может запросить сертификат клиента.

После завершения приветствия сервером инициатива переходит к клиенту, который должен представить свой сертификат (если таковой был запрошен) и ключевой материал для выработки предварительного мастер-секрета (или сам секрет, зашифрованный открытым ключом сервера, если таков согласованный метод выработки ключей). В случае

предоставления клиентом сертификата, открытый ключ в котором пригоден для проверки электронной подписи, клиент может подписать все сообщения, отправленные и полученные к этому моменту в процессе установления соединения, что позволит аутентифицировать его как обладателя соответствующего секретного ключа и подтвердить целостность процесса.

Сообщения о завершении формирования сеанса (соединения), отправляемые как клиентом, так и сервером, - первые, защищенные только что согласованными алгоритмами. Они позволяют убедиться, что выработка ключей и аутентификация прошли успешно. После того как стороны отправили подобное сообщение, получили и верифицировали соответствующее сообщение партнера, они могут переходить к обмену прикладными данными.

Структура сообщения о завершении формирования сеанса (соединения) показана на листинге 10.9.

```
struct {
  opaque verify_data[12];
} Finished;

Finished.verify_data = PRF (master_secret,
  finished_label, MD5(handshake_messages) +
  SHA-1(handshake_messages)) [0..11];

/* Хэшируются все сообщения, участвовавшие в */
/* установлении соединения */
/* Значениями параметра "finished_label"
/* служат, соответственно, цепочка символов */
/*"client finished" на стороне клиента */
/* и "server finished" на стороне сервера. */
```

Листинг 10.9. Структура сообщения о завершении формирования сеанса в протоколе установления соединений.

Мастер-секрет вычисляется единообразно для всех методов выработки ключей (см. листинг 10.10).

```
master_secret = PRF
```

```
(pre_master_secret,
 "master secret",
 ClientHello.random + ServerHello.random)
    [0..47];
```

Листинг 10.10. Вычисление мастер-секрета.

Участвующий в процессе формирования сеанса протокол смены параметров шифрования устроен предельно просто и заключает в себе один тип однобайтных сообщений.

Более содержательный протокол оповещения предназначен для передачи предупреждений и сообщений об ошибках. Наиболее употребительное предупреждение - уведомление о завершении сеанса. Типичные ошибки - неожиданное сообщение, неверная имитовставка, неверный параметр, ошибка расшифрования и т.п. После получения сообщения об ошибке соединение разрывается.

Применение протокола HTTP над TLS

Применение протокола HTTP над TLS описано в спецификациях [73]. С концептуальной точки зрения, оно организовано весьма просто. HTTP/TLS-сервер слушает порт 443. HTTP/TLS-клиент, являясь, в частности, TLS -клиентом, начинает процесс установления соединения с посылки приветственного сообщения. По сформированному TLS - соединению направляются обычные HTTP-запросы и ответы на них, которые трактуются протоколом TLS как прикладные данные.

В уникальном идентификаторе ресурсов (URI) сочетание HTTP/TLS обозначается как "https":

```
https://www.example.com/home.html
```

Обычно после анализа URI клиент узнает имя хоста, на котором функционирует сервер. Это имя должно быть сопоставлено с тем, которое фигурирует в сертификате сервера. Если сервер задан IP-адресом, тот же адрес должен присутствовать в сертификате и подвергаться проверке.

В качестве сигнала окончания взаимодействия используется

уведомление о завершении сеанса.

Спецификация Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности"

Рассматривается прикладной программный интерфейс к средствам защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Данная спецификация логически дополняет защитные протоколы сетевого и транспортного уровней.

Введение

Обобщенный прикладной программный интерфейс службы безопасности (Generic Security Service Application Program Interface - GSS-API, см. [64], [82]) предназначен для защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Он предоставляет услуги по взаимной аутентификации осуществляющих контакт партнеров и по контролю целостности и обеспечению конфиденциальности пересылаемых сообщений.

Пользователями интерфейса безопасности GSS-API являются коммуникационные протоколы (обычно прикладного уровня) или другие программные системы, самостоятельно выполняющие пересылку данных.

Обобщенный интерфейс безопасности GSS-API не зависит от конкретной языковой среды и от механизмов безопасности, обеспечивающих реальную защиту. Последнее обстоятельство позволяет создавать приложения, которые на уровне исходного текста мобильны по отношению к смене механизмов безопасности. Тем самым реализуется открытость прикладных систем и соответствующих средств защиты.

Следует отметить, что средства защиты могут быть очень разными - от систем Kerberos (см. [91]) до продуктов, реализующих спецификации X.509, т. е. GSS-API имеет под собой вполне конкретную почву.

На каждом компьютере, где предполагается применять интерфейс

безопасности GSS-API, должно быть установлено клиентское программное обеспечение соответствующего механизма защиты. Приложение, использующее GSS-API, локальным образом вызывает необходимые функции, получая в ответ так называемые токены безопасности. Подобный токен может содержать зашифрованное удостоверение пользователя, электронную подпись или целое зашифрованное сообщение. Приложения обмениваются токенами безопасности, достигая тем самым аутентификации, целостности и конфиденциальности общения. Поскольку коммуникационные аспекты вынесены за пределы GSS-API, он автоматически оказывается независимым от сетевых протоколов. Сетевая мобильность приложений должна обеспечиваться иными средствами.

Основные понятия

Обобщенный прикладной программный интерфейс службы безопасности содержит следующие основные понятия:

- удостоверение ;
- контекст безопасности ;
- токен безопасности ;
- механизм безопасности ;
- имя;
- канал передачи данных.

Удостоверение - это структура данных, позволяющая ее владельцу доказать партнеру по общению или третьей стороне, что он (владелец) является именно тем, за кого себя выдает. Таким образом, в GSS-API удостоверения выступают как средство аутентификации.

Естественно, что служба безопасности (например, Kerberos) совместно с операционной системой должны обеспечить защиту удостоверений от несанкционированного использования и/или изменения. Процессам, действующим от имени пользователей, не предоставляется прямого доступа к удостоверениям. Вместо этого при необходимости процессы снабжаются дескрипторами удостоверений, которые не содержат секретной информации и не нуждаются в защите. Нет смысла воровать дескрипторы, поскольку их интерпретация для разных процессов-

предъявителей будет различной.

Одному пользователю могут понадобиться удостоверения нескольких видов. Во-первых, структура удостоверений, несомненно, зависит от механизма безопасности, стоящего за обобщенным интерфейсом. Во-вторых, иногда для связи с разными партнерами нужны различные удостоверения. В-третьих, особым образом должны быть устроены так называемые делегируемые удостоверения, служащие для передачи прав на выполнение определенных действий от имени некоторого пользователя. Есть и другие факторы, влияющие на структуру удостоверений.

В процессе входа пользователя в систему могут формироваться удостоверения стандартного вида, выдаваемые по умолчанию.

Контекст безопасности - это пара структур данных (по одной локально хранимой структуре для каждого контактирующего партнера), где содержится разделяемая информация о состоянии процесса общения, необходимая для защиты пересылаемых сообщений. Как и удостоверения, контексты безопасности хранятся внутренним (для службы безопасности) образом - прикладные процессы снабжаются лишь дескрипторами контекстов. Контексты формируются на основании локально выданных или делегированных удостоверений.

Партнеры могут по очереди или одновременно использовать несколько контекстов, если необходимо поддерживать информационные потоки разной степени защищенности.

Интерфейс GSS-API не зависит от используемых коммуникационных протоколов, поэтому формирование контекста безопасности никак не связано с установлением соединения в сетевом смысле. Более того, для GSS-API безразлично, какой протокол используется - с установлением соединения или без такового. Организация потока сообщений, а также выделение из входного потока данных, генерируемых в рамках GSS-API, - обязанность прикладных систем.

Токены безопасности - элементы данных, пересылаемые между пользователями интерфейса GSS-API с целью поддержания работоспособности этого интерфейса и защиты прикладной информации. Токены подразделяются на два класса. Контекстный класс

предназначен для установления контекстов безопасности и для выполнения над ними управляющих действий. В рамках уже установленного контекста для защиты сообщений используются токены сообщений.

Перед началом общения с удаленным партнером приложение обращается к интерфейсу GSS-API с просьбой инициализировать контекст. В ответ возвращается контекстный токен безопасности, который приложение обязано переслать партнеру. Тот, получив токен, передает его локальному экземпляру GSS-API для проверки подлинности инициатора и продолжения (обычно - завершения) формирования контекста.

Если приложению необходимо защитить сообщение, обеспечив возможность контроля целостности и подлинности источника данных, оно передает его интерфейсу GSS-API, получая в ответ токен, содержащий криптографическую контрольную сумму (имитовставку, хэш, дайджест), заверенную электронной подписью отправителя. После этого приложение должно переслать как само сообщение, так и защищающий его токен. Партнер, получив обе порции данных, передает их своему локальному экземпляру GSS-API для проверки авторства и целостности.

Для приложения структура токенов безопасности закрыта. Токены генерируются и контролируются исключительно функциями GSS-API. Дело приложения - переслать их и передать соответствующим функциям для обработки. Естественно, служба безопасности обнаружит попытки приложения изменить токен, если таковые будут предприняты.

Вполне возможно, что на удаленных системах функционирует несколько различных служб безопасности. В этих условиях для успешного формирования контекста безопасности партнеры должны тем или иным способом договориться, какая именно служба будет использоваться.

Конкретная служба характеризуется типом реализуемого механизма безопасности. В свою очередь, тип обозначается посредством структуры данных, называемой идентификатором объекта . На уровне обобщенного программного интерфейса структура идентификаторов объектов не уточняется.

Каждая система обязана предлагать некоторый механизм безопасности как подразумеваемый, которым и рекомендуется пользоваться приложению из соображений мобильности.

Если токены являются структурой, закрытой для приложений, то структура имен, употребляемых при формировании контекста безопасности (имеются в виду имена партнеров по общению), закрыта для функций GSS-API. Имена рассматриваются этими функциями как последовательности байт, интерпретируемые, вероятно, коммуникационными компонентами приложений.

В GSS-API предусматривается наличие трех типов имен - внутренних, печатных и объектных. Как правило, аргументами функций GSS-API служат внутренние имена. Интерфейс GSS-API предоставляет функции для преобразования имен и выполнения некоторых других действий над ними.

Отметим, что интерпретация имен - дело довольно сложное, поскольку они могут принадлежать разным пространствам имен. Чтобы избежать неоднозначности, в состав имени включается идентификатор его типа.

Для усиления защиты информации в интерфейсе GSS-API предлагается возможность связывания контекста безопасности с определенными каналами передачи данных: инициатор формирования контекста может указать набор каналов, которые допустимо использовать в рамках открываемого сеанса общения. Партнер должен подтвердить свое согласие на связывание с этим набором каналов. Канал характеризуется целевым адресом и некоторыми другими параметрами, включая формат пересылаемой по нему информации, степень ее защищенности и т.п. Если токен, отправленный для установления контекста, будет перехвачен, использование соответствующего контекста ограничится рамками связанных с ним каналов. Можно надеяться, что подобное препятствие затруднит действия злоумышленника.

Каждая функция, входящая в состав обобщенного интерфейса безопасности GSS-API, возвращает два кода ответа - основной и дополнительный. Набор основных кодов регламентируется в рамках GSS-API, дополнительные могут быть специфичны для различных служб безопасности.

Основные коды подразделяются на информирующие и сигнализирующие об ошибке. Перечислим некоторые информирующие коды:

- GSS_S_COMPLETE - нормальное завершение;
- GSS_S_CONTINUE_NEEDED - требуется дополнительный вызов данной функции;
- GSS_S_DUPLICATE_TOKEN - обнаружено дублирование токена защиты сообщений.

Следующие значения входят в число кодов, сигнализирующих об ошибке:

- GSS_S_BAD_NAME - задано некорректное имя;
- GSS_S_CONTEXT_EXPIRED - истек срок действия контекста;
- GSS_S_CREDENTIALS_EXPIRED - истек срок действия удостоверения;
- GSS_S_DEFECTIVE_TOKEN - обнаружено повреждение токена безопасности;
- GSS_S_NO_CONTEXT - не задан контекст;
- GSS_S_NO_CRED - не задано удостоверение.

Проанализировав основной код, приложение сделает вывод о нормальном или ненормальном завершении функции. В последнем случае оно может принять во внимание дополнительный код, что даст пользователю больше информации, но уменьшит мобильность приложения.

Функции для работы с удостоверениями

Работа приложения, опирающегося на интерфейс GSS-API, должна начинаться с получения удостоверения, которое засвидетельствует, что приложение имеет право выступать от имени определенного субъекта.

Интерфейс GSS-API предоставляет следующие функции для применения удостоверений:

- GSS_Acquire_cred - запрос удостоверения для последующего использования;
- GSS_Release_cred - отказ от удостоверения, ставшего ненужным;
- GSS_Inquire_cred - получение информации об удостоверении ;
- GSS_Add_cred - постепенное формирование удостоверения;
- GSS_Inquire_cred_by_mech - получение информации об удостоверении, связанной с конкретным механизмом безопасности.

Как уже указывалось, приложение получает в свое распоряжение не само удостоверение, а его дескриптор, впоследствии используемый в качестве аргументов функций GSS_Release_cred, GSS_Inquire_cred, GSS_Add_cred, а также функций формирования контекста безопасности.

Функция GSS_Acquire_cred нужна в первую очередь серверным процессам, желающим сообщить, от чьего имени они выступают. Интерактивные пользователи могут получать подразумеваемые удостоверения неявным образом при входе в систему. Аналогично, при выходе такого пользователя из системы может автоматически выполняться вызов функции GSS_Release_cred.

Функция GSS_Inquire_cred позволяет получить информацию об удостоверении: имя ассоциированного субъекта, срок годности, возможность употребления в операциях с контекстом (инициация и/или принятие), поддерживаемые механизмы безопасности. Данная функция особенно полезна применительно к подразумеваемому удостоверению, характеристики которого могут меняться от системы к системе.

С помощью функции GSS_Add_cred возможно постепенно формировать удостоверения, добавляя в них поля, необходимые различным механизмам безопасности.

Функция GSS_Inquire_cred_by_mech пригодится в среде, поддерживающей несколько механизмов безопасности. Она, в частности, позволяет убедиться в том, что допускается использование данного удостоверения совместно с конкретным механизмом

безопасности.

Создание и уничтожение контекстов безопасности

Создание контекста безопасности предшествует всем операциям по обмену сообщениями между потенциальными партнерами. В процессе его формирования партнеры могут убедиться в подлинности друг друга, а также договориться о степени защищенности коммуникаций. Впрочем, обычно, в силу асимметричности отношения клиент/сервер, аутентификация носит односторонний характер - сервер убеждается в подлинности клиента.

Для работы с контекстами обобщенный интерфейс безопасности GSS-API предоставляет следующие функции:

- `GSS_Init_sec_context` - формирование "исходящего" контекста, т. е. части контекста, относящейся к инициатору общения;
- `GSS_Accept_sec_context` - формирование "входящего" контекста, т. е. части контекста, относящейся к вызываемому партнеру;
- `GSS_Delete_sec_context` - отказ от контекста, ставшего ненужным;
- `GSS_Process_context_token` - обработка полученного контекстного токена;
- `GSS_Context_time` - выяснение срока годности контекста;
- `GSS_Inquire_context` - получение информации о контексте ;
- `GSS_Wrap_size_limit` - выяснение максимального размера сообщения, которое можно зашифровать в рамках заданного контекста безопасности ;
- `GSS_Export_sec_context` - передача контекста другому процессу ;
- `GSS_Import_sec_context` - прием контекста, переданного другим процессом.

Инициатор общения вызывает функцию `GSS_Init_sec_context`, передавая ей свое удостоверение - явно полученное или

подразумеваемое. Кроме того, инициатор специфицирует запрашиваемую процедуру взаимной аутентификации и уровень защиты сообщений. В ответ ему возвращается токен, который следует переслать партнеру.

Партнер, получив токен, передает его функции GSS_Accept_sec_context (вместе со своим удостоверением). Как правило, на этом формирование контекста заканчивается. Партнеры должны проанализировать флаги, ассоциированные с контекстом, чтобы узнать, каков реально предоставленный уровень защиты.

Если инициатор общения (обычно это клиент) желает убедиться в подлинности партнера, он передает функции GSS_Init_sec_context флаг mutual_req_flag (требуется взаимная аутентификация). В таком случае вызов GSS_Init_sec_context возвращает в качестве основного кода значение GSS_S_CONTINUE_NEEDED (а не GSS_S_COMPLETE). Соответствующим образом меняется и генерируемый контекстный токен. Партнер, приняв и обработав (с помощью функции GSS_Accept_sec_context) присланную информацию, получит на выходе установленный флаг mutual_state и новый контекстный токен, который следует вернуть инициатору. Последний должен повторно обратиться к функции GSS_Init_sec_context с полученным токеном. При отсутствии ошибок GSS_Init_sec_context вернет, наконец, основной код GSS_S_COMPLETE, и формирование контекста на этом завершится.

При формировании контекста служба безопасности может требовать обмена несколькими токенами (даже без взаимной аутентификации). Тогда инициатору придется несколько раз вызывать функцию GSS_Init_sec_context, а его партнеру - функцию GSS_Accept_sec_context. Все вызовы, кроме последнего, вернут основной код GSS_S_CONTINUE_NEEDED. Последний вызов, завершающий формирование контекста на соответствующей стороне, в нормальном случае выдаст основной код GSS_S_COMPLETE.

Партнеры должны сами определять (способами, внешними по отношению к GSS-API), что именно из пересылаемой информации представляет собой контекстный токен и какой функции его следует

передать. При отказе от контекста, ставшего ненужным, функция GSS_Delete_sec_context может передать управляющий токен, подлежащий пересылке партнеру. Партнер, приняв токен, должен вызвать функцию GSS_Process_context_token, которая проанализирует управляющую информацию и удалит вторую половину сбрасываемого контекста.

Как правило, в процессе формирования контекста партнер получает информацию о его инициаторе. Инициатор может запросить формирование "анонимного" контекста посредством флага anon_req_flag. Это имеет смысл при пользовании общедоступными услугами (получение свободно распространяемой информации и т.п.). Партнер вправе принять или отвергнуть анонимный контекст.

Функция GSS_Inquire_context позволяет получить информацию о контексте - имена инициатора общения и его партнера, срок годности, тип задействованного механизма безопасности, а также ассоциированные флаги (replay_det_state - обеспечивается отслеживание продублированных сообщений, conf_avail - предоставляется возможность шифровать сообщения и т.п.).

Функция GSS_Export_sec_context предоставляет токен, пригодный для передачи контекста безопасности другому процессу в пределах одной вычислительной системы. Передавать можно только полностью сформированный контекст. Вообще говоря, экспортировав контекст, процесс теряет право на его использование.

Для приема (импорта) контекста безопасности служит функция GSS_Import_sec_context.

Защита сообщений

При формировании контекста партнеры по общению имеют возможность убедиться в подлинности друг друга. Все остальные средства службы безопасности направлены на защиту сообщений.

Интерфейс GSS-API предоставляет следующие функции для работы с сообщениями:

- GSS_GetMIC - формирование токена, позволяющего контролировать целостность сообщения и подлинность его источника;
- GSS_VerifyMIC - проверка целостности сообщения и подлинности источника с помощью ассоциированного токена;
- GSS_Wrap - формирование инкапсулированного, возможно, зашифрованного, сообщения, содержащего информацию для контроля целостности и проверки подлинности источника;
- GSS_Unwrap - разбор инкапсулированного сообщения.

При формировании контекста инициатор специфицирует требуемый уровень защиты сообщений. Ответные флаги показывают, обеспечивается ли этот уровень на самом деле. Флаг integ_avail информирует о возможности контроля целостности и подлинности источника сообщения, conf_avail - о доступности средств шифрования. Прежде чем обращаться к функциям GSS_GetMIC / GSS_Wrap, приложение должно проверить состояние перечисленных флагов.

Функция GSS_GetMIC на основе сообщения формирует отдельный токен безопасности. Функция GSS_Wrap "упаковывает" контрольную информацию вместе с сообщением (быть может, зашифрованным). Приложения должны уметь различать токены безопасности и сообщения (инкапсулированные или нет) и обрабатывать их соответствующим образом.

Служба безопасности способна предоставлять дополнительные услуги в виде отслеживания продублированных сообщений и усиленного контроля последовательности сообщений. При формировании контекста эти услуги могут быть заказаны (флаги replay_det_req_flag и sequence_req_flag). Ответные флаги показывают, действительно ли обеспечивается запрошенный уровень защиты - тогда в ассоциированные токены безопасности или инкапсулированные сообщения прозрачным для приложения образом могут вставляться порядковые номера, временные штампы и т.п. Соответственно, приложение должно быть готово получить от функций GSS_VerifyMIC / GSS_Unwrap основные коды завершения: GSS_S_DUPLICATE_TOKEN (обнаружено дублирование сообщений),

GSS_S_OLD_TOKEN (старое сообщение), GSS_S_UNSEQ_TOKEN (опоздавшее сообщение), GSS_S_GAP_TOKEN (сообщение пришло слишком рано - некоторые предшествующие сообщения еще не получены). Подозрительные сообщения, несмотря на ненормальный код завершения, передаются приложению, которое трактует ситуацию в соответствии с избранной политикой безопасности (в частности, ничто не мешает обработать сообщение обычным образом).

Некоторые службы безопасности могут предоставлять различное качество защиты (Quality Of Protection - QOP). Выбор подходящего качества важен для приложения с точки зрения разумного расходования ресурсов, поскольку сильная защита может требовать значительных накладных расходов. В спецификациях интерфейса GSS_API определяется формат элемента данных, описывающего качество защиты. Это 32-битное целое, состоящее из двух 16-битных частей, одна из которых относится к контролю целостности, а другая - к обеспечению конфиденциальности. В обоих случаях задается степень контроля, идентификаторы используемых алгоритмов и информация, специфичная для выбранного алгоритма.

Логика работы пользователей интерфейса безопасности

Приведем примерный сценарий взаимодействия между клиентом и сервером (см. рис. 11.1). Предполагается, что для взаимной аутентификации достаточно обмена одной парой токенов безопасности и что партнеры запрашивают и контроль целостности, и обеспечение конфиденциальности сообщений, а служба безопасности предоставляет им эти средства.

Детали, связанные с преобразованием имен, опущены. Текст в фигурных скобках является комментарием. Стрелка --> отделяет входные параметры от выходных.


Клиент
Сервер
(Получение удостоверения сервером)
GSS_Acquire_cred (server_name
(имя, под которым регистрируется
сервер), ...)
-->
GSS_S_COMPLETE, ...,
serv_cred_handle
(дескриптор удостоверения сервера),
...
(Обслуживание других клиентов)
(Получение удостоверения клиентом)
(Неявное получение подразумеваемого
удостоверения при входе в систему)
(Начало формирования контекста
клиентом)
GSS_Init_sec_context (NULL
(подразумеваемое удостоверение),
0 (дескриптор контекста пока
не сформирован),
targ_name (имя удаленного сервера),
...,
mutual_req_flag
(истина, если нужна
взаимная аутентификация), ...,
NULL (пока нет токена,
полученного от партнера))
-->
GSS_S_CONTINUE_NEEDED, ...,
client_context_handle (дескриптор
контекста для клиента), ...,
con_token_1 (контекстный токен,
который нужно переслать серверу),
... (флаги), ...
Пересылка токена con_token_1 серверу
(Принятие контекста сервером)
GSS_Accept_sec_context
(serv_cred_handle,
0 (дескриптор контекста пока не
сформирован), ...,
con_token_1)
-->
GSS_S_COMPLETE, ...,
client_name (имя инициатора
формирования контекста), ...,
serv_context_handle (дескриптор
контекста для сервера),
... (флаги), ...,
con_token_2 (контекстный токен,
который нужно вернуть клиенту)
Пересылка токена con_token_2 клиенту
(Завершение формирования
контекста клиентом)
GSS_Init_sec_context (NULL,
client_context_handle,
targ_name, ...,
con_token_2)
-->
GSS_S_COMPLETE, ...,
client_context_handle, ...,
NULL (нет токена, который нужно
переслать серверу), ...
(Формирование клиентом
сообщения с контролем целостности
и доказательством подлинности
источника данных)
GSS_GetMIC (client_context_handle,
0 (подразумеваемое качество защиты),
message_1 (защищаемое сообщение))
-->
GSS_S_COMPLETE, ...,
mes_token_1 (токен, защищающий
сообщение)
Пересылка сообщения message_1 и токена mes_token_1 серверу
(Проверка сервером целостности и
аутентичности полученного сообщения)
GSS_VerifyMIC (serv_context_handle,
message_1,
mes_token_1)
-->
qop_state (обеспечиваемое
качество защиты),
GSS_S_COMPLETE (если все в порядке),
...
(Формирование сервером
зашифрованного сообщения)
GSS_Wrap (serv_context_handle,
conf_req_flag (истина, если требуется
шифрование),
0 (подразумеваемое качество защиты),
message_2)
-->
GSS_S_COMPLETE, ...,
conf_state (истина, если служба
безопасности обеспечивает
конфиденциальность),
encaps_message_2 (инкапсулированное
сообщение message_2, зашифрованное,
с добавленной информацией для
контроля целостности и подлинности
источника)
Пересылка зашифрованного сообщения encaps_message_2 клиенту
(Прием клиентом зашифрованного
сообщения)
GSS_Unwrap (client_context_handle,
encaps_message_2)
-->
conf_state (истина, если служба
безопасности обеспечивает
конфиденциальность),
qop_state (обеспечиваемое
качество защиты),
GSS_S_COMPLETE (если все в
порядке), ...,
message_2 (расшифрованное
сообщение)
(Обмен другими сообщениями)
(Сброс сервером контекста
безопасности, ставшего ненужным)
GSS_Delete_sec_context
(serv_context_handle)
-->
GSS_S_COMPLETE, ...,
con_token_3 (контекстный токен,
который можно переслать клиенту,
чтобы тот также удалил свою часть
контекста безопасности)
Пересылка токена con_token_3 клиенту
(Обработка полученного
управляющего токена)
GSS_Process_context_token
(client_context_handle,
con_token_3)
-->
GSS_S_COMPLETE, ...
(Выход клиента из системы)
(Обслуживание других клиентов)

Рис. 11.1. Примерный сценарий взаимодействия между клиентом и сервером под защитой обобщенного интерфейса безопасности.

Мы видим, что общая схема взаимодействия удаленных партнеров под защитой интерфейса безопасности GSS-API довольно проста, однако практическая реализация всех необходимых проверок (кодов завершения, установленных флагов) требует известной аккуратности.

Представление некоторых объектов интерфейса безопасности в среде языка C

Представление средствами языка C объектов, фигурирующих в обобщенном интерфейсе безопасности GSS-API, по большей части довольно очевидно (или не может быть стандартизовано, так как зависит от специфики механизма безопасности).

Прежде всего, вводится тип `OM_uint32`, соответствующий 32-битным беззнаковым целым значениям. Большинство структурных значений представляется с помощью указателя на дескриптор (см. листинг 11.1).

```
typedef struct gss_buffer_desc_struct {
  size_t length;
  void *value;
} gss_buffer_desc, *gss_buffer_t;
```

Листинг 11.1. Описание дескриптора буфера и указателя на него.

Тип `gss_buffer_t` используется при задании составных аргументов - имен, дескрипторов, токенов, сообщений и т.п.

Идентификаторы объектов представляются следующим образом (см. листинг 11.2).

```
typedef struct gss_OID_desc_struct {
  OM_uint32 length;
  void *elements;
} gss_OID_desc, *gss_OID;
```

Листинг 11.2. Описание дескриптора идентификаторов объектов и указателя на него.

Указатели `elements` ссылаются на начало представления идентификаторов, т. е. на последовательности байт, устроенных в соответствии с базовыми правилами ASN.1.

Наборы объектных идентификаторов представляются так, как показано на листинге 11.3.

```
typedef struct gss_OID_set_desc_struct {
  int    count;
  gss_OID elements;
} gss_OID_set_desc, *gss_OID_set;
```

Листинг 11.3. Описание дескриптора набора объектных идентификаторов и указателя на него.

Вводятся и некоторые другие типы, уточняющие представление структурированных значений.

На листинге 11.4 показано, как выглядит на языке C описание функции `GSS_Init_sec_context`.

```
OM_uint32 GSS_Init_sec_context (
  OM_uint32 *minor_status,
  const gss_cred_id_t initiator_cred_handle,
  gss_ctx_id_t  *context_handle,
  const gss_name_t  target_name,
  const gss_OID mech_type,
  OM_uint32 req_flags,
  OM_uint32 time_req,
  const gss_channel_bindings_t
    input_chan_bindings,
  const gss_buffer_t input_token
  gss_OID *actual_mech_type,
  gss_buffer_t output_token,
  OM_uint32 *ret_flags,
  OM_uint32 *time_rec
);
```

Листинг 11.4. Описание функции GSS_Init_sec_context.

Отметим, что параметр `context_handle` является здесь одновременно входным и выходным, а основной код завершения возвращается как результат функции.

Разумеется, есть еще много аспектов, оговоренных в спецификациях [82], например, кто и когда отводит память под объекты и под дескрипторы, и каким образом эту память можно освобождать. Мы, однако, не будем на этом останавливаться.

Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия"

Анализируются рекомендации по формированию политики безопасности организации, имеющей современную информационную систему и активно использующей сетевые сервисы.

Основные понятия

Мы приступаем к рассмотрению спецификаций Internet-сообщества, относящихся к административному и процедурному уровням информационной безопасности (см. курс "Основы информационной безопасности" [91]). Центральное место среди них занимает "Руководство по информационной безопасности предприятия" ([44], [42]), причем предшествующая (с формальной точки зрения - устаревшая) версия этой спецификации, [44], представляется более информативной. В своем изложении мы опираемся на публикацию [26].

Данное Руководство призвано помочь организациям, имеющим выход в Internet, сформировать политику безопасности и разработать соответствующие процедуры. В нем перечисляются вопросы и факторы, которые следует предварительно проанализировать, даются некоторые рекомендации, обсуждается ряд смежных тем. Руководство содержит лишь основные элементы, необходимые для выработки политики и процедур безопасности. Чтобы получить эффективный набор защитных средств, ответственным лицам придется принять немало решений, заключить многочисленные соглашения, и лишь после этого довести политику безопасности до сотрудников и приступить к ее реализации.

Руководство рассчитано на руководителей и системных администраторов. Основной акцент делается на политику и процедуры, необходимые для поддержки технических средств, выбранных организацией.

Слова "организация" и "предприятие" трактуются в нем как синонимы, обозначающие собственника компьютеров и иных сетевых ресурсов. В число последних входят хосты, на которых работают пользователи, а

также маршрутизаторы, терминальные серверы, ПК и другие устройства, имеющие связь с Internet.

Организация может выступать в роли конечного пользователя сервисов Internet или поставщиком соответствующих услуг. Тем не менее, Руководство рассчитано в основном на конечных пользователей.

Предполагается, что организация способна создавать собственные политику и процедуры безопасности при согласии и поддержке реальных владельцев ресурсов.

Термин " системный администратор " относится к тем, кто отвечает за повседневную работу ресурсов. Администрирование может выполнять группа людей или независимая компания.

Понятие " руководитель " обозначает сотрудника организации, вырабатывающего или одобряющего политику безопасности. Часто (но не всегда) руководитель одновременно является собственником ресурсов.

Документ отвечает на вопросы о том, что входит в политику безопасности, какие процедуры необходимы для обеспечения безопасности, что нужно делать в ситуациях, угрожающих безопасности. При выработке политики следует помнить не только о защите локальной сети, но также о нуждах и требованиях других подсоединенных сетей.

Системные администраторы и руководители должны располагать сведениями о современных угрозах, связанных с ними рисках, размере возможного ущерба, а также о наборе доступных мер для предотвращения и отражения нападений.

Проблемы, с которыми может столкнуться организация

В Руководстве рассматривается гипотетическая, но весьма вероятная последовательность проблем в области информационной безопасности.

- Системный администратор получает сообщение о том, что главный подпольный бюллетень крэкеров распространяется с

административной машины, находящейся в его ведении, и попадает в пять тысяч американских и западноевропейских компьютеров.

- Спустя восемь недель тот же администратор получает официальное уведомление, что информация из одного бюллетеня была использована для выведения из строя на пять часов службы "911" в одном из больших городов.
- Пользователь звонит и сообщает, что он не может войти в систему под своим именем в 3 часа утра субботы. Администратору также не удается войти в систему.
- После перезагрузки и входа в однопользовательский режим он обнаруживает, что файл паролей пуст. К утру понедельника выясняется, что между данной машиной и местным университетом в привилегированном режиме было передано несколько файлов.
- Во вторник утром на университетском компьютере найдена копия стертого файла паролей вместе с аналогичными файлами с дюжины других машин.
- Спустя неделю администратор обнаруживает, что файлы инициализации системы изменены враждебным образом.
- Администратор получает сообщение о том, что в компьютер правительственной лаборатории совершено вторжение с подведомственной ему машины. Ему предлагают предоставить регистрационную информацию для отслеживания нападавшего.
- Спустя неделю администратор получает список подведомственных компьютеров, подвергшихся успешным атакам крэкеров.
- Администратору звонит репортер и интересуется подробностями проникновения на компьютеры организации. Администратор ничего не слышал о таких проникновениях.
- Через три дня выясняется, что случай проникновения имел-таки место. Глава организации использовал в качестве пароля имя жены.
- Обнаруживаются модификации системных бинарных файлов.
- После восстановления файлы в тот же день вновь оказываются модифицированными. Так повторяется несколько недель.

С подобными проблемами может столкнуться любая организация, имеющая выход в Internet. Необходимо иметь заранее заготовленные

ответы по крайней мере на следующие вопросы:

- Если в системе обнаруживается присутствие злоумышленника, следует ли оставить систему открытой и попытаться проследить за ним, или компьютер нужно немедленно выключить и залатать обнаруженные дыры?
- Если злоумышленник использует компьютеры вашей организации, должны ли вы обращаться в правоохранительные органы? Кто принимает решение о таком обращении? Если представитель властей предложит оставить системы открытыми, кто ответит за это решение?
- Какие шаги следует предпринять, если звонят из другой организации и сообщают о подозрительных действиях со стороны одного из ваших пользователей? Что делать, если этим пользователем окажется местный системный администратор?

Основы предлагаемого подхода

Формирование политики и процедур безопасности означает выработку плана действий по информационной защите, для этого необходимо:

- выяснить, что следует защищать;
- выяснить, от чего следует защищаться;
- определить вероятность угроз;
- реализовать меры, которые позволят защитить активы экономически оправданным образом;
- постоянно возвращаться к предыдущим этапам и совершенствовать защиту после выявления новых уязвимых мест.

В рассматриваемом Руководстве основной упор делается на два последних этапа, однако следует помнить и о критической важности первых трех этапов для принятия эффективных решений в области безопасности, поскольку стоимость защиты не должна превосходить вероятный ущерб от осуществления угроз.

Руководство [44], помимо вводного, содержит еще пять разделов, где обсуждаются вопросы, которые организация должна рассмотреть при выработке политики безопасности и формировании процедур,

реализующих эту политику. В некоторых случаях анализируются имеющиеся альтернативы и аргументы в пользу выбора какой-либо из них.

В плане общей структуры обсуждение политики безопасности предшествует рассмотрению процедур, необходимых для ее реализации. Первый из пяти разделов посвящен особенностям официальной политики предприятия, касающейся доступа к вычислительным ресурсам. Рассматриваются также вопросы ее нарушения. Политика определяет набор необходимых процедур, поэтому руководителю следует сначала разобраться в политических составляющих предмета обсуждения и только после этого переходить к процедурным. Ключевым компонентом формирования политики безопасности является производимая в той или иной форме оценка рисков, позволяющая установить, что необходимо защищать и каков объем ресурсов, которые разумно выделить на защиту.

Когда политика выработана, можно приступать к созданию процедур, решающих проблемы безопасности. В разделе "Выработка процедур для предупреждения нарушений безопасности" определяются и предлагаются действия, которые необходимо предпринять при возникновении подозрений по поводу совершения неавторизованных операций, и анализируются ресурсы, необходимые для предотвращения нарушений режима безопасности.

В разделе "Типы процедур безопасности " перечисляются типы процедур, служащих для предотвращения нападений. Профилактика - основа безопасности.

Раздел "Реакция на нарушения безопасности" посвящен реагированию на нарушения безопасности, т. е. кругу вопросов, с которыми организация сталкивается, когда кто-то отступает от политики безопасности. Если такое случается, приходится принимать целый комплекс решений, но многие из них можно продумать заранее. По крайней мере, следует договориться о распределении обязанностей и способах взаимодействия. И здесь важнейшую роль играет политика безопасности.

Тема последнего раздела - меры, предпринимаемые после ликвидации нарушения безопасности. Планирование защитных действий - это

непрерывный циклический процесс, поэтому очередной инцидент становится прекрасным поводом для пересмотра и улучшения политики и процедур.

Общие принципы выработки официальной политики предприятия в области информационной безопасности

Целью формирования официальной политики предприятия в области информационной безопасности является определение правильного (с точки зрения организации) способа использования вычислительных и коммуникационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности. Чтобы достичь данной цели, следует учесть специфику конкретной организации.

Во-первых, необходимо принять во внимание ее цели и основные направления деятельности. Например, на военной базе и в университете требования к конфиденциальности весьма отличаются.

Во-вторых, разрабатываемая политика должна согласовываться с существующими законами и правилами, относящимися к организации. Значит, и те, и другие необходимо принять во внимание при разработке политики.

В-третьих, если локальная сеть организации не изолирована, вопросы безопасности следует рассматривать в более широком контексте. Политика должна освещать проблемы, возникающие на локальном компьютере из-за действий удаленной стороны, а также удаленные проблемы, причиной которых является локальный хост или пользователь.

Политика безопасности призвана стать результатом совместной деятельности технического персонала, способного понять все аспекты ее структуры и реализации, а также руководителей, способных влиять на неуклонное выполнение установленных правил. Нереализуемая или неподдерживаемая политика бесполезна.

Ключевой элемент политики - доведение до каждого сотрудника его обязанностей по поддержанию режима безопасности. Она не может

предусмотреть всего, однако обязана гарантировать, что для любого вида проблем существует ответственный исполнитель.

В связи с информационной безопасностью можно выделить несколько уровней ответственности. На первом уровне каждый пользователь компьютерного ресурса обязан заботиться о защите своего счета. Пользователь, допустивший его компрометацию, увеличивает вероятность компрометации других счетов и ресурсов.

Системные администраторы образуют другой уровень ответственности. Они должны обеспечивать защиту компьютерных систем. Сетевых администраторов можно отнести к еще более высокому уровню.

Важно определить, кто будет интерпретировать политику безопасности, поскольку вне зависимости от того, насколько хорошо она написана, время от времени ее содержание нуждается в разъяснении, а заодно и в пересмотре.

После того как все положения записаны и одобрены, необходимо начать активный процесс, гарантирующий, что политика безопасности воспринята и обсуждена.

Целесообразно провести собрания, чтобы выслушать пожелания пользователей и заодно убедиться в правильном понимании предложенных правил.

Помимо усилий по оглашению политики на начальном этапе, необходимо постоянно напоминать о ней. Опытные пользователи нуждаются в периодических напоминаниях, новичкам ее нужно разъяснять, вводя в курс дела. Прежде чем допускать сотрудника к работе, разумно заручиться его подписью, свидетельствующей о том, что с политикой безопасности он ознакомился и понял ее суть.

Анализ рисков, идентификация активов и угроз

Один из главных побудительных мотивов выработки политики безопасности состоит в получении уверенности, что деятельность по защите информации построена экономически оправданным образом. Данное положение кажется очевидным, но не исключены ситуации,

когда усилия прикладываются не там, где нужно.

Процесс анализа рисков включает в себя определение того, что следует защищать, от чего и как это делать. Необходимо рассмотреть все возможные риски и ранжировать их в зависимости от потенциального размера ущерба.

Один из этапов анализа рисков состоит в идентификации всех объектов, нуждающихся в защите. Некоторые активы (аппаратура т.п.) идентифицируются очевидным образом. Про другие (например, про людей, использующих информационные системы) нередко забывают. Важно принять во внимание все, что может пострадать от нарушений режима безопасности.

В Руководстве фигурирует следующая классификация активов:

- аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, маршрутизаторы;
- программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;
- данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям;
- люди: пользователи, обслуживающий персонал;
- документация: по программам, по аппаратуре, системная, по административным процедурам;
- расходные материалы: бумага, формы, красящая лента, магнитные носители.

После выявления активов, нуждающихся в защите, необходимо идентифицировать угрозы и размеры возможного ущерба. К числу основных классов возможных угроз относятся:

- несанкционированный доступ;
- нелегальное ознакомление с информацией;

- отказ в обслуживании.

Регламентация использования ресурсов

При разработке политики безопасности ряд вопросов требует обязательных ответов:

- Кто имеет право пользоваться ресурсами?
- Как правильно использовать ресурсы?
- Кто наделен правом давать привилегии и разрешать использование?
- Кто может иметь административные привилегии?
- Каковы права и обязанности пользователей?
- Каковы права и обязанности системных администраторов по отношению к обычным пользователям?
- Как работать с конфиденциальной информацией?

После определения круга лиц, имеющих доступ к системным ресурсам, необходимо описать правильные и неправильные способы их применения. Для разных категорий пользователей (студентов, внешних пользователей, штатных сотрудников и т.д.) эти способы могут различаться. Следует явно указать, что допустимо, а что - нет.

Пользователи должны знать: они несут ответственность за свои действия независимо от применяемых защитных средств, использовать чужие счета и обходить механизмы безопасности запрещено.

Для регламентации доступа к ресурсам нужно ответить на следующие вопросы:

- Разрешается ли использование чужих счетов?
- Можно ли отгадывать чужие пароли?
- Допускается ли разрушение сервисов?
- Должны ли пользователи предполагать, что если файл доступен на чтение всем, то они имеют право его читать?
- Вправе ли пользователи модифицировать чужие файлы, если по каким-либо причинам у них есть доступ на запись?
- Обязаны ли пользователи разделять счета?

В большинстве случаев ответы на подобные вопросы будут отрицательными.

В политике могут найти отражение авторские и лицензионные права на программное обеспечение. Лицензионное соглашение с поставщиком налагает на организацию определенные обязательства; чтобы не нарушить их, необходимо приложить некоторые усилия.

Тщательно сформулированная политика в области правильного использования ресурсов очень важна: если явно не сказано, что запрещено, не удастся доказать, что нежелательные действия пользователя - это нарушения.

Бывают исключительные случаи, когда в исследовательских целях пользователи или администраторы пытаются "взломать" защиту сервиса или лицензионной программы. Политика должна давать ответ на вопрос, разрешены ли подобные исследования в организации и каковы могут быть их рамки.

Применительно к исключительным случаям следует дать ответы на такие вопросы:

- Разрешены ли вообще подобные исследования?
- Что именно разрешено: попытки проникновения, выращивание червей и вирусов и т.п.?
- Каким образом должны контролироваться подобные исследования (например, изолировать их в рамках отдельного сегмента сети)?
- Как защищены пользователи (в том числе внешние) от подобных исследований?
- Как получать разрешение на проведение исследований?

В случае, если разрешение получено, следует отделить тестируемые сегменты от основной сети предприятия: бесспорно, черви и вирусы нельзя выпускать в производственную сеть.

Политика безопасности должна давать ответ на вопрос, кто распоряжается правами доступа к сервисам. Кроме того, необходимо точно знать, какие именно права этим людям позволено распределять.

Существует много возможных схем управления распределением прав доступа к сервисам. При выборе подходящей целесообразно принять во внимание следующие моменты:

- Как будут распределяться права доступа - централизованно или из нескольких мест?
- Какие методы предполагается использовать для заведения счетов и запрещения доступа?

Наделение пользователей правами доступа - одна из самых уязвимых процедур. Прежде всего следует позаботиться, чтобы начальный пароль не был легко угадываемым, не являлся функцией от имени пользователя или его полного имени. Не стоит автоматически генерировать начальные пароли, если результат легко предсказуем.

Нельзя разрешать пользователям до бесконечности полагаться на начальный пароль. По возможности следует создавать условия для обязательной его замены при первом входе в систему.

Одно из решений, которое должно быть тщательно взвешено, относится к выбору лиц, имеющих доступ к административным привилегиям и паролям. Очевидно, подобный доступ полагается системным администраторам, но неизбежны ситуации, когда за привилегиями будут обращаться другие пользователи, что с самого начала следует предусмотреть в политике безопасности.

Сотрудники, имеющие специальные привилегии, должны быть подотчетны некоторому должностному лицу.

Политика безопасности должна содержать положения о правах и обязанностях пользователей применительно к использованию компьютерных систем и сервисов предприятия. Должно быть явно оговорено, что все сотрудники обязаны понимать и выполнять правила безопасной эксплуатации систем. Ниже приведен перечень тем, которые целесообразно осветить в данном разделе политики безопасности:

- Каковы общие рамки использования ресурсов? Существуют ли ограничения на ресурсы и каковы они?

- Что является злоупотреблением с точки зрения производительности системы?
- Как "секретные" пользователи должны охранять свои пароли?
- Насколько часто пользователи должны менять пароли? Каковы другие аналогичные ограничения и требования?
- Как обеспечивается резервное копирование - централизованно или индивидуально?
- Какой должна быть реакция на случаи просмотра конфиденциальной информации?
- Соблюдается ли конфиденциальность почты?
- Какова политика в отношении неправильно адресованной почты, отправлений по спискам рассылки или в адрес телеконференций?
- Должен соблюдаться баланс между правом пользователей на тайну и обязанностью системного администратора собирать достаточно информации для разрешения проблем и расследования случаев нарушения режима безопасности. Политика должна определять границы, в пределах которых системный администратор вправе исследовать пользовательские файлы с целью разрешения проблем и для иных нужд, и конкретизировать права пользователей. При необходимости можно сформулировать положение относительно обязанности администратора соблюдать конфиденциальность информации, полученной при оговоренных выше обстоятельствах.

Следует сообщить пользователям, какие сервисы (при наличии таковых) пригодны для хранения конфиденциальной информации. Должны рассматриваться различные способы хранения данных (на диске, файловом сервере и т.д.).

Реагирование на нарушения политики безопасности (административный уровень)

Очевидно, что любая официальная политика, вне зависимости от ее отношения к информационной безопасности, время от времени нарушается. Нарушение может стать следствием пользовательской небрежности, случайной ошибки, отсутствия должной информации о текущей политике или ее непонимания. Возможно также, что некое лицо или группа лиц сознательно совершают действия, прямо

противоречащие утвержденной политике безопасности.

Необходимо заранее определить характер действий, предпринимаемых в случае обнаружения нарушений политики, чтобы они были быстрыми и правильными, а также организовать расследование и выяснить, как и почему нарушение стало возможным. После этого нужно внести коррективы в систему защиты.

Политику безопасности могут нарушать самые разные лица. Некоторые из них являются сотрудниками предприятия, другие нападают извне. Полезно определить сами понятия "свои" и "чужие", исходя из административных, правовых или политических положений.

Правильно организованное обучение - лучшая защита. Надо поставить дело так, чтобы не только внутренние, но и внешние легальные пользователи знали положения политики безопасности.

Каждое предприятие должно заранее определить набор административных санкций, применяемых к местным пользователям, нарушающим политику безопасности другой организации, и, кроме того, позаботиться о защите от ответных действий с ее стороны.

Для взаимодействия с внешними организациями, в число которых входят правоохранительные органы, другие учреждения, команды "быстрого реагирования", средства массовой информации, политика безопасности предприятия должна содержать специальные процедуры, регламентирующие, кто имеет право на такие контакты и как именно они совершаются. Среди прочих нужно дать ответы на следующие вопросы:

- Кому поручено разговаривать с прессой?
- Когда следует обращаться в правоохранительные органы?
- Какого рода сведения об инцидентах могут выходить за пределы организации?
- Помимо политических положений, необходимо продумать и написать процедуры, исполняемые в случае обнаружения нарушений режима безопасности.

Когда на организацию совершается нападение, грозящее нарушением

информационной безопасности, стратегия ответных действий может строиться под влиянием двух противоположных подходов.

Если руководство опасается уязвимости предприятия, оно может предпочесть стратегию "защититься и продолжить". Главная ее цель - защита информационных ресурсов и максимально быстрое восстановление нормальной работы пользователей. Действиям нарушителя оказывается максимальное противодействие, дальнейший доступ предотвращается, после чего немедленно начинается процесс оценки повреждения и восстановления. Возможно, придется выключить компьютерную систему, закрыть доступ в сеть или предпринять иные жесткие меры. Оборотная сторона медали состоит в том, что пока злоумышленник не выявлен, он может вновь напасть на эту же или другую организацию прежним или новым способом.

Другой подход, "выследить и осудить", опирается на иные философию и систему целей: злоумышленнику продолжать свои действия, пока организация не сможет установить его личность. Такой подход приветствуют правоохранительные органы. К сожалению, они не смогут освободить организацию от ответственности, если пользователи обратятся в суд с иском по поводу ущерба, нанесенного их программам и данным.

Следующий контрольный перечень помогает сделать выбор между стратегиями "защититься и продолжить" и "выследить и осудить".

Перечень обстоятельств, обусловливающих стратегию "защититься и продолжить":

- активы организации недостаточно защищены;
- продолжающееся вторжение сопряжено с большим финансовым риском;
- нет возможности или намерения осудить злоумышленника ;
- неизвестен круг пользователей;
- пользователи неопытны, а их работа уязвима;
- пользователи могут привлечь организацию к суду за нанесенный ущерб.

Когда предпочтительна стратегия "выследить и осудить":

- активы и системы хорошо защищены;
- имеются качественные резервные копии;
- угроза активам организации меньше потенциального ущерба от будущих повторных вторжений;
- имеет место скоординированная атака, повторяющаяся с большой частотой и настойчивостью;
- организация "притягивает" злоумышленников и, следовательно, подвергается частым атакам.
- организация готова идти на риск, позволяя продолжить вторжение ;
- действия злоумышленника можно контролировать;
- доступны развитые средства отслеживания, поэтому преследование нарушителя имеет шансы на успех;
- обслуживающий персонал обладает достаточной квалификацией для успешного отслеживания;
- руководство организации желает осудить злоумышленника ;
- имеется тесный контакт с правоохранительными органами;
- среди сотрудников есть человек, хорошо знающий соответствующие законы;
- организация готова к искам собственных пользователей по поводу программ и данных, скомпрометированных во время выслеживания злоумышленника.

Подход к выработке процедур для предупреждения нарушений безопасности

Политика безопасности отвечает на вопрос ЧТО:

- Что следует защищать?
- Что является самым важным?
- Что за свойства у защищаемых объектов?
- Что за подход к проблемам безопасности избран?

Сама по себе политика безопасности не говорит, КАК защищаются объекты. Ответы на вопросы КАК дают процедуры безопасности.

Политика безопасности оформляется в виде высокоуровневого документа, описывающего общую стратегию. Процедуры безопасности

должны в деталях специфицировать шаги, предпринимаемые организацией для собственной защиты.

Политика безопасности должна включать в себя общую оценку рисков по отношению к наиболее вероятным угрозам и оценку возможных последствий их осуществления. Часть процесса оценки рисков заключается в составлении списка активов, нуждающихся в защите. Данная информация необходима для выработки экономически эффективных процедур.

Заманчиво начать разработку процедур безопасности, отправляясь от защитных механизмов: "На всех компьютерах нашей организации должны вестись регистрационные журналы, модемы обязаны выполнять обратный дозвон, а всем пользователям необходимо выдать интеллектуальные карточки". Однако подобный подход может повести к массированной защите областей с небольшим риском и к недостаточной защите действительно уязвимых участков. Если же начать с политики и описанных ею рисков, можно быть уверенным, что процедуры обеспечивают достаточный уровень защиты для всех активов.

Чтобы определить риски, необходимо выявить уязвимые места. Одна из целей политики безопасности состоит в том, чтобы их прикрыть и тем самым уменьшить риск для максимально возможного числа активов. К числу типичных уязвимостей и их источников относятся:

- точки доступа ;
- неправильно сконфигурированные системы;
- программные ошибки;
- внутренние злоумышленники.

Выбор регуляторов для практичной защиты

После определения объектов защиты и оценки рисков, грозящих активам, необходимо решить, как реализовать средства безопасности. Регуляторы и защитные механизмы следует выбирать так, чтобы успешно и в то же время без излишних затрат противостоять угрозам, выявленным в процессе анализа рисков.

Выбранные регуляторы представляют собой реальное воплощение политики безопасности. Они образуют первую (и главную) линию обороны. В этой связи особенно важно, чтобы регуляторы в совокупности составляли правильный набор. Если наибольшая угроза для системы - внешние злоумышленники, то нет смысла использовать биометрические устройства для аутентификации обычных, внутренних пользователей. Если, с другой стороны, основная опасность состоит в неавторизованном использовании вычислительных ресурсов внутри предприятия, целесообразно воспользоваться процедурами автоматического учета совершаемых действий.

Здравый смысл - лучшее средство формирования политики безопасности. Тщательная проработка схем и механизмов - занятие увлекательное и в определенной степени необходимое, но едва ли имеет смысл тратить деньги и время на такую проработку, если без внимания остались простые регуляторы. Например, как бы тщательно ни была продумана система, построенная на основе существующих средств безопасности, один пользователь с плохо выбранным паролем способен поставить под удар всю организацию.

Целесообразно построить эшелонированную оборону, применяя несколько стратегий защиты. При подобном подходе, если одна линия обороны оказывается прорванной, в дело вступает другая - и активы не остаются беззащитными. Комбинация нескольких простых стратегий зачастую позволяет создать более надежный заслон, чем один, даже очень сложный, метод.

Если не обеспечена физическая защита, говорить о других аспектах информационной безопасности не имеет смысла. Имея доступ к машине, злоумышленник может остановить ее, перезагрузить в привилегированном режиме, заменить диск или изменить его содержимое и т.п.

Критически важные коммуникационные каналы, серверы и другие ключевые элементы должны быть сосредоточены в закрытых помещениях. Некоторые механизмы безопасности (например, сервер аутентификации Kerberos) выполняют свои функции только при условии физической защищенности.

Для обнаружения большинства видов неавторизованного

использования компьютерных систем существуют несложные процедуры, применяющие стандартные средства операционных систем или опирающиеся на инструментарий, свободно доступный из различных источников.

Системный мониторинг может выполняться как администратором, так и специально написанными программами. Он включает в себя просмотр различных частей системы в поисках чего-нибудь необычного.

Отслеживание использования систем очень важно выполнять постоянно. Бессмысленно выделять для мониторинга один день в месяце, поскольку нарушения режима безопасности зачастую длятся всего несколько часов.

Пользователям необходимо объяснить, как выявлять случаи нелегального вторжения в их счета. Если при входе в систему выдается время предыдущего входа, они должны сопоставить его со своими прошлыми действиями.

Должны быть разработаны процедуры, позволяющие докладывать о замеченных проблемах, связанных с неправильным использованием счета или с другими аспектами безопасности.

Отслеживайте состояние привилегированных счетов ("root" в ОС UNIX). Как только привилегированный пользователь увольняется или перестает нуждаться в привилегиях, следует изменить пароли всех принадлежавших ему счетов.

При установке с дистрибутива операционной системы или дополнительного программного продукта необходимо тщательно проверить результирующую конфигурацию. Многие процедуры установки исходят из предположения, что всем пользователям в организации можно доверять, оставляя файлы общедоступными для записи или иным способом компрометируя безопасность.

Тщательной проверке должны подвергаться и сетевые сервисы. Часто поставщики в стандартной конфигурации предполагают надежность всех внешних хостов, что едва ли разумно, если речь идет о такой глобальной сети, как Internet.

Многие злоумышленники собирают информацию о слабостях конкретных версий систем. Чем старее версия, тем вероятнее наличие в ее защите известных ошибок, исправленных поставщиком в более поздних выпусках. В этой связи необходимо сопоставить риск от сохранения старой версии (с "дырами" в безопасности) и стоимость перехода на новое программное обеспечение (включая возможные проблемы с продуктами неизвестных производителей). Точно так же оценивается и целесообразность постановки "заплат", предоставляемых поставщиком, но с учетом того обстоятельства, что заплаты к системе безопасности, как правило, закрывают действительно серьезные дыры.

Невозможно переоценить важность хорошей стратегии резервного копирования. Резервные копии, особенно ежедневные, могут быть полезны, помимо прочего, и для прослеживания действий злоумышленников. Анализируя старые копии, нетрудно выяснить, когда система была скомпрометирована в первый раз. Резервные копии - это и материал для правоохранительных органов.

Ресурсы для предупреждения нарушений безопасности

Конфиденциальность, т. е. обеспечение скрытности или секретности, - одна из главных практических целей информационной безопасности.

Как правило, с информацией могут несанкционированно ознакомиться в трех местах:

- там, где она хранится (на компьютерных системах);
- там, где она передается (в сети);
- там, где хранятся резервные копии.

В первом случае для защиты используются права доступа к файлам, списки управления доступом и/или аналогичные механизмы. В последнем возможно физическое ограничение доступа. И во всех случаях помощь способны оказать криптографические средства.

Обычно мы принимаем на веру, что в заголовке электронного сообщения отправитель указан правильно. Заголовок, однако, нетрудно подделать. Аутентификация источника данных позволяет удостоверить подлинность отправителя сообщения или другого объекта.

Говорят, что информация находится в целостном состоянии, если она полна, корректна и не изменилась с момента последней проверки "цельности".

На целостность системной информации влияют многочисленные программно-технические и процедурные механизмы. Традиционные средства управления доступом обеспечивают контроль над тем, кто имеет доступ к системной информации. Необходимо также ограничение сетевого доступа. Дополнительно могут использоваться простые или криптографические контрольные суммы (имитовставки).

Широк спектр механизмов аутентификации. В простейшем случае в роли такового выступает системный администратор, заводящий новые пользовательские счета. На другом конце спектра находятся высокотехнологичные системы распознавания отпечатков пальцев и сканирования роговицы потенциальных пользователей. В некоторых системах для облегчения аутентификации применяются интеллектуальные карты. Здесь подлинность пользователя подтверждается обладанием определенным объектом.

Политика управления паролями важна для поддержания их секретности. Соответствующие процедуры могут варьироваться от эпизодических просьб или приказаний пользователю сменить пароль до активных попыток этот пароль подобрать с последующим информированием владельца о легкости выполнения данного действия. Другая часть политики управления описывает, кто может распространять пароли.

Некоторые системы программным образом вынуждают пользователей регулярно менять пароли. Компонентом многих из них является генератор паролей.

Конфигурационное управление, которое обычно применяют в процессе разработки программного обеспечения, полезно и на этапе эксплуатации. Поскольку довольно часто системные программы предназначены для проведения в жизнь политики безопасности, необходима уверенность в их корректности.

Конфигурационное управление разумно применять и к физическому конфигурированию аппаратуры.

Иногда (например, на экранирующих системах) для противостояния стандартным атакам полезно ввести в конфигурацию небольшие нестандартности, в число которых могут входить оригинальный алгоритм шифрования паролей, необычное расположение конфигурационных файлов, а также переписанные или функционально ограниченные системные команды.

Проверки безопасности (контроль защищенности) - важная часть функционирования любой компьютерной среды. Элементом таких проверок должна стать ревизия политики безопасности и защитных механизмов, используемых для ее реализации.

Периодически нужно проводить плановые учения, чтобы проверить, адекватны ли выбранные процедуры безопасности предполагаемым угрозам.

В процессе проверок необходимо с максимальной тщательностью подбирать тесты политики безопасности, четко определить, что тестируется, как проводится тестирование и какие результаты ожидаются. Все это нужно документировать, включить в основной текст политики безопасности или издать в качестве дополнения.

Важно протестировать все аспекты политики безопасности, процедурные и программно-технические, с упором на автоматизированные механизмы проведения политики в жизнь. Должна быть уверенность в полноте тестирования каждого средства защиты.

Реагирование на нарушения безопасности (процедурный уровень)

Традиционная информационная безопасность, как правило, концентрируется вокруг защиты от атак и, до некоторой степени, вокруг их обнаружения. Обычно почти не уделяют внимания мерам, предпринимаемым во время уже начавшейся атаки. В результате поспешных, непродуманных действий могут быть затруднены выявление причины инцидента, сбор улик для расследования, подготовка к восстановлению системы и защита ценной информации.

Враждебные акции, будь то нападение внешних злоумышленников или месть обиженного сотрудника, необходимо предусмотреть заранее. Ничто не может заменить предварительно составленного плана восстановительных работ.

В разделах политики безопасности, касающихся реакции на инциденты, должны быть освещены следующие темы:

- обзор (цели, преследуемые политикой безопасности в плане реакции на инциденты);
- оценка (насколько серьезно произошедшее событие);
- извещение (кого следует известить о нем);
- ответные меры (что следует предпринять в ответ);
- правовой аспект (каковы правовые последствия случившегося);
- регистрационная документация (что следует фиксировать до, во время и после инцидента).

Важно заранее определить приоритеты действий, совершаемых во время инцидента. Шкала приоритетов может выглядеть следующим образом:

- защита жизни и здоровья людей;
- защита секретных и/или критически важных данных;
- защита прочих данных, включая частную, научную и управленческую информацию;
- предотвращение повреждения систем; минимизация урона, нанесенного вычислительным ресурсам.

Идентификации инцидента сопутствует выяснение его масштабов и возможных последствий, а для эффективного противодействия важно правильно определить его границы. Кроме того, оценка возможных последствий позволит установить приоритеты при выделении ресурсов для принятия ответных мер.

Когда есть уверенность, что нарушение режима безопасности действительно имеет место, следует известить соответствующий персонал. Чтобы удержать события под контролем и с технической, и с эмоциональной точек зрения, очень важно, кто и как будет извещен.

Любое сообщение об инциденте должно быть внятным, любая фраза - ясной, точной и полной. Попытки скрыть отдельные моменты, сообщая ложную или неполную информацию, способны не только помешать принятию эффективных ответных мер, но и привести к ухудшению ситуации.

Меры, предпринимаемые для борьбы с нарушением, можно подразделить на основные категории:

- сдерживание ;
- ликвидация ;
- восстановление ;
- анализ.

Цель сдерживания - ограничить атакуемую область. Например, как можно быстрее приостановить распространение червя в сети.

Когда задача сдерживания решена, можно приступать к ликвидации. В этом поможет программный инструментарий (в частности, антивирусные пакеты).

После ликвидации атаки наступает время восстановления, т. е. приведения системы в нормальное состояние.

Следует предпринять по крайней мере следующие действия:

- произвести переучет системных активов, т. е. тщательно проверить состояние систем;
- отразить уроки, извлеченные из инцидента, в пересмотренной программе обеспечения безопасности, чтобы не допустить повторения аналогичного нарушения;
- произвести новый анализ риска с учетом полученной информации;
- начать следствие против виновников инцидента, если это признано необходимым.

Устранить все уязвимые места, сделавшие возможным нарушение режима безопасности, непросто, но необходимо. Ключевым моментом здесь является понимание механизма вторжения.

При восстановлении, возможно, придется вернуться к начальному состоянию системы с последующей ее настройкой. Чтобы облегчить действия даже в таком, наихудшем, случае, целесообразно хранить записи о начальных установках и обо всех внесенных изменениях.

Анализ - одна из самых важных стадий реакции на инциденты, о которой, тем не менее, почти всегда забывают. Она важна потому, что позволяет всем причастным лицам извлечь поучительные уроки, чтобы в будущем в аналогичных ситуациях действовать эффективнее.

Требуется получить ответы по крайней мере на следующие вопросы:

- Что именно и когда произошло?
- Насколько хорошо сработал персонал?
- Какая срочная информация понадобилась в первую очередь, и что способствовало ее скорейшему получению?
- Что в следующий раз нужно делать по-другому?

После восстановления системы в ней нередко остаются уязвимости или даже ловушки. На фазе анализа система должна быть тщательно обследована, чтобы выявить проблемы, упущенные при восстановлении. В качестве отправной точки разумно воспользоваться программными средствами контроля защищенности.

Целесообразно документировать все детали, связанные с инцидентом: способы его обнаружения, процедуры исправления ситуации, процедуры мониторинга и усвоенные уроки. Детальное документирование в конечном итоге ведет к экономии времени, позволяет оценить размер нанесенного ущерба.

Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности"

Рассматривается взаимодействие групп реагирования на нарушения информационной безопасности и опекаемого сообщества во время ликвидации нарушений; анализируются используемые при этом документы, правила и процедуры.

Основные понятия

Тема реагирования на нарушения информационной безопасности исключительно важна, но, на наш взгляд, она пока не получила достаточного освещения в отечественной литературе. Детальное рассмотрение спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности " [30] призвано отчасти восполнить этот пробел. В последующем изложении использована публикация [7] .

Цель интересующей нас спецификации - сформулировать ожидания Internet-сообщества по отношению к группам реагирования на нарушения информационной безопасности (Computer Security Incident Response Teams, CSIRTs). Потребители имеют законное право (и необходимость) досконально понимать правила и процедуры работы "своей" группы реагирования.

Словосочетание " группа реагирования на нарушения информационной безопасности" обозначает группу, выполняющую, координирующую и поддерживающую реагирование на нарушения, затрагивающие информационные системы в пределах определенной зоны ответственности.

Коллектив, называющий себя группой реагирования, обязан должным образом отвечать на выявленные нарушения безопасности и на угрозы своим подопечным, действуя в интересах конкретного сообщества и способами, принятыми в этом сообществе.

Чтобы считаться группой реагирования, необходимо:

- предоставлять защищенный канал для приема сообщений о предполагаемых нарушениях;
- помогать членам опекаемого сообщества в ликвидации нарушений;
- распространять информацию, относящуюся к нарушению, среди представителей опекаемого сообщества и других заинтересованных сторон.

Деятельность группы реагирования предполагает наличие опекаемого сообщества - группы пользователей, систем, сетей или организаций.

Существуют разные виды групп реагирования. Некоторые заботятся о безопасности весьма обширных сообществ. Так, Координационный центр CERT (Computer Emergency Response Team, см. ссылка: http://www.cert.org/) опекает Internet. У других масштабы деятельности не столь велики (например, группа DFN-CERT поддерживает немецкую исследовательскую сеть DFN, см. ссылка: http://www.cert.dfn.de/), у коммерческих или корпоративных групп реагирования они могут быть совсем небольшими. Группы реагирования и безопасности координируют свою работу на всемирном форуме - FIRST (Forum of Incident Response and Security Teams, см. ссылка: http://www.first.org/).

Под нарушением информационной безопасности понимается любой вид компрометации каких-либо аспектов безопасности систем и/или сетей, к их числу относятся:

- потеря конфиденциальности информации;
- нарушение целостности информации;
- нарушение доступности информационных услуг;
- неправомочное использование услуг, систем или информации;
- повреждение систем.

Атаки, даже если они оказались неудачными из-за правильно построенной защиты, могут трактоваться как нарушения.

Иногда администратор может лишь подозревать нарушение. В процессе реагирования необходимо установить, действительно ли оно имело место.

Важно, чтобы каждый член сообщества понимал, на что способна его группа, которая, в связи с этим, должна объяснить, кого она опекает и определить, какие услуги предоставляет. Кроме того, каждая группа реагирования обязана опубликовать свои правила и регламенты. Аналогично, членам сообщества нужно знать, чего ожидают от них, т. е. группа должна также ознакомить с правилами доклада о нарушениях.

Без активного участия пользователей эффективность работы групп реагирования может заметно снизиться, особенно это касается докладов о нарушениях. Пользователей необходимо уведомить, что о нарушениях информационной безопасности следует сообщать. Должны они знать и о том, как и куда направлять свои доклады.

Источники многих нарушений, затрагивающих внутренние системы, лежат за пределами контролируемого сообщества. С другой стороны, некоторые внутренние нарушения воздействуют на внешние системы. Расследование подобных инцидентов требует взаимодействия между отдельными системами и группами. Пользователи должны точно знать, как их группа будет сотрудничать с другими группами и организациями и какая информация будет разделяться.

Взаимодействие между группой реагирования, опекаемым сообществом и другими группами

Каждый пользователь услуг группы реагирования на нарушения информационной безопасности должен заранее, задолго до возникновения реального инцидента, узнать как можно больше об этих услугах и порядке взаимодействия с группой.

Ясное изложение правил и процедур помогает пользователям понять, как сообщать о нарушениях и какую поддержку ожидать. Окажет ли группа содействие в расследовании инцидента? Поможет ли она избежать подобных нарушений в будущем? Доскональное понимание ее возможностей и ограничений в предоставляемых услугах сделает взаимодействие между пользователями и группой более эффективным.

Целесообразно, чтобы каждая группа реагирования разместила рекомендации и процедуры на своем информационном сервере (например, на Web-сервере). Тем самым пользователи получат

свободный доступ к документам, хотя остается проблема поиска "своей" группы.

Независимо от источника, пользователь должен проверять аутентичность информации о группе. Настоятельно рекомендуется защищать подобные жизненно важные документы цифровой подписью, чтобы убедиться, что они на самом деле опубликованы определенной группой реагирования и их целостность не была нарушена.

В некоторых случаях группа реагирования может эффективно работать лишь в тесном взаимодействии с опекаемым сообществом. Но в условиях современных международных сетей гораздо более вероятно, что в большинство нарушений будут вовлечены третьи стороны.

Межгрупповое взаимодействие может включать в себя получение рекомендаций от других групп, распространение знаний о возникших проблемах, а также совместную работу по ликвидации нарушения, затронувшего одно или несколько опекаемых сообществ.

При установлении взаимоотношений, обеспечивающих подобное взаимодействие, группы должны решить, какого рода соглашения могут существовать между ними (например, как разделяется информация о защите, может ли раскрываться факт существования взаимоотношений, и если может, то перед кем).

После того как одна из сторон решила разделять информацию с другой либо две стороны заключили соглашение о разделении информации или совместной работе, как того требует скоординированная реакция на нарушение информационной безопасности, появляется необходимость в доверенных коммуникационных каналах.

Цели организации доверенных коммуникаций состоят в следующем:

- обеспечение конфиденциальности;
- обеспечение целостности;
- обеспечение аутентичности.

Важный фактор эффективной защиты - обеспечение аутентичности криптографических ключей, используемых в доверенных коммуникациях.

Коммуникации критичны для всех аспектов реагирования. Группа может действовать наилучшим образом, только собрав и систематизировав всю относящуюся к делу информацию. Специфические требования (в частности, звонок по определенному номеру для проверки аутентичности ключей) должны быть оговорены с самого начала.

Порядок публикации правил и процедур деятельности групп реагирования

Правила и процедуры группы реагирования должны быть опубликованы и доведены до пользователей. Рекомендуется следовать при этом определенному шаблону. Заполненный шаблон будем называть бланком. Как правило, он должен заверяться электронной подписью группы.

Далее мы поясним назначение некоторых полей шаблона и возможные способы их заполнения.

Любой документ должен начинаться с идентифицирующей информации, которую в данном случае составляют специальные требования:

- дата последнего изменения; она необходима для проверки актуальности сведений, поскольку детали работы группы со временем изменяются;
- список рассылки ; почтовые списки - удобное средство распространения обновлений среди большого числа пользователей, обычно в них перечислены коллективы, с которыми группа реагирования активно взаимодействует;
- расположение документа; текущая версия документа должна быть доступна в рамках оперативных информационных сервисов группы. В таком случае пользователи смогут легко получить дополнительную информацию о группе, проанализировать недавние изменения.

В следующем разделе бланков должна быть приведена исчерпывающая контактная информация:

- название группы реагирования;
- почтовый адрес;
- часовой пояс (эта информация полезна при реакции на нарушения, затрагивающие несколько часовых поясов);
- номер телефона;
- номер факса;
- адрес электронной почты;
- открытые ключи и способы шифрования; использование конкретных механизмов зависит от того, доступны ли партнерам по коммуникациям соответствующие программы, ключи и т.п. Наличие подобной информации дает возможность пользователям определить, способны ли они организовать защищенное взаимодействие с группой реагирования и каким образом это сделать;
- члены группы;
- часы работы.

Может быть представлена более детальная контактная информация, например, разные способы контакта для разных услуг, список оперативных информационных сервисов и т.п.

Каждая группа реагирования должна иметь устав, который определяет, что она должна делать и на каком основании. В уставе должны присутствовать по крайней мере следующие разделы:

- виды деятельности ;
- клиентура ;
- спонсоры и вышестоящие организации ;
- полномочия.

Определение клиентуры должно задать рамки, в пределах которых группа будет предоставлять свои услуги.

Сообщества пользователей могут пересекаться. Например, поставщик услуг Internet обеспечивает реагирование для своих потребителей, возможно, имеющих собственные группы.

Сведения о компаниях-спонсорах и вышестоящих организациях помогут пользователям выяснить возможности группы, что необходимо для

формирования доверительных отношений с клиентами.

Полномочия существенно зависят от специфики группы. Например, компетенция корпоративной группы определяется руководством, общественная группа может поддерживаться и выбираться на началах самоуправления, играть консультативную роль и т.п.

Не все группы наделяются правами на вмешательство в работу всех систем в пределах контролируемого периметра. Иными словами, область управления отличается от круга пользователей; в других случаях она может быть устроена иерархически, и тогда этот факт нужно зафиксировать с указанием подчиненных групп.

Описание полномочий группы может сделать ее уязвимой для судебных исков, поэтому в данном вопросе следует опираться на помощь юристов.

В рассматриваемой спецификации приводится пример устава для вымышленной группы реагирования XYZ-CERT университета XYZ.

Виды деятельности. Целью группы XYZ-CERT является помощь сотрудникам университета XYZ в реализации профилактических мер, снижающих риск нарушений информационной безопасности, и помощь в реагировании на все-таки произошедшие нарушения.

Клиентура. Опекаемое сообщество группы XYZ-CERT - сотрудники, студенты и аспиранты университета XYZ. Это определено в политике университета по отношению к вычислительным ресурсам, с ней можно ознакомиться по адресу `http://www.../policies/pcf.html`. Услуги группы распространяются только на производственные системы.

Спонсоры и вышестоящие организации. Спонсором группы XYZ-CERT является компания ACME Canadian Research Network, предлагающая свои услуги в Канаде и США в качестве вышестоящей организации для различных университетских групп реагирования, если они того пожелают.

Полномочия. Группа XYZ-CERT работает под покровительством и с полномочиями, делегированными отделом компьютерных услуг университета XYZ. Предполагается, что XYZ-CERT взаимодействует с

системными администраторами и пользователями университета XYZ и, по возможности, избегает авторитарных решений. Однако, под давлением обстоятельств, члены группы могут обратиться в отдел компьютерных услуг, чтобы "употребить власть". Все они входят в комитет системных администраторов и сполна наделены правами и обязанностями, полагающимися администраторам вычислительных ресурсов в соответствии с политикой, либо представлены в руководстве университета. Члены университетского сообщества, желающие обжаловать действия группы XYZ-CERT, должны обратиться к заместителю директора по техническим вопросам или в университетское бюро прав и обязанностей.

Описание правил группы реагирования

Критически важно, чтобы группа реагирования определила свои правила, которые регламентируют следующие аспекты:

- типы нарушений и уровень поддержки ;
- кооперация, взаимодействие и раскрытие информации ;
- коммуникации и аутентификация.

Должны быть специфицированы типы нарушений, на которые группа способна реагировать, а также уровень поддержки, предоставляемой для каждого из заданных типов.

Уровень поддержки может меняться в зависимости от таких факторов, как загруженность группы и полнота доступной информации. Подобные факторы должны быть описаны, а их влияние разъяснено. Поскольку список известных типов нарушений нельзя составить в исчерпывающей полноте по отношению ко всем возможным или будущим инцидентам, необходимо описать поддержку для "прочих" нарушений.

Следует определить, будет ли группа действовать на основе получаемой информации об уязвимостях, которые делают возможными будущие нарушения. Согласие учитывать такую информацию в интересах своих пользователей рассматривается как дополнительная профилактическая услуга, а не как обязательный сервис.

По поводу кооперации, взаимодействия и раскрытия информации

необходимо проинформировать пользователей, с какими родственными группами налажено взаимодействие.

Правила докладов и раскрытия информации должны разъяснять, кто и в каких случаях имеет право получать доклады группы, предполагается ли работа силами другой группы или непосредственное взаимодействие с членом другого сообщества по вопросам, касающимся именно этого пользователя.

Необходимость взаимодействия с другими группами реагирования возникает часто. Например, корпоративная группа сообщает о нарушении национальной группе, которая, в свою очередь, передает доклад в другие страны, чтобы охватить все информационные системы, ставшие жертвами широкомасштабной атаки.

У некоторых поставщиков есть собственные группы реагирования, у других нет. В последнем случае группа должна работать непосредственно с поставщиком, чтобы предложить улучшения или изменения, проанализировать техническую проблему или протестировать предлагаемые решения. Если продукты поставщика оказываются вовлеченными в нарушение, он играет особую роль в реагировании.

Группы реагирования и пользователи должны соблюдать действующее законодательство, которое существенно различается в разных странах. Группа реагирования может давать рекомендации по техническим деталям атаки или запрашивать совета по правовым последствиям нарушения. В законодательстве нередко содержатся специфические требования к предоставлению докладов и соблюдению конфиденциальности.

Время от времени от прессы поступают запросы на информацию и комментарии. Явные правила, касающиеся передачи информации такого рода, весьма полезны; они должны разъяснять все вопросы как можно подробнее, поскольку пользователи весьма болезненно воспринимают контакты с журналистами.

Подразумеваемый статус любых сведений, получаемых группой и имеющих отношение к информационной безопасности, - "конфиденциально", однако, строгое следование этому положению

превращает группу в информационную "черную дыру", что может уменьшить ее привлекательность как партнера для пользователей и других организаций. Необходимо определить, что именно докладывается или раскрывается, кому и когда.

Возможно, разные группы будут являться субъектами разного законодательства, требующего раскрытия информации или, напротив, ограничивающего его, особенно, если речь идет о группах из разных стран. Кроме того, они могут руководствоваться требованиями на доклады, налагаемыми спонсорскими организациями. Все такие ограничения должны быть специфицированы, чтобы прояснить ситуацию для пользователей и других групп.

Необходимо иметь политику, определяющую методы защиты и контроля коммуникаций. Это важно для взаимодействия как между группами, так и между группой и пользователями. В дополнение к максимально полному шифрованию критичной информации ее следует снабжать цифровой подписью.

Для упомянутой выше вымышленной группы реагирования XYZ-CERT определены специальные правила.

Типы нарушений и уровень поддержки. Группа XYZ-CERT уполномочена заниматься всеми видами нарушений безопасности, а также угрозами нарушений в университете XYZ.

Уровень поддержки, предоставляемой группой XYZ-CERT, зависит от типа и серьезности нападения, типа опекаемого сообщества, числа пострадавших, а также от количества наличных ресурсов, хотя в любом случае некоторый ресурс в течение рабочего дня будет выделен. Ресурсы выделяются в соответствии со следующими приоритетами, перечисленными по убыванию:

- угрозы физической безопасности людей;
- атаки на уровне суперпользователя или системном уровне на любую административную информационную систему или часть инфраструктуры магистральной сети;
- атаки на уровне суперпользователя или системном уровне на любую машину, предоставляющую крупный сервис,

многопользовательский или специализированный;
- компрометация конфиденциальных счетов пользователей на сервисах ограниченного доступа или компрометация установок программного обеспечения, особенно тех, что используются администраторами и приложениями, работающими с конфиденциальными данными;
- атака на доступность сервисов, перечисленных в предыдущем пункте;
- любое из перечисленных выше нападений, направленных на другие системы и исходящих из университета XYZ;
- масштабные атаки любого типа, например: перехват пакетов, атаки в IRC путем морально-психологического воздействия, атаки на пароли;
- угрозы, причинение беспокойства и другие противоправные действия, направленные на отдельных пользователей;
- компрометация отдельных счетов пользователей в многопользовательских системах;
- компрометация настольных систем;
- подделка, неправильное представление и другие относящиеся к безопасности нарушения местных правил: подделка новостей и электронной почты, несанкционированное использование роботов IRC;
- атака на доступность отдельных счетов пользователей, в частности применение почтовых бомб.

Типы нарушений, не перечисленные выше, получают приоритет в соответствии со своей наблюдаемой серьезностью и масштабом.

Непосредственная помощь конечным пользователям не предоставляется; предполагается, что они будут взаимодействовать со своим системным или сетевым администратором или уполномоченным по отделу. С этими сотрудниками XYZ-CERT и будет работать.

В группе понимают, что уровень подготовки системных администраторов в университете XYZ может быть очень разным. Группа XYZ-CERT намерена предоставлять информацию и помощь в форме, понятной всем, тем не менее, она не может повышать квалификацию администраторов "на лету", равно как и администрировать системы вместо них. В большинстве случаев

предоставляются ссылки на информацию, необходимую для принятия соответствующих мер.

Группа XYZ-CERT стремится информировать системных администраторов университета XYZ о потенциальных уязвимостях, по возможности до того, как их используют для нападений.

Кооперация, взаимодействие и раскрытие информации. Существуют законодательные и этические ограничения на раскрытие информации группой XYZ-CERT (многие из этих ограничений упомянуты в политике университета по отношению к вычислительным ресурсам; безусловно, все они будут соблюдаться), но группа подтверждает свою приверженность духу сотрудничества, создавшему Internet. Поэтому, принимая необходимые меры для сокрытия личной информации членов опекаемого сообщества и организаций-партнеров, группа, по возможности, станет свободно разделять информацию, если это целесообразно с точки зрения отражения или предупреждения нападений.

Далее в тексте под "пострадавшими сторонами" понимаются законные владельцы, операторы и пользователи вычислительных систем. В этот круг не входят неавторизованные пользователи, а также авторизованные пользователи, работающие с вычислительными системами неавторизованным образом; таким злоумышленникам не гарантируется сохранение конфиденциальности группой XYZ-CERT. Они могут иметь или не иметь законных прав на конфиденциальность; если такие права существуют, они, конечно, будут соблюдаться.

Информация, которая, возможно, будет распространяться, классифицируется следующим образом:

- персональные данные пользователей. Это информация о конкретных пользователях или, в некоторых случаях, о конкретных приложениях, которая должна считаться конфиденциальной по юридическим, контрактным и/или этическим причинам. Персональные данные пользователей не будут раскрываться в узнаваемой форме за пределами группы XYZ-CERT; исключения оговорены ниже. Если личность пользователя скрыта, информация может распространяться свободно;

- информация о злоумышленнике аналогична персональным данным пользователя, но относится к злоумышленнику. Хотя информацию о злоумышленнике (в частности, идентифицирующие данные) не сделают общедоступной (если только она уже не стала достоянием общественности, например, по причине возбуждения судебного преследования), ее будут свободно пересылать системным администраторам и группам реагирования, прослеживающим нарушение;
- информация о частной системе - это техническая информация о конкретных системах или организациях. Она не будет разглашаться без согласия соответствующих организаций. Исключения оговорены ниже;
- информация об уязвимостях - техническая информация об уязвимостях или атаках, включая исправления и сопутствующие меры. Она распространяется свободно, хотя и будут прилагаться все усилия, чтобы заинтересованный в ней поставщик получил ее раньше других;
- информация, бросающая тень, - сообщение о том, что нарушение имело место, а также сведения о его масштабе или серьезности. Не будет распространяться без разрешения соответствующих организаций или пользователей. Исключения оговорены ниже;
- статистическая информация - это информация, бросающая тень, снабженная удаленными идентифицирующими данными. Она распространяется по усмотрению отдела компьютерных услуг;
- контактная информация позволяет обратиться к системным администраторам и группам реагирования. Она будет распространяться свободно, если только контактное лицо или организация не попросит об обратном или если группа XYZ-CERT не решит, что такое распространение вызовет недовольство.

Потенциальные получатели информации от группы XYZ-CERT также отнесены к различным категориям:

- по роду своей деятельности, в том числе по соблюдению конфиденциальности, администраторы университета XYZ имеют право получать всю информацию, необходимую для эффективной реакции на нарушения безопасности, затрагивающие вверенные им системы;
- системные администраторы университета XYZ также, в силу

возложенных на них обязанностей, допущены к работе с конфиденциальной информацией. Однако, если эти лица не являются членами группы XYZ-CERT, они будут получать только те сведения, которые нужны им для проведения расследования или обеспечения безопасности вверенных им систем;

- пользователи университетских систем допущены к информации, которая касается безопасности их собственных компьютерных счетов, даже если это означает утечку "информации о злоумышленнике" или "информации, бросающей тень" на другого пользователя;
- университетское сообщество не будет получать никакой информации ограниченного распространения, если только стороны, затронутые нарушением, не дадут разрешения на распространение сведений. Статистическая информация может предоставляться общественности. Группа XYZ-CERT не считает себя обязанной информировать общественность о нарушениях, хотя и может делать это; в частности, вероятно, известит все заинтересованные стороны о том, каким образом они были атакованы, или одобрит распространение этими сторонами подобной информации;
- широкая общественность не получит никакой информации ограниченного распространения. На самом деле, к ней не будут обращаться, хотя группа XYZ-CERT понимает, что сведения, сообщенные университетскому сообществу, могут стать всеобщим достоянием;
- сообщество специалистов по информационной безопасности рассматривается наравне с широкой общественностью. Хотя члены группы XYZ-CERT могут принимать участие в дискуссиях в рамках этого сообщества, например, посредством телеконференций, списков рассылки (включая раскрывающий все детали список "bugtraq") и совещаний разного рода, они (члены группы) рассматривают такие форумы как обращение к широкой общественности. Хотя технические вопросы (в том числе уязвимости) могут обсуждаться сколь угодно подробно, все примеры, взятые из опыта группы XYZ-CERT, будут изменены, чтобы сделать невозможной идентификацию затронутых сторон;
- пресса также рассматривается как часть широкой общественности. Группа XYZ-CERT не будет вступать с ней в непосредственные контакты по поводу нарушений безопасности, если только речь не

идет о распространении сведений, уже ставших всеобщим достоянием;

- другие организации и группы реагирования, являющиеся партнерами в расследовании нарушения безопасности, в некоторых случаях допустят к конфиденциальной информации. При этом добропорядочность внешних организаций подлежит проверке, а передаваемая информация будет сводиться к минимуму, полезному для ликвидации нарушения. Вероятнее всего, доступ к информации доверят организациям, хорошо известным группе XYZ-CERT;
- поставщики, как правило, рассматриваются XYZ-CERT наравне с внешними группами реагирования. Приветствуется желание поставщиков всех видов сетевого и компьютерного оборудования, программного обеспечения и услуг повышать безопасность своих продуктов. С этой целью им будет передаваться информация об уязвимостях, обнаруженных в их продуктах, вместе с техническими деталями, позволяющими идентифицировать и ликвидировать проблему;
- правоохранительные органы получат от группы XYZ-CERT всю информацию, необходимую для проведения расследования, в соответствии с политикой по отношению к вычислительным ресурсам.

Коммуникации и аутентификация. Проанализировав типы информации, с которой имеет дело группа XYZ-CERT, можно сделать вывод, что телефоны без средств шифрования можно считать достаточно безопасными. Нешифрованная электронная почта не особенно защищена, однако ее можно использовать для передачи данных низкой степени критичности.

Если по электронной почте нужно передать критичные данные, будет применяться PGP. С точки зрения безопасности, передача файлов по сети рассматривается наравне с электронной почтой: критичные данные должны шифроваться.

Когда необходимо получить уверенность в подлинности партнера, например, перед началом действий на основе информации, предоставленной группе XYZ-CERT, или перед раскрытием конфиденциальной информации, с высокой степенью надежности будет

проверяться его личность и репутация.

Описание услуг группы реагирования

Услуги, оказываемые группой реагирования, можно разделить на две категории:

- действия в реальном времени, непосредственно связанные с главной задачей - реагированием на нарушения;
- профилактические действия, играющие вспомогательную роль и осуществляемые не в реальном масштабе времени.

Вторая категория и часть первой состоит из услуг, которые являются дополнительными в том смысле, что их предлагают не все группы реагирования.

Реагирование на нарушения обычно включает оценку входящих докладов ("классификация нарушений") и работу над поступившей информацией вместе с другими группами, поставщиками услуг Internet и иными организациями ("координация реагирования"). Третья группа услуг - помощь локальным пользователям в восстановлении нормальной работы после нарушения ("разрешение проблем") - обычно состоит из дополнительных сервисов, предоставляемых лишь частью групп.

Классификация нарушений обычно включает в себя следующие действия:

- оценка докладов: входящая информация интерпретируется, классифицируется по степени важности, соотносится с продолжающимися событиями и выявляемыми тенденциями;
- верификация ; определяется, действительно ли имеет место нарушение и каковы его масштабы.

Под координаций реагирования обычно понимается:

- категорирование информации: информация, относящаяся к нарушению (регистрационные журналы, контактная информация

и т.д.) категорируется согласно политике раскрытия сведений;
- координация: в соответствии с политикой раскрытия сведений о нарушении извещаются другие стороны.

Перечислим действия, предоставляемые в рамках услуг по разрешению проблем:

- техническая поддержка (например, анализ "взломанных" систем);
- искоренение проблем: устранение причин нарушения (использованных уязвимостей) и его проявлений (например, прерывание сеанса пользователя-нарушителя);
- восстановление: помощь в возвращении систем и услуг к состоянию, имевшему место до нарушения безопасности.

В профилактические действия входят:

- предоставление информации. Под этим понимается поддержка архива известных уязвимостей, заплат, способов разрешения прошлых проблем или организация списков рассылки с рекомендательными целями; предоставление средств безопасности (например, средств аудита);
- обучение и подготовка кадров ;
- оценка продуктов ;
- оценка защищенности организации, консультационные услуги.

Еще один важный момент - использование форм для докладов о нарушениях. Оно упрощает работу как пользователей, так и групп реагирования. Пользователи могут заготовить ответы на некоторые важные вопросы заранее, в спокойной обстановке. Группа сразу, в первом сообщении, получает всю необходимую информацию, что закладывает основу эффективного реагирования.

В зависимости от целей и набора услуг конкретной группы, может использоваться несколько форм. Например, форма для сообщения о новой уязвимости может существенно отличаться от доклада о нарушении. Лучше всего предоставлять формы в рамках оперативных информационных услуг группы. Точные ссылки на них должны присутствовать в документах, описывающих группу, вместе с перечнем

правил пользования и руководством по порядку работы с формами. Если для "докладов по форме" поддерживаются отдельные адреса электронной почты, они также должны быть указаны.

Один из примеров - форма для доклада о нарушениях координационного центра CERT, представленная на Web-сервере ссылка: http://www.cert.org/.

Документы, описывающие группу реагирования, не являются контрактом, но возможность последующих судебных санкций может вытекать из описания услуг и целей. По этой причине рекомендуется размещать в конце бланков соответствующий отвод (письменный отказ), предупреждающий пользователей о возможных ограничениях.

Группа XYZ-CERT предоставляет соответствующие задачам услуги.

Реагирование на нарушения. XYZ-CERT помогает системным администраторам в технических и организационных аспектах реагирования на нарушения. В частности, оказывается помощь или даются советы о следующих аспектах реагирования:

1. Классификация нарушений:
    - выяснение того, действительно ли имеет место нарушение;
    - определение масштаба нарушения.
2. Координация реагирования:
    - выяснение первоначальной причины нарушения (использованной уязвимости);
    - облегчение контактов с другими системами, возможно, затронутыми нарушением;
    - облегчение контактов со службой безопасности университета XYZ и/или правоохранительными органами, если это необходимо;
    - предоставление отчетов другим группам реагирования;
    - составление уведомлений для пользователей, если это необходимо.
3. Разрешение проблем:
    - устранение уязвимостей;
    - ликвидация последствий нарушения;
    - оценка возможных дополнительных действий с учетом их

стоимости и риска (например, исчерпывающее расследование или дисциплинарные действия: сбор улик после нарушения, накопление информации во время инцидента, установка ловушек для злоумышленников и т.п.);
- возможный сбор улик для судебного преследования или дисциплинарных акций.

Кроме того, группа XYZ-CERT накапливает статистическую информацию о нарушениях, затрагивающих университетское сообщество, и, при необходимости, информирует сообщество, помогая ему защититься от известных атак.

Чтобы воспользоваться услугами группы XYZ-CERT по реагированию на нарушения, следует направить электронное письмо по контактному адресу.

Профилактические действия. Группа XYZ-CERT координирует и предоставляет следующие услуги в объеме, возможно, зависящем от наличия ресурсов:

1. Информационное обслуживание:
   - список контактных координат уполномоченных лиц по безопасности в отделах (административных и технических). Эти списки общедоступны по таким каналам, как Web;
   - списки рассылки для информирования уполномоченных лиц о появлении новой информации, относящейся к их компьютерной среде, которые доступны только для системных администраторов университета XYZ;
   - хранилище защитных заплат, распространяемых поставщиками или источниками, для различных операционных систем. Хранилище общедоступно, если это позволяют лицензионные соглашения. Доступ к нему предоставляется по обычным каналам - Web и/или ftp;
   - хранилище защитного инструментария и документации для использования системными администраторами. По возможности предоставляются предварительно скомпилированные версии, готовые к установке. Как обычно, доступ предоставляется через Web или ftp;
   - подготовка краткого изложения инцидента для различных

информационных ресурсов, включая основные списки рассылки и телеконференции. Результирующие аннотации распространяются через списки рассылки с ограниченным доступом или через Web, в зависимости от критичности и срочности информации.

2. Повышение квалификации:
    - члены группы XYZ-CERT периодически проводят семинары по различным аспектам информационной безопасности; системные администраторы университета XYZ приглашаются на эти занятия.
3. Аудит безопасности:
    - проверка целостности основных файлов;
    - присвоение уровней безопасности. Машины и подсети в университете XYZ проверяются на предмет присвоения им уровня безопасности. Информация об уровнях доступна университетскому сообществу, чтобы упростить установку соответствующих прав доступа;
    - централизованное протоколирование для машин, поддерживающих удаленное протоколирование в Unix-стиле. Регистрационные журналы автоматически просматриваются анализирующей программой, а события или тенденции, указывающие на потенциальные проблемы безопасности, доводятся до сведения соответствующих системных администраторов; - сохранение записей о нарушениях безопасности. Хотя эти записи остаются конфиденциальными, периодически готовятся и распространяются статистические отчеты.

Детальное описание перечисленных выше услуг вместе с инструкциями по присоединению к спискам рассылки, скачиванию информации или получению таких услуг, как централизованное протоколирование или проверка целостности файлов, доступны через Web-сервер группы XYZ-CERT.

На этом мы завершаем рассмотрение спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности ".

Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг"

Данная спецификация важна с точки зрения формирования организационной и архитектурной безопасности, на которой базируются прочие меры процедурного и программно-технического уровней.

Общие положения

Полное название рассматриваемой спецификации (точнее, проекта спецификации) [37] - "Дополнение к Руководству по информационной безопасности предприятия: Как выбирать поставщика Интернет-услуг ". Далее, для краткости, мы будем называть ее "Дополнением к Руководству" или просто Дополнением. Напомним, что "Руководство по информационной безопасности предприятия" было рассмотрено нами ранее. При изложении Дополнения мы опираемся на публикацию [22].

"Дополнение к Руководству" призвано помочь в выработке политики и процедур безопасности в организациях, информационные системы которых подключены к Internet, а также служить для потребителей контрольным перечнем при обсуждении вопросов информационной безопасности с поставщиками Internet-услуг. В данном документе выделено три типа потребителей:

- потребители коммуникационных услуг;
- потребители услуг по размещению ресурсов;
- потребители, разместившиеся там же, где и поставщики услуг.

Еще одна цель Дополнения состоит в том, чтобы, информируя поставщиков Internet-услуг об ожиданиях общественности, побудить их принять упреждающие меры, сделав безопасность одним из приоритетных направлений развития.

Поставщик Internet-услуг определяется как организация, обеспечивающая для других подключение к Internet, а также иные Internet-услуги, в том числе размещение Web-серверов, поставку информационного наполнения, услуги электронной почты и т.д.

Вероятно, для многих привычнее называть такого поставщика Internet-провайдером; мы не стали этого делать, поскольку тогда, по соображениям концептуальной целостности, потребителя пришлось бы именовать Internet-консьюмером, а этот термин пока не прижился.

Роль поставщика Internet-услуг в реагировании на нарушения безопасности

Мы уже обсуждали тему реагирования на нарушения информационной безопасности и взаимодействие групп реагирования с опекаемым сообществом. Затронута она и в Дополнении.

Независимо от того, есть ли у поставщика Internet-услуг группа реагирования, он должен определить и довести до потребителей порядок передачи и обработки докладов о нарушениях, а также документировать собственные возможности по реагированию.

У некоторых поставщиков есть группы реагирования на нарушения информационной безопасности, однако даже в этом случае помощь часто предоставляется в качестве дополнительно оплачиваемой услуги, а группа включает в зону своей ответственности только тех, кто специально на нее подписался.

Если группы реагирования нет, поставщику следует определить, какую роль он возьмет на себя (если возьмет вообще) при реагировании на нарушение, и существует ли группа, ответственность которой распространяется на потребителя, чтобы направлять ей доклады о нарушениях.

Поставщику Internet-услуг следует иметь специальные почтовые ящики: SECURITY - для сообщений о нарушениях безопасности, ABUSE - для сообщений о ненадлежащем поведении и NOC - для сообщений о проблемах в сетевой инфраструктуре.

Когда происходит нарушение информационной безопасности, затрагивающее инфраструктуру поставщика, необходимо немедленно сообщить потребителям такие сведения:

- кто координирует реакцию на нарушение;

- какая уязвимость использована атакующим;
- как нарушение сказалось на предоставляемых услугах;
- что делается для реагирования на нарушение ;
- могут ли быть скомпрометированы данные потребителей ;
- какие действия предпринимаются для устранения выявленной уязвимости ;
- предполагаемый график реагирования, если он может быть составлен.

Если имеет место нарушение, направленное на какого-либо потребителя услуг подключения, поставщик Internet-услуг должен проинформировать его об атаке и, по возможности, оказать помощь в следующем:

- проследить видимый источник атаки и попытаться определить достоверность каждого шага на этом маршруте. Если исходный адрес подделан, поставщик может определить точку в своей сети, через которую поступает поток данных злоумышленника;
- получить контактную информацию источника атаки ;
- собрать и защитить свидетельства нарушения, предохраняя их от уничтожения или непреднамеренного разглашения.

В случае продолжения нарушения поставщик Internet-услуг, по запросу потребителя, может оказать помощь путем протоколирования с целью дальнейшей диагностики проблемы или посредством фильтрации определенных видов трафика.

Если окажется, что источником нарушения информационной безопасности является кто-то из потребителей, поставщик может помочь администраторам источника и цели атаки, вступив с нарушителем в контакт и переслав им контактную информацию для связи с пострадавшими.

К поставщику могут также обратиться за помощью в случае атак, которые проходят через его сеть, но используют поддельные исходные адреса. Поддержка возможна в предоставлении сетевой регистрационной информации, генерируемой маршрутизаторами, чтобы найти точку, в которой поток данных с поддельными адресами вошел в сеть поставщика. При прослеживании источника подобных

атак требуется координация усилий со смежными поставщиками.

Поставщикам Internet-услуг следует иметь правила и процедуры, касающиеся разделения информации о нарушении безопасности со своими потребителями, с другими поставщиками или группами реагирования, с правоохранительными органами, средствами массовой информации и общественностью. Понадобятся средства для организации доверенного канала с целью передачи подобной информации.

Меры по защите Internet-сообщества

Поставщики Internet-услуг играют критически важную роль в повышении безопасности Internet.

Каждому из них следует иметь политику добропорядочного пользования, с учетом которой составляется контракт с потребителем. В политике определяются права потребителей на те или иные действия в разных частях сети и на разных системах.

Во многих странах есть законы о защите данных. В ситуациях, когда они применимы, поставщики должны проанализировать характер поступающих к ним персональных данных и, если нужно, принять меры, препятствующие их противозаконному использованию. Учитывая глобальный характер Internet, поставщикам Internet-услуг, действующим в странах, где таких законов нет, необходимо хотя бы ознакомиться с идеей защиты данных.

Важно, чтобы штат поставщика постоянно помнил о проблемах информационной безопасности, с пониманием подходил к их решению, умел должным образом применять средства повышения безопасности. К числу наиболее значимых принадлежат вопросы использования доверенных каналов для передачи конфиденциальной информации, управления аутентификационными данными и т.д.

Поставщики Internet-услуг ответственны за такое управление сетевой инфраструктурой Internet, чтобы обеспечивалась устойчивость к появлению уязвимостей, а атакующие не могли легко организовать плацдарм для последующих атак.

Ключевой элемент сетевой инфраструктуры - маршрутизаторы. К сожалению, они не только сами по себе являются притягательными целями атак на безопасность, но и представляют собой отличный плацдарм для организации нападений на другие цели.

Многие маршрутизаторы позволяют злоумышленникам совершать опасные действия, например:

- "прослушивать" транзитные потоки данных;
- манипулировать таблицами маршрутизации для перенаправления потоков данных;
- изменять состояние интерфейсов с целью нарушения обслуживания;
- вызывать "трепыхание" маршрутных таблиц, чреватое отказом в обслуживании для крупных частей Internet;
- создавать пакеты с поддельными адресами и любым желаемым набором флагов;
- порождать штормы ICMP-пакетов, устраивать другие атаки на доступность ;
- отправлять потоки данных в "черную дыру";
- скрывать обращения по внешним адресам, что облегчается недостаточным протоколированием в маршрутизаторах.

Доступ к маршрутизаторам следует основывать на одноразовых паролях или еще более сильных средствах и ограничивать в максимально возможной степени. Обращения к маршрутизатору - протоколировать, привлекая ресурсы других систем.

Сеансы взаимодействия с маршрутизаторами подлежат шифровке для предотвращения краж сеансов или данных и для недопущения атак, основанных на воспроизведении трафика.

На маршрутизаторы нельзя возлагать выполнение мелких услуг, которые нередко включены по умолчанию.

Поставщики Internet-услуг должны быть столь же бдительными при конфигурировании всех видов сетевого оборудования, по возможности ограничивая доступ к сетевому оборудованию, предоставляя его только уполномоченным сетевым администраторам.

Конфигурационную информацию маршрутизаторов и коммутаторов следует сопровождать на файловом сервере.

Производители предлагают много сетевых устройств - от недорогих маршрутизаторов до принтеров, - принимающих соединения по протоколу telnet без запроса пароля. Если в сети поставщика Internet-услуг есть такое оборудование, доступ к нему следует ограничить. Кроме того, потребителям необходимо рекомендовать блокировать доступ к подобным устройствам из внешних сетей. Крайне нежелательно использовать протокол telnet для управления компонентами сети.

Центр управления сетью (ЦУС) является критически важной частью инфраструктуры поставщика Internet-услуг, поэтому его работу следует строить с соблюдением должных мер безопасности.

ЦУС располагает административным контролем над конфигурационными данными сетевого оборудования и обязан ограничить доступ к такой информации.

Как правило, ЦУС выполняет функции мониторинга сети, периодически опрашивая множество сетевых устройств. Помимо простого опроса, для взаимодействия с сетевыми устройствами ЦУС может использовать управляющий протокол, в частности SNMP. Обычно с его помощью выясняют значения различных переменных, например, число пакетов, принятых через определенный интерфейс. Однако протокол может применяться и для установки переменных, возможно, с далеко идущими последствиями (к примеру, переконфигурирование устройства). В любом случае, в SNMPv1 присутствует только тривиальная аутентификация. По возможности, к SNMP следует прибегать только как к средству получения информации от удаленных устройств, трактуя ее как конфиденциальную.

Еще одно применение протокола SNMP состоит в уведомлении управляющей станции о возникновении исключительных ситуаций. Такую информацию также необходимо считать конфиденциальной и проявить осторожность, чтобы SNMP-сообщения сами по себе не вылились в атаку на доступность.

В плане физической защиты наибольший интерес представляет ситуация, когда оборудование потребителей располагается на площадке

поставщика Internet-услуг. В идеале каждый потребитель должен получить полностью закрытую, запирающуюся "клетку", т. е. небольшое помещение со стенами и проемами для прокладки множества кабелей, а также со стойками для монтажа оборудования. Потребители проходят туда в сопровождении сотрудника поставщика (либо получают ключи только от своей комнаты).

Выделение отдельных комнат, однако, может оказаться слишком накладным, поэтому многие поставщики идут на компромисс, собирая "чужое" оборудование в одном машинном зале и тщательно контролируя все, что в нем происходит. К сожалению, этого может оказаться недостаточно, чтобы избежать таких недоразумений, как нечаянное отключение оборудования другого потребителя. Вместо единого открытого пространства следует разделить зал перегородками и предоставлять каждому потребителю отдельное помещение с запирающейся дверью.

Вблизи чужого оборудования никого нельзя оставлять без присмотра. Такое оборудование запрещается трогать, фотографировать или исследовать.

Надо помнить также о безопасности на втором уровне семиуровневой модели, запрещая разделение физического сегмента сети между оборудованием потребителя и компьютерами, принадлежащими другим потребителям или поставщику Internet-услуг. Нередки случаи, когда злоумышленники пользуются уязвимостями или незашифрованными удаленными входами в оборудование потребителя, получают контроль над этими устройствами, переводят его в режим прослушивания сегмента локальной сети, потенциально нарушая тем самым конфиденциальность или безопасность других устройств в этом сегменте.

Вопросы безопасности чрезвычайно важны и тогда, когда компоненты сетевой инфраструктуры поставщика Internet-услуг размещены вне его территории (например, у партнера или в удаленной точке присутствия). Такие компоненты нередко являются жизненно важными с точки зрения топологии сети и, в то же время, могут стать объектом атаки или пострадать от несчастного случая. Для ограничения физического доступа оборудование в идеальном случае следует размещать в

полностью закрытых, запирающихся комнатах или "клетках". Если на чужой площади хранятся запчасти, их также следует защищать от кражи, порчи или встраивания "жучков". По возможности необходимо использовать системы безопасности и замки, открывающиеся персональными картами. Удаленные компоненты нужно периодически проверять на предмет встраивания постороннего оборудования, которое может использоваться для прослушивания сетевых соединений. Как и на других площадках, компьютеры не следует подключать к транзитным сегментам или допускать подсоединение к сети неиспользуемых физических интерфейсов.

Маршрутизация, фильтрация и ограничение вещания

Способность поставщика Internet-услуг направлять потоки данных к правильному конечному пункту зависит от правил маршрутизации, заданных в виде маршрутных таблиц. Поставщики должны убедиться, что находящаяся в их ведении маршрутная информация может быть изменена только после надежной аутентификации и что права на внесение изменений должным образом ограничены.

В граничных маршрутизаторах следует аутентифицировать соседей в рамках протокола BGP.

При выборе протоколов внутренней маршрутизации нельзя забывать о безопасности. В случае изменения маршрутов необходимо обратиться к наивысшему уровню аутентификации, поддерживаемому протоколом внутренней маршрутизации.

Нередко атакующие скрывают следы, подделывая исходные адреса. Чтобы отвлечь внимание от своей системы, в качестве исходного они выбирают адрес невинной удаленной системы. Кроме того, поддельные исходные адреса часто встречаются в атаках, основанных на использовании отношения доверия между узлами сети.

Чтобы уменьшить область распространения подобных атак, поставщики Internet-услуг должны применять входную фильтрацию потоков данных, т. е. фильтрацию в направлении от периферийной системы (потребитель) к Internet (см. рис. 14.1). Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу

отфильтровывать идущие от них сетевые пакеты и имеющие исходные адреса, отличные от выделенных данным потребителям.

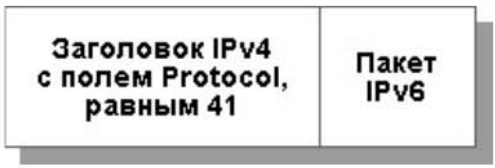

Рис. 14.1. Входная фильтрация IP-пакетов по исходным адресам.

Дополнительной мерой защиты потребителей от атак, основанных на подделке исходных адресов, является выходная фильтрация - от сети Internet к периферийной системе (см. рис. 14.2). Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу отфильтровывать потоки данных, идущие к потребителю и имеющие исходные адреса из выделенного ему пространства.

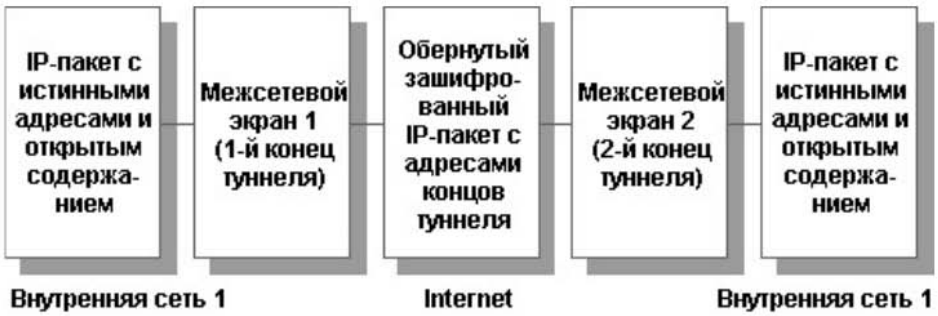

Рис. 14.2. Выходная фильтрация IP-пакетов по исходным адресам.

Иногда возникают ситуации, когда фильтрация оказывается невозможной. Например, большой агрегирующий маршрутизатор не выдерживает дополнительной нагрузки, вызванной применением пакетных фильтров. Кроме того, входная фильтрация способна привести к трудностям для мобильных пользователей. Следовательно, хотя данный метод для борьбы с подделкой адресов настоятельно рекомендуется, им не всегда удается воспользоваться.

В тех редких случаях, когда фильтрация на стыке потребителя и поставщика Internet-услуг невозможна, следует рекомендовать потребителю организовать фильтрацию внутри его сети.

Злоумышленники могут прибегнуть к избыточным изменениям маршрутной информации как к средству увеличения загрузки, на базе которого развивается атака на доступность. По меньшей мере это приведет к деградации производительности. Поставщикам Internet-услуг следует отфильтровывать поступающие объявления о маршрутах, игнорируя, например, маршруты к адресам для частных объединений сетей, избегая фиктивных маршрутов и реализуя политику расщепления и агрегирования маршрутов.

Поставщики Internet-услуг должны применять методы, уменьшающие риск нарастания нагрузки на маршрутизаторы в других частях сети. Следует отфильтровывать "кустарные" маршруты, настойчивое агрегирование и расщепление маршрутов.

Протокол IP поддерживает направленное вещание (посылку) через сеть пакетов, которые в определенной подсети станут широковещательными. Практической пользы от такой возможности немного, зато на ней основываются несколько различных видов атак (в первую очередь, это атаки на доступность, использующие эффект размножения широковещательных пакетов). Следовательно, маршрутизаторы, подключенные к вещательной среде, не следует конфигурировать так, чтобы было возможным непосредственное вещание на эту среду.

Защита системной инфраструктуры

То, как поставщик услуг управляет своими системами, критически важно для безопасности и надежного функционирования сети. Нарушения в работе систем могут в лучшем случае привести к снижению производительности или функциональности, но способны также вызвать потерю данных или сделать возможным перехват сетевого трафика (не исключена и последующая атака методом "нелегального посредника").

В общедоступном месте, например, на Web-сервере поставщика услуг, следует опубликовать его политику по отношению к защите персональных данных, обеспечению аутентичности, подотчетности, наложению защитных заплат, поддержке доступности, реагированию на доклады о нарушениях.

Предоставление разных услуг следует возлагать на разные системы. Кроме выгод от облегчения системного администрирования можно сослаться на многократно проверенный факт, что при таком подходе гораздо проще построить защищенную систему.

Все услуги выиграют от организации надежной защиты на сетевом уровне средствами IPsec.

Доступ ко всем системам поставщика, выполняющим критически важные функции (среди которых - почта, телеконференции и размещение Web-серверов), следует ограничить, разрешая его только администраторам соответствующих услуг, предоставлять после надежной аутентификации и осуществлять по доверенному каналу. Доступными из внешних сетей должны быть только те порты, на которых ожидают подключения уже востребованные услуги.

Если распространение и обновление программного обеспечения производится с помощью автоматизированных средств, им выделяется доверенный канал. Целостность ПО необходимо гарантировать путем вычисления и распространения вместе с ПО криптографических контрольных сумм.

Регистрационная информация должна быть доступна на чтение только системному администратору.

Если поставщик услуг ведет учет работы потребителей, то системы, обеспечивающие этот учет, изолируются от остальной части сети.

Нельзя подключать системы к транзитным сегментам.

Резервное копирование может являться слабым звеном в системной безопасности, если защита резервных носителей не налажена должным образом. При копировании по сети следует пользоваться доверенным каналом. Если в процессе резервного копирования данные помещаются на промежуточные диски, то доступ к этим дискам ограничивается в максимально возможной степени.

Отслужившие срок носители должны уничтожаться, а не выбрасываться.

Пользователей систем и услуг необходимо информировать о том, что сохраняется на резервных копиях, а что нет.

Доменная система имен (DNS) играет критически важную роль в повседневной деятельности миллионов пользователей Internet. Поставщикам услуг при администрировании DNS-серверов следует обратить внимание на следующие аспекты:

- мониторинг: обязательный контроль доступности DNS (способности отвечать на запросы);
- синхронизация часов: синхронизация установленного на серверах времени с помощью протокола NTP с аутентификацией.

При конфигурировании почтовых серверов поставщики Internet-услуг должны руководствоваться такими положениями:

- по возможности использовать ПО с раздельными агентами приема/отправки и обработки, чтобы агент приема/отправки, взаимодействующий с удаленными почтовыми серверами, выполнялся с минимальными привилегиями ;
- ограничить запуск очередей по запросу (предоставляемый для удобства потребителей, получающих почту в своем домене и не имеющих постоянного соединения), желательно средствами надежной аутентификации;
- запретить предоставлять информацию о локальных пользователях или механизмах доставки, выходящую за рамки необходимого;
- выявлять исключительные ситуации (повторяющиеся неудачи аутентификации, зацикливание почты, ненормальная длина очереди) и генерировать соответствующие доклады.

Говорят, что почтовый SMTP-сервер функционирует в режиме "открытой" системы промежуточного хранения и пересылки почты, если он допускает прием и пересылку нелокальным адресатам таких сообщений, которые были порождены нелокально. Подобные открытые системы пересылки почты нередко используются "спамерами", организующими массовую незапрошенную рассылку с сокрытием инициатора. Только в весьма специфических обстоятельствах можно оправдать решение администратора сделать систему пересылки в Internet полностью открытой.

При конфигурировании серверов телеконференций (NNTP) поставщикам Internet-услуг необходимо соблюдать следующие требования:

- использовать ПО, устойчивое к вредоносным управляющим сообщениям и к переполнению буферов;
- освободить сервер телеконференций от выполнения каких-либо иных функций;
- если поддерживаются входящие пакеты статей, не подавать их на вход командного интерпретатора.

Размещение Web-серверов

Многие организации передают свои Web-серверы поставщикам Internet-услуг вместе с обязанностями по эксплуатации и администрированию, исходя, главным образом, из соображений информационной безопасности.

Помимо перечисленных выше аспектов, поставщики услуг при администрировании оборудования, на котором размещены Web-серверы, должны руководствоваться такими положениями:

- разумное использование DNS. В момент подключения клиента не следует выполнять поиск его имени, поскольку это делает Web-серверы уязвимыми для атак на доступность и заметно сказывается на производительности;
- минимизация привилегий. Web-демон следует выполнять от имени пользователя и группы, специально выделенных для этой цели и имеющих минимальные привилегии. Ответственный за информационное наполнение Web-сервера должен работать от имени другого пользователя;
- контроль DocumentRoot. Все, что располагается ниже этого каталога, надо тщательнейшим образом проконтролировать. Желательно использовать системный вызов chroot для смены корневого каталога HTTP-демона;
- контроль UserDir. На сервере нельзя регистрировать других пользователей, кроме администраторов. Если такие пользователи все-таки есть, директиве "UserDir" (в случае ее разрешения) не следует предоставлять доступ к информации пользователей - в

частности, не разрешать выполнение командных процедур от имени этих пользователей;

- разбиение на виртуальные серверы. Единый сервер, на котором размещено множество серверов (виртуальных доменов), необходимо организовать так, чтобы все данные, программы и регистрационные журналы различных виртуальных серверов были отделены друг от друга и чтобы доступ к "чужой" конфигурации или данным был невозможен. Кроме того, надо исключить доступ к данным или программам на сервере одного потребителя через локатор ресурсов, в хостовой части которого указано имя сервера другого потребителя ;
- управление доступом. Следует сделать возможным разграничение доступа к определенным частям сервера на основе механизмов надежной аутентификации - сертификатов или одноразовых паролей.

Программы на серверной стороне, поддерживающие CGI или какой-либо другой интерфейс, важны для гибкости web как коммуникационной среды. Однако эта гибкость достигается ценой появления угроз безопасности, а слабая программа может сделать уязвимыми все виртуальные домены на сервере. Правила, сообразно которым поставщик Internet-услуг разделяет программы на допустимые и недопустимые, является показательным аспектом всей его политики безопасности.

Поставщику следует руководствоваться такими положениями:

- политика безопасности; выработка для своих потребителей ясной методики написания безопасных программ в имеющейся среде размещения Web-серверов с обязательным описанием тех приемов программирования, при применении которых программы будут отвергаться.
- установка программ: запрет на установку собственных программ потребителей. Все программы и командные процедуры передаются поставщику для первоначальной проверки на соответствие политике безопасности. Программы устанавливаются так, чтобы только администратор сервера мог их модифицировать.
- выбор пользователя и группы процесса: программы выполняются

от имени пользователя и группы, специально выбранных для этой цели и имеющих минимальные привилегии (часто используют "nobody").
- отображение в навигаторах: запрет при любых обстоятельствах на отображение программ в навигаторах. Как следствие - программы нельзя размещать под DocumentRoot.
- разделение виртуальных серверов: программы не следует делать доступными через сервер другого потребителя или для Web-мастера другого потребителя ;
- обработка пользовательского ввода: не вычислять выражения в пользовательском вводе, если нет механизма изоляции небезопасных действий.
- лимитирование потребления ресурсов: ввести лимит потребляемого астрономического и процессорного времени, а также дискового пространства для всех программ.
- маршрутные имена: все маршрутные имена делать абсолютными или начинающимися с DocumentRoot. Переменную PATH устанавливает только системный администратор.

Данные, которые пишет программа серверной стороны, следует считать конфиденциальными. Чтобы сделать невозможным доступ к таким данным через навигаторы, права устанавливаются так, чтобы у Web-демона не было права на чтение этих данных.

Если через Web-сервер предоставляется доступ к базам данных, то программам, осуществляющим такой доступ, выделяются лишь те полномочия, которые абсолютно необходимы для их функционирования.

Данные, относящиеся к управлению состояниями (идентифицирующие цепочки - cookies), следует считать конфиденциальными. Требуется исключить возможность доступа к ним из навигаторов.

Регистрационная информация, генерируемая Web-демоном, должна быть весьма конфиденциальной. Для реализации этого положения понадобится:

- поставщику Internet-услуг разрешить выполнение лишь необходимых операций с регистрационной информацией -

генерацию счетов и периодическую ротацию;
- регистрационную информацию хранить вне дерева с корнем в DocumentRoot, чтобы исключить возможность доступа через навигаторы;
- регистрационную информацию в первоначальном или обработанном виде передавать потребителю только по доверенному каналу.

Многие поставщики Internet-услуг предоставляют своим потребителям средства для продажи товаров или услуг через размещенные у поставщика Web-серверы. Поставщику, разместившему у себя приложения электронной коммерции, следует руководствоваться такими положениями:

- шифрование транзакций: транзакции нельзя хранить на сервере в открытом виде. Разрешается использование криптографии с открытыми ключами, так что только потребитель сможет расшифровать транзакции. Даже если транзакции передаются напрямую в финансовое учреждение или потребителю, поставщик услуг вправе сохранять у себя какую-то часть данных для обеспечения подотчетности;
- передача транзакций: передача производится по доверенному каналу, если транзакции не обрабатываются немедленно, а передаются потребителю пакетами;
- резервное копирование: в случае записи транзакций на резервные носители должна гарантироваться физическая безопасность этих носителей.

Загрузку информационного наполнения на сервер поставщика Internet-услуг следует производить по доверенному каналу.

Поставщики услуг нередко предоставляют для использования потребителями поисковые машины, средства контроля целостности ссылок и т.д. Зачастую такие средства создают весьма существенную дополнительную нагрузку, поэтому их запуск по запросу необходимо запретить, чтобы защититься от атак на доступность.

Поисковые машины надо сконфигурировать так, чтобы поиск ограничивался частями Web-сервера, доступными всем.

Результат проверки целостности ссылок следует считать конфиденциальным, а доступ к нему предоставить только лицу, управляющему информационным наполнением.

Возможные вопросы к поставщику Internet-услуг

При выборе поставщика Internet-услуг потребителям имеет смысл выяснить целый ряд вопросов:

1. Есть ли у поставщика документированная политика безопасности?
2. Имеется ли документированная политика добропорядочного пользования? Каковы санкции за ненадлежащее поведение?
3. Существует ли группа реагирования на нарушения информационной безопасности?

   Если существует, то:

   - Какие у нее права, правила работы и предоставляемые услуги?
   - Какова цепочка эскалации докладов, которой должен следовать потребитель?

   Если группы реагирования нет, то:

   - Какую роль играет поставщик услуг в реагировании на нарушения информационной безопасности?
   - Есть ли какая-нибудь группа реагирования, к которой потребитель может обратиться?
4. Оказывает ли поставщик Internet-услуг какие-либо дополнительные услуги в области информационной безопасности?
5. Информирует ли поставщик своих потребителей об атаках против них?
6. Оказывается ли помощь в прослеживании источника атаки?
7. Осуществляется ли сбор и сохранение улик, свидетельствующих о нарушении информационной безопасности?
8. Какую информацию сообщает поставщик услуг своим потребителям при обнаружении уязвимостей в предоставляемых

им сервисах?

9. Как и когда информация об уязвимостях передается потребителям?
10. К кому может обратиться потребитель по электронной почте для прояснения вопросов информационной безопасности?
11. К кому может обратиться потребитель по электронной почте для доклада о ненадлежащем поведении сторонних пользователей?
12. Как организованы коммуникации между поставщиком Internet-услуг и потребителями, если имеют место признаки нарушения информационной безопасности?
13. Какие меры принимает поставщик услуг, чтобы не допустить несанкционированной маршрутизации потоков данных в свою сеть или через нее?
14. Разделены ли на сегменты сети, поддерживающие потребителей услуг подключения и услуг размещения серверов?
15. Какие принимаются меры для обеспечения безопасности производственных сервисов, предоставляемых по Internet потребителями, в том числе для защиты от атак на доступность, вторжений, подделок?
16. Насколько быстро поставщик накладывает защитные заплаты на программное и микропрограммное обеспечение, функционирующее на производственном оборудовании?
17. Сканируются ли порты в сетях потребителей, и сообщается ли им о найденных аномалиях?
18. Предоставляются ли услуги по аудиту безопасности и усилению защиты систем потребителей?
19. Есть ли у поставщика Internet-услуг система активного аудита, обнаруживающая в реальном времени сетевые и системные атаки?
20. Какова политика добропорядочного пользования для информационного наполнения Web-сервера, размещенного у поставщика?
21. Как организована физическая защита оборудования, использующегося для размещения серверов потребителей?
22. Как часто производится резервное копирование информационного наполнения Web-серверов?
23. Как часто резервные носители передаются на внешнее хранение?
24. Осуществляет ли поставщик услуг балансировку нагрузки, чтобы предотвратить насыщение сети трафиком других потребителей?

25. Какое резервное оборудование используется в случае поломок? Как быстро оно может быть развернуто?
26. Какие виды доступа предоставляются для управления информационным наполнением размещенных у поставщика серверов?
27. Предоставляет ли поставщик защищенные Web-серверы (https)?
28. Закрыт ли доступ к информационному наполнению защищенного Web-сервера для других потребителей?
29. Как передавать информационное наполнение на защищенный Web-сервер?
30. Какова политика добропорядочного пользования для потребителей, разделяющих площади с поставщиком Internet-услуг?
31. Как организована физическая защита оборудования потребителей, размещенного на площадях поставщика?
32. Как обеспечена разводка по сети питания для оборудования разных потребителей, размещенного на общих площадях?
33. Как обеспечено сетевое разделение для оборудования разных потребителей, размещенного на общих площадях?

На этом мы завершаем рассмотрение спецификации Internet-сообщества "Как выбирать поставщика Internet-услуг ".

Британский стандарт BS 7799

Подробно рассматривается британский стандарт BS 7799, ставший основой международного стандарта ISO/IEC 17799. Он помогает решить проблемы административного и процедурного уровней информационной безопасности.

Обзор стандарта BS 7799

Продолжая рассмотрение стандартов и спецификаций, относящихся к административному и процедурному уровням информационной безопасности, мы приступаем к изучению двух частей британского стандарта BS 7799 (см. [28], [29]), фактически имеющего статус международного (ISO/IEC 17799). Русский перевод первой части опубликован в качестве приложения к информационному бюллетеню Jet Info [25].

Первая часть стандарта, по-русски именуемая "Управление информационной безопасностью". Практические правила", содержит систематический, весьма полный, универсальный перечень регуляторов безопасности, полезный для организации практически любого размера, структуры и сферы деятельности. Она предназначена для использования в качестве справочного документа руководителями и рядовыми сотрудниками, отвечающими за планирование, реализацию и поддержание внутренней системы информационной безопасности.

Согласно стандарту, цель информационной безопасности - обеспечить бесперебойную работу организации, по возможности предотвратить и/или минимизировать ущерб от нарушений безопасности.

Управление информационной безопасностью позволяет коллективно использовать данные, одновременно обеспечивая их защиту и защиту вычислительных ресурсов.

Подчеркивается, что защитные меры оказываются значительно более дешевыми и эффективными, если они заложены в информационные системы и сервисы на стадиях задания требований и проектирования.

Предлагаемые в первой части стандарта регуляторы безопасности

разбиты на десять групп:

- политика безопасности ;
- общеорганизационные аспекты защиты;
- классификация активов и управление ими ;
- безопасность персонала ;
- физической безопасности и безопасность окружающей среды ;
- администрирование систем и сетей ;
- управление доступом к системам и сетям;
- разработка и сопровождение информационных систем ;
- управление бесперебойной работой организации;
- контроль соответствия требованиям.

В стандарте выделяется десять ключевых регуляторов, которые либо являются обязательными в соответствии с действующим законодательством, либо считаются основными структурными элементами информационной безопасности. К ним относятся:

- документ о политике информационной безопасности;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала к поддержанию режима информационной безопасности;
- уведомление о случаях нарушения защиты ;
- антивирусные средства ;
- процесс планирования бесперебойной работы организации;
- контроль за копированием программного обеспечения, защищенного законом об авторском праве;
- защита документации;
- защита данных ;
- контроль соответствия политике безопасности.

Для обеспечения повышенного уровня защиты особо ценных ресурсов или оказания противодействия злоумышленнику с исключительно высоким потенциалом нападения могут потребоваться другие (более сильные) средства, которые в стандарте не рассматриваются.

Следующие факторы выделены в качестве определяющих для успешной реализации системы информационной безопасности в организации:

- цели безопасности и ее обеспечение должны основываться на производственных задачах и требованиях. Функции управления безопасностью должно взять на себя руководство организации;
- необходима явная поддержка и приверженность к соблюдению режима безопасности со стороны высшего руководства;
- требуется хорошее понимание рисков (как угроз, так и уязвимостей), которым подвергаются активы организации, и адекватное представление о ценности этих активов;
- необходимо ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации.

Во второй части стандарта BS 7799-2:2002 "Системы управления информационной безопасностью - спецификация с руководством по использованию" предметом рассмотрения, как следует из названия, является система управления информационной безопасностью.

Под системой управления информационной безопасностью (СУИБ) (Information Security Management System, ISMS) понимается часть общей системы управления, базирующаяся на анализе рисков и предназначенная для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. Эту систему составляют организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы.

В основу процесса управления положена четырехфазная модель, включающая:

- планирование;
- реализацию;
- оценку;
- корректировку.

По-русски данную модель можно назвать ПРОК (в оригинале - Plan-Do-Check-Act, PDCA). Детальный анализ каждой из выделенных фаз и составляет основное содержание стандарта BS 7799-2:2002.

Регуляторы безопасности и реализуемые ими цели.

Часть 1. Регуляторы общего характера

Мы приступаем к рассмотрению десяти групп регуляторов безопасности, выделенных в стандарте BS 7799.

К первой группе отнесено то, что связано с политикой безопасности, а именно:

- документально оформленная политика;
- процесс ревизии политики.

Цель регуляторов этой группы - определить стратегию управления безопасностью и обеспечить ее поддержку.

Рекомендуемая структура документированной политики изложена в курсе "Основы информационной безопасности" [91].

Вторая группа регуляторов безопасности касается общеорганизационных аспектов. По сравнению с первой она более многочисленна и наделена внутренней структурой. Ее первая подгруппа - инфраструктура информационной безопасности - преследует цель управления безопасностью в организации и включает следующие регуляторы:

- создание форума по управлению информационной безопасностью ;
- меры по координации действий в области информационной безопасности;
- распределение обязанностей в области информационной безопасности;
- утверждение руководством (административное и техническое) новых средств обработки информации;
- получение рекомендаций специалистов по информационной безопасности;
- сотрудничество с другими организациями (правоохранительными органами, поставщиками информационных услуг и т.д.);
- проведение независимого анализа информационной безопасности.

Регуляторы второй подгруппы - безопасность доступа сторонних организаций - предназначены для обеспечения безопасности вычислительных и информационных ресурсов, к которым имеют доступ сторонние организации. Этих регуляторов два:

- идентификация рисков, связанных с подключениями сторонних организаций, и реализация соответствующих защитных мер;
- выработка требований безопасности для включения в контракты со сторонними организациями.

Цель третьей подгруппы - обеспечение информационной безопасности при использовании услуг внешних организаций. Предлагается выработать требования безопасности для включения в контракты с поставщиками информационных услуг.

Очень важна третья группа регуляторов безопасности - классификация активов и управление ими. Необходимым условием обеспечения надлежащей защиты активов является их идентификация и классификация. Должны быть выработаны критерии классификации, в соответствии с которыми активы тем или иным способом получают метки безопасности.

Регуляторы четвертой группы - безопасность персонала - охватывают все этапы работы персонала, и первый из них - документирование ролей и обязанностей в области информационной безопасности при определении требований ко всем должностям. В соответствии с этими требованиями должны производиться отбор новых сотрудников, заключаться соглашения о соблюдении конфиденциальности, оговариваться в контрактах другие условия.

Для сознательного поддержания режима информационной безопасности необходимо обучение всех пользователей, регулярное повышение их квалификации.

Наряду с превентивными, стандарт предусматривает и меры реагирования на инциденты в области безопасности, чтобы минимизировать ущерб и извлечь уроки на будущее. Предусмотрены уведомления (доклады) об инцидентах и замеченных уязвимостях, нештатной работе программного обеспечения. Следует разработать

механизмы оценки ущерба от инцидентов и сбоев и дисциплинарного наказания провинившихся сотрудников.

Пятая группа регуляторов направлена на обеспечение физической безопасности и безопасности окружающей среды. Она включает три подгруппы:

- организация защищенных областей;
- защита оборудования;
- меры общего характера.

Для организации защищенных областей требуется определить периметры физической безопасности, контролировать вход в защищенные области и работу в них, защитить производственные помещения (особенно имеющие специальные требования по безопасности) и места погрузочно/разгрузочных работ, которые, по возможности, надо изолировать от производственных помещений.

Чтобы предупредить утерю, повреждение или несанкционированную модификацию оборудования рекомендуется размещать его в защищенных областях, наладить бесперебойное электропитание, защитить кабельную разводку, организовать обслуживание оборудования, перемещать устройства (в том числе за пределы организации) только с разрешения руководства, удалять информацию перед выведением из эксплуатации или изменением характера использования оборудования.

К числу мер общего характера принадлежат политика чистого рабочего стола и чистого экрана, а также уничтожение активов - оборудования, программ и данных - только с разрешения руководства.

Регуляторы безопасности и реализуемые ими цели. Часть 2. Регуляторы технического характера

Меры по безопасному администрированию систем и сетей разделены в стандарте BS 7799 на семь подгрупп:

- операционные процедуры и обязанности;

- планирование и приемка систем;
- защита от вредоносного программного обеспечения;
- повседневное обслуживание;
- администрирование сетей ;
- безопасное управление носителями;
- обмен данными и программами с другими организациями.

Документирование операционных процедур и обязанностей преследует цель обеспечения корректного и надежного функционирования средств обработки информации. Требуется обязательно контролировать все изменения этих средств. Доклады о нарушениях безопасности должны быть своевременными и эффективными. Разделение обязанностей должно препятствовать злоупотреблению полномочиями. Средства разработки и тестирования необходимо отделить от производственных ресурсов. Для безопасного управления внешними ресурсами предлагается предварительно оценить риски и включить в контракты со сторонними организациями соответствующие положения.

Планирование и приемка систем призваны минимизировать риск их отказа. Для этого рекомендуется отслеживать и прогнозировать вычислительную нагрузку, требуемые ресурсы хранения и т.д. Следует разработать критерии приемки новых систем и версий, организовать их тестирование до введения в эксплуатацию.

Защита от вредоносного программного обеспечения должна включать как превентивные меры, так и меры обнаружения и ликвидации вредоносного ПО.

Под повседневным обслуживанием в стандарте имеется в виду резервное копирование, протоколирование действий операторов, регистрация, доведение до сведения руководства и ликвидация сбоев и отказов.

Вопросы администрирования сетей в стандарте, по сути, не раскрываются, лишь констатируется необходимость целого спектра регуляторов безопасности и документирования обязанностей и процедур.

Безопасное управление носителями подразумевает контроль за

съемными носителями, безвредную утилизацию отслуживших свой срок носителей, документирование процедур обработки и хранения информации, защиту системной документации от несанкционированного доступа.

Более детально регламентирован обмен данными и программами с другими организациями. Предлагается заключать формальные и неформальные соглашения, защищать носители при транспортировке, обеспечивать безопасность электронной коммерции, электронной почты, офисных систем, систем общего доступа и других средств обмена. В качестве универсальных защитных средств рекомендуются документированная политика безопасности, соответствующие процедуры и регуляторы.

Самой многочисленной является группа регуляторов, относящихся к управлению доступом к системам и сетям. Она состоит из восьми подгрупп:

- производственные требования к управлению доступом;
- управление доступом пользователей;
- обязанности пользователей;
- управление доступом к сетям;
- управление доступом средствами операционных систем;
- управление доступом к приложениям;
- контроль за доступом и использованием систем;
- контроль мобильных пользователей и удаленного доступа.

Производственные требования к управлению доступом излагаются в документированной политике безопасности, которую необходимо проводить в жизнь.

Управление доступом пользователей должно обеспечить авторизацию, выделение и контроль прав в соответствии с политикой безопасности. Этой цели служат процедуры регистрации пользователей и ликвидации их системных счетов, управление привилегиями в соответствии с принципом их минимизации, управление паролями пользователей, а также дисциплина регулярной ревизии прав доступа.

Обязанности пользователей, согласно стандарту, сводятся к

правильному выбору и применению паролей, а также к защите оборудования, остающегося без присмотра.

Управление доступом к сетям опирается на следующие регуляторы:

- политика использования сетевых услуг (прямой доступ к услугам должен предоставляться только по явному разрешению);
- задание маршрута от пользовательской системы до используемых систем (предоставление выделенных линий, недопущение неограниченного перемещения по сети и т.д.);
- аутентификация удаленных пользователей;
- аутентификация удаленных систем;
- контроль доступа (особенно удаленного) к диагностическим портам;
- сегментация сетей (выделение групп пользователей, информационных сервисов и систем);
- контроль сетевых подключений (например, контроль по предоставляемым услугам и/или времени доступа);
- управление маршрутизацией ;
- защита сетевых сервисов (должны быть описаны атрибуты безопасности всех сетевых сервисов, используемых организацией).

Управление доступом средствами операционных систем направлено на защиту от несанкционированного доступа к компьютерным системам. Для этого предусматриваются:

- автоматическая идентификация терминалов;
- безопасные процедуры входа в систему (следует выдавать как можно меньше информации о системе, ограничить разрешаемое количество неудачных попыток, контролировать минимальную и максимальную продолжительность входа и т.п.);
- идентификация и аутентификация пользователей;
- управление паролями, контроль их качества;
- разграничение доступа к системным средствам;
- уведомление пользователей об опасных ситуациях;
- контроль времени простоя терминалов (с автоматическим отключением по истечении заданного периода);
- ограничение времени подключения к критичным приложениям.

Для управления доступом к приложениям предусматривается разграничение доступа к данным и прикладным функциям, а также изоляция критичных систем, помещение их в выделенное окружение.

Контроль за доступом и использованием систем преследует цель выявления действий, нарушающих политику безопасности. Для ее достижения следует протоколировать события, относящиеся к безопасности, отслеживать и регулярно анализировать использование средств обработки информации, синхронизировать компьютерные часы.

Контроль мобильных пользователей и удаленного доступа должен основываться на документированных положениях политики безопасности.

Регуляторы безопасности и реализуемые ими цели. Часть 3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия

Регуляторы группы "разработка и сопровождение информационных систем" охватывают весь жизненных цикл систем. Первым шагом является анализ и задание требований безопасности. Основу анализа составляют:

- необходимость обеспечения конфиденциальности, целостности и доступности информационных активов;
- возможность использования различных регуляторов для предотвращения и выявления нарушений безопасности и для восстановления нормальной работы после отказа или нарушения безопасности.

В частности, следует рассмотреть необходимость:

- управления доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- протоколирования для повседневного контроля или специальных расследований;
- контроля и поддержания целостности данных на всех или

избранных стадиях обработки;
- обеспечения конфиденциальности данных, возможно, с использованием криптографических средств;
- выполнения требований действующего законодательства, договорных требований и т.п.
- резервного копирования производственных данных;
- восстановления систем после отказов (особенно для систем с повышенными требованиями к доступности);
- защиты систем от несанкционированных модификаций;
- безопасного управления системами и их использования сотрудниками, не являющимися специалистами.

Подгруппа регуляторов, обеспечивающих безопасность прикладных систем, включает:

- проверку входных данных;
- встроенные проверки корректности данных в процессе их обработки;
- аутентификацию сообщений как элемент контроля их целостности;
- проверку выходных данных.

Третью подгруппу рассматриваемой группы составляют криптографические регуляторы. Их основой служит документированная политика использования средств криптографии. Стандартом предусматривается применение шифрования, электронных цифровых подписей, механизмов неотказуемости, средств управления ключами.

Четвертая подгруппа - защита системных файлов - предусматривает:

- управление программным обеспечением, находящимся в эксплуатации;
- защиту тестовых данных систем;
- управление доступом к библиотекам исходных текстов.

Регуляторы пятой подгруппы направлены на обеспечение безопасности процесса разработки и вспомогательных процессов. В нее входят следующие регуляторы:

- процедуры управления внесением изменений;
- анализ и тестирование систем после внесения изменений;
- ограничение на внесение изменений в программные пакеты;
- проверка наличия скрытых каналов и троянских программ ;
- контроль за разработкой ПО, выполняемой внешними организациями.

Группа "управление бесперебойной работой организации" исключительно важна, но устроена существенно проще. Она включает пять регуляторов, направленных на предотвращение перерывов в деятельности предприятия и защиту критически важных бизнес-процессов от последствий крупных аварий и отказов:

- формирование процесса управления бесперебойной работой организации;
- выработка стратегии (на основе анализа рисков) обеспечения бесперебойной работы организации;
- документирование и реализация планов обеспечения бесперебойной работы организации;
- поддержание единого каркаса для планов обеспечения бесперебойной работы организации, чтобы гарантировать их согласованность и определить приоритетные направления тестирования и сопровождения;
- тестирование, сопровождение и регулярный пересмотр планов обеспечения бесперебойной работы организации на предмет их эффективности и соответствия текущему состоянию.

Процесс планирования бесперебойной работы организации должен включать в себя:

- идентификацию критически важных производственных процессов и их ранжирование по приоритетам;
- определение возможного воздействия аварий различных типов на производственную деятельность;
- определение и согласование всех обязанностей и планов действий в нештатных ситуациях;
- документирование согласованных процедур и процессов;
- подготовку персонала к выполнению согласованных процедур и

процессов в нештатных ситуациях.

Для обеспечения бесперебойной работы организации необходимы процедуры трех типов:

- процедуры реагирования на нештатные ситуации;
- процедуры перехода на аварийный режим;
- процедуры возобновления нормальной работы.

Примерами изменений, которые могут потребовать обновления планов, являются:

- приобретение нового оборудования или модернизация систем;
- новая технология выявления и контроля проблем, например, обнаружения пожаров;
- кадровые или организационные изменения;
- смена подрядчиков или поставщиков;
- изменения, внесенные в производственные процессы;
- изменения, внесенные в пакеты прикладных программ;
- изменения в эксплуатационных процедурах;
- изменения в законодательстве.

Назначение регуляторов последней, десятой группы - контроль соответствия требованиям. В первую очередь имеется в виду соответствие требованиям действующего законодательства. Для этого необходимо:

- идентифицировать применимые законы, нормативные акты и т.п.
- обеспечить соблюдение законодательства по защите интеллектуальной собственности;
- защитить деловую документацию от утери, уничтожения или фальсификации;
- обеспечить защиту персональных данных ;
- предотвратить незаконное использование средств обработки информации;
- обеспечить выполнение законов, касающихся криптографических средств;
- обеспечить сбор свидетельств на случай взаимодействия с

правоохранительными органами.

Ко второй подгруппе отнесены регуляторы, контролирующие соответствие политике безопасности и техническим требованиям. Руководители всех уровней должны убедиться, что все защитные процедуры, входящие в их зону ответственности, выполняются должным образом и что все такие зоны регулярно анализируются на предмет соответствия политике и стандартам безопасности. Информационные системы нуждаются в регулярной проверке соответствия стандартам реализации защитных функций.

Регуляторы, относящиеся к аудиту информационных систем, объединены в третью подгруппу. Их цель - максимизировать эффективность аудита и минимизировать помехи, создаваемые процессом аудита, равно как и вмешательство в этот процесс. Ход аудита должен тщательно планироваться, а используемый инструментарий - защищаться от несанкционированного доступа.

На этом мы завершаем рассмотрение регуляторов безопасности, предусмотренных стандартом BS 7799.

Четырехфазная модель процесса управления информационной безопасностью

Мы приступаем к детальному рассмотрению четырехфазной (планирование - реализация - оценка - корректировка, ПРОК) модели процесса управления информационной безопасностью, примененной в стандарте BS 7799-2:2002.

Процесс управления имеет циклический характер; на фазе первоначального планирования осуществляется вход в цикл. В качестве первого шага должна быть определена и документирована политика безопасности организации.

Затем определяется область действия системы управления информационной безопасностью. Она может охватывать всю организацию или ее части. Следует специфицировать зависимости, интерфейсы и предположения, связанные с границей между СУИБ и ее окружением; это особенно важно, если в область действия попадает

лишь часть организации. Большую область целесообразно поделить на подобласти управления.

Ключевым элементом фазы планирования является анализ рисков. Этот вопрос детально рассмотрен в курсе "Основы информационной безопасности" [91]; здесь мы не будем на нем останавливаться.

Результат анализа рисков - выбор регуляторов безопасности. План должен включать график и приоритеты, детальный рабочий план и распределение обязанностей по реализации этих регуляторов.

На второй фазе - фазе реализации - руководством организации выделяются необходимые ресурсы (финансовые, материальные, людские, временные), выполняется реализация и внедрение выбранных регуляторов, сотрудникам объясняют важность проблем информационной безопасности, проводятся курсы обучения и повышения квалификации. Основная цель этой фазы - ввести риски в рамки, определенные планом.

Назначение фазы оценки - проанализировать, насколько эффективно работают регуляторы и система управления информационной безопасностью в целом. Кроме того, следует принять во внимание изменения, произошедшие в организации и ее окружении, способные повлиять на результаты анализа рисков. При необходимости намечаются корректирующие действия, предпринимаемые в четвертой фазе. Коррекция должна производиться, только если выполнено по крайней мере одно из двух условий:

- выявлены внутренние противоречия в документации СУИБ;
- риски вышли за допустимые границы.

Оценка может выполняться в нескольких формах:

- регулярные (рутинные) проверки;
- проверки, вызванные появлением проблем;
- изучение опыта (положительного и отрицательного) других организаций;
- внутренний аудит СУИБ;
- инспекции, проводимые по инициативе руководства;

- анализ тенденций.

Аудит должен выполняться регулярно, не реже одного раза в год. В процессе аудита следует убедиться в следующем:

- политика безопасности соответствует производственным требованиям;
- результаты анализа рисков остаются в силе;
- документированные процедуры выполняются и достигают поставленных целей;
- технические регуляторы безопасности (например, межсетевые экраны или средства ограничения физического доступа) расположены должным образом, правильно сконфигурированы и работают в штатном режиме;
- действия, намеченные по результатам предыдущих проверок, выполнены.

Даже если недопустимых отклонений не выявлено и уровень безопасности признан удовлетворительным, целесообразно зафиксировать изменения в технологии и производственных требованиях, появление новых угроз и уязвимостей, чтобы предвидеть будущие изменения в системе управления.

Систему управления информационной безопасностью надо постоянно совершенствовать, чтобы она оставалась эффективной . Эту цель преследует четвертая фаза рассматриваемого в стандарте цикла - корректировка. Она может потребовать как относительно незначительных действий, так и возврата к фазам планирования (например, если появились новые угрозы) или реализации (если следует осуществить намеченное ранее).

При корректировке прежде всего следует устранить несоответствия следующих видов:

- отсутствие или невозможность реализации некоторых требований СУИБ;
- неспособность СУИБ обеспечить проведение в жизнь политики безопасности или обслуживать производственные цели организации.

Задача фазы оценки - выявить проблемы. На фазе корректировки необходимо докопаться до их корней и устранить первопричины несоответствий, чтобы избежать повторного появления. С этой целью могут предприниматься как реактивные, так и превентивные действия, рассчитанные на среднесрочную или долгосрочную перспективу.

Таково (в сжатом изложении) содержание двух частей стандарта BS 7799. Может показаться, что каждое из его положений самоочевидно; тем не менее, собранные вместе и систематизированные, они обладают несомненной ценностью.

Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"

Рассматриваемый стандарт играет организующую роль, описывая внешний интерфейс криптографического модуля и общие требования к подобным модулям. Наличие такого стандарта упрощает разработку сервисов безопасности и профилей защиты для них.

Основные понятия и идеи стандарта FIPS 140-2

В федеральном стандарте США FIPS 140-2 "Требования безопасности для криптографических модулей" под криптографическим модулем понимается набор аппаратных и/или программных (в том числе встроенных) компонентов, реализующих утвержденные функции безопасности (включая криптографические алгоритмы, генерацию и распределение криптографических ключей, аутентификацию) и заключенных в пределах явно определенного, непрерывного периметра .

В стандарте FIPS 140-2 рассматриваются криптографические модули, предназначенные для защиты информации ограниченного доступа, не являющейся секретной, т. е. речь идет о промышленных изделиях, представляющих интерес для основной массы организаций. Наличие подобного модуля - необходимое условие обеспечения защищенности сколько-нибудь развитой информационной системы, однако, чтобы выполнять предназначенную ему роль, сам модуль также нуждается в защите, как собственными средствами, так и средствами окружения (например, операционной системы).

Согласно стандарту, перед криптографическим модулем ставятся следующие высокоуровневые функциональные цели безопасности:

- применение и безопасная реализация утвержденных функций безопасности для защиты информации ограниченного доступа ;
- обеспечение защиты модуля от несанкционированного использования и нештатных методов эксплуатации;
- предотвращение несанкционированного раскрытия содержимого модуля (криптографических ключей и других данных, критичных

для безопасности);
- предотвращение несанкционированной и необнаруживаемой модификации модуля и криптографических алгоритмов, в том числе несанкционированной модификации, подмены, вставки и удаления криптографических ключей и других данных, критичных для безопасности;
- обеспечение отображения (индикации) режима работы (состояния) модуля ;
- обеспечение доверия тому, что модуль функционирует должным образом при работе в утвержденном режиме;
- обнаружение ошибок в функционировании модуля и предотвращение компрометации информации ограниченного доступа и данных модуля, критичных для безопасности вследствие подобных ошибок.

Из перечисленных целей вытекают требования безопасности, относящиеся к этапам проектирования и реализации модуля и разделенные в стандарте на одиннадцать групп:

- спецификация криптографического модуля ;
- требования к портам и интерфейсам модуля ;
- роли, сервисы и аутентификация ;
- конечноавтоматная модель ;
- физическая безопасность ;
- эксплуатационное окружение ;
- управление криптографическими ключами ;
- электромагнитная совместимость;
- самотестирование ;
- доверие проектированию ;
- сдерживание прочих атак.

Спецификация модуля включает определение криптографического периметра, реализуемых функций и режимов, описание модуля, его аппаратных и программных компонентов, а также документированную политику безопасности.

Среди портов и интерфейсов модуля должны быть выделены обязательные и дополнительные. Следует специфицировать все интерфейсы, а также все маршруты входных и выходных данных. Кроме

того, порты для незащищенных параметров, критичных для безопасности, должны быть логически отделены от других портов.

Среди ролей и сервисов необходимо провести логическое разделение на обязательные и дополнительные, обеспечить персональную или ролевую аутентификацию.

Модель в виде конечного автомата должна описывать деление на обязательные и дополнительные состояния.

Меры физической самозащиты модуля включают замки, защитные кожухи, сохраняющие свидетельства вторжений пломбы, средства оперативного выявления и реагирования на попытки вторжений, меры по противодействию атакам, основанным на использовании нештатных внешних условий.

Ядром допустимого эксплуатационного окружения должна служить операционная система, удовлетворяющая требованиям утвержденного профиля защиты, обеспечивающая произвольное управление доступом, протоколирование и аудит, доверенные маршруты. Кроме того, следует применять утвержденные методы контроля целостности и построить модель политики безопасности.

В число поддерживаемых механизмов управления ключами должны входить генерация случайных чисел, распределение ввод/вывод, хранение и обнуление ключей.

На требованиях электромагнитной совместимости мы останавливаться не будем.

При включении питания и при выполнении определенных условий необходимо выполнение тестов криптографических алгоритмов, контроль целостности программного обеспечения, проверки критичных функций.

Меры доверия проектированию должны включать конфигурационное управление, процедуры безопасной установки, генерации и распространения. Следует подготовить функциональную спецификацию, при реализации использовать язык высокого уровня, продемонстрировать соответствие проекта и политики, снабдить

пользователей соответствующими руководствами.

Наконец, предусматриваются меры по сдерживанию атак, для которых пока нет стандартизованных требований.

Стандартом FIPS 140-2 предусмотрено четыре уровня защищенности криптографических модулей, что позволяет экономически целесообразным образом защищать данные разной степени критичности (регистрационные журналы, счета на миллионы долларов или данные, от которых зависит жизнь людей) в разных условиях (строго охраняемая территория, офис, неконтролируемый объект).

К первому (самому слабому) уровню применяется минимальный набор требований безопасности, которым удовлетворяет, например, шифрующая плата для персонального компьютера. Программные компоненты соответствующих модулей могут выполняться на универсальных вычислительных системах с несертифицированной ОС.

На втором уровне требуются:

- ролевая аутентификация ;
- замки на съемных оболочках и дверцах, защитные покрытия и пломбы, сохраняющие свидетельства вторжений;
- использование ОС, сертифицированных на соответствие определенным профилям защиты на основе "Общих критериев" с оценочным уровнем доверия не ниже второго.

К третьему уровню предъявляются следующие дополнительные требования:

- отделение портов и интерфейсов, применяемых для нешифрованного ввода/вывода криптографических ключей и других данных, критичных для безопасности;
- персональная аутентификация с проверкой допустимости принятия определенных ролей ;
- наличие средств оперативного выявления и реагирования на попытки вторжений (к примеру, микросхемы, обеспечивающие обнуление критичных данных модуля при попытке вскрыть корпус);

- использование ОС, сертифицированных на соответствие определенным профилям защиты с оценочным уровнем доверия не ниже третьего и поддержкой доверенного маршрута.

Четвертый уровень самый сильный. Его требования предусматривают полный спектр мер физической защиты, включая меры по противодействию атакам, берущим на вооружение нештатные внешние условия (электрические или температурные). Операционная система должна соответствовать оценочному уровню доверия не ниже четвертого.

Далее будут детально рассмотрены наиболее содержательные группы требований. Здесь же обратим внимание на параллель с профилем защиты для смарт-карт, общность целого ряда целей, предположений и требований безопасности для криптографических модулей и смарт-карт (что, разумеется, вполне естественно). На наш взгляд, сравнительный анализ этого профиля и стандарта FIPS 140-2 позволяет в полной мере оценить достоинства "Общих критериев" и ассоциированных спецификаций, высокую степень их полноты и систематичности. Конечно, "Общие критерии" можно критиковать, их нужно развивать и совершенствовать, но перевод стандарта FIPS 140-2 на рельсы "Общих критериев", несомненно, повысил бы его качество.

Требования безопасности. Часть 1. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация

Мы приступаем к детальному рассмотрению первых трех из перечисленных выше одиннадцати групп требований безопасности.

В спецификации криптографического модуля должны фигурировать аппаратные и/или программные компоненты, влияющие на его безопасность и заключенные в пределах определенных физических границ - криптографического периметра . Если модуль является программным, в пределах периметра окажутся процессор и другие аппаратные компоненты, хранящие и защищающие программы.

В спецификации должны быть определены физические порты и логические интерфейсы, все входные и выходные маршруты данных.

Следует описать ручные и логические средства управления криптографическим модулем, физические или логические индикаторы состояния, применимые физические (в частности, электрические) и логические характеристики.

В проектной документации необходимо представить схемы взаимосвязей таких компонентов, как микропроцессоры, буферы ввода/вывода, буферы открытых и шифрованных данных, управляющие буферы, ключевая, рабочая и программная память. Проект должен выполняться с использованием языка спецификаций высокого уровня.

Следует специфицировать все данные, критичные для безопасности, в том числе криптографические ключи, аутентификационные данные, параметры криптографических алгоритмов, регистрационные данные и т.д.

Обязательный элемент документации - политика безопасности криптографического модуля.

Прохождение всех информационных потоков, как и физический доступ к модулю, производится через определенный набор физических портов и логических интерфейсов. Интерфейсы должны логически различаться, хотя они могут разделять один порт (например, для ввода и вывода данных) или охватывать несколько портов (например, вывод данных может осуществляться через последовательный и параллельный порты). Прикладной программный интерфейс программного компонента модуля может трактоваться как один или несколько логических интерфейсов.

Следующие четыре логических интерфейса являются обязательными:

- интерфейс ввода данных. Все данные, поступающие в модуль для обработки и/или использования (кроме управляющих данных, см. далее) должны вводиться через этот интерфейс ;
- интерфейс вывода данных. Все выходные данные (кроме информации о состоянии, см. далее) должны покидать модуль через этот интерфейс . При возникновении ошибочных ситуаций и во время выполнения тестов вывод должен быть запрещен;
- входной управляющий интерфейс. Через него должны подаваться

все команды и сигналы (в том числе вызовы функций и ручные управляющие воздействия, например, нажатие на переключатель или клавишу), применяемые для управления функционированием криптографического модуля ;

- выходной интерфейс состояния. Через этот интерфейс выдаются все выходные сигналы, индикаторы и информация о состоянии (в том числе коды завершения и физические индикаторы, в частности, показания светодиодов), отображающие состояние криптографического модуля .

Все внешнее электрическое питание должно поступать через порт питания. Его может и не быть, если применяются внутренние батарейки.

Каждому обязательному логическому интерфейсу соответствует свой маршрут данных. Маршрут вывода данных логически отсоединяется от средств обработки в момент генерации, ручного ввода или обнуления ключей. Чтобы предотвратить непреднамеренный вывод данных, критичных для безопасности, следует предусмотреть два независимых внутренних действия, необходимых для использования интерфейсов, применяемых при выводе криптографических ключей, информации ограниченного доступа и т.п.

На третьем и четвертом уровнях безопасности порты (интерфейсы), предназначенные для ввода или вывода данных, критичных для безопасности, необходимо физически (логически) отделить от других портов (интерфейсов), а критичные данные должны поступать прямо в модуль (например, по непосредственно подсоединенному кабелю или доверенному маршруту).

В рамках криптографического модуля для операторов поддерживаются роли и ассоциированные с ними сервисы и права доступа (ролевой доступ рассматривался в курсе "Основы информационной безопасности" [91]). Один оператор может быть приписан нескольким ролям. Если модуль поддерживает параллельную работу нескольких операторов, он должен управлять разделением ролей.

Требуется поддержка по крайней мере следующих ролей:

- роль пользователя. В рамках этой роли выполняются обычные сервисы безопасности, включая криптографические операции и другие утвержденные функции;
- роль крипто-офицера. Она предназначена для выполнения криптографической инициализации и иных функций управления - инициализация модуля, ввод/вывод криптографических ключей, аудит и т.п.

Если операторам разрешается производить обслуживание модуля (например, диагностирование аппаратуры и/или программ), поддерживается роль инженера, при активизации и завершении которой следует обнулять все незащищенные критичные данные.

Криптографический модуль должен предоставлять следующие сервисы:

- отображение состояния;
- выполнение тестов;
- выполнение утвержденной функции безопасности.

Если модуль поддерживает режим обхода (режим без выполнения криптографической обработки данных), то для его активизации необходимы два независимых внутренних действия, а текущее состояние должно соответствующим образом отображаться.

Если не производится чтение, модификация или замена критичных данных (например, выполняется лишь изучение состояния или тестирование модуля), оператор не обязан активизировать какую-либо роль.

Начиная со второго уровня безопасности, активизации роли должна предшествовать аутентификация оператора: ролевая или (на третьем и четвертом уровнях безопасности) персональная.

В стандарте не оговорены требуемые механизмы аутентификации, специфицирована лишь их стойкость. Вероятность случайного успеха одной попытки должна составлять менее 1/1000000, вероятность случайного успеха какой-либо из нескольких попыток, производимых в течение минуты, - менее 1/100000. Это весьма (а на наш взгляд - чрезмерно) мягкие требования, если учитывать, что в году 525600

минут. Очевидно, необходимы меры противодействия многократным неудачным попыткам аутентификации.

Требования безопасности. Часть 2. Модель в виде конечного автомата, физическая безопасность

В конечноавтоматной модели криптографического модуля должны быть предусмотрены следующие состояния, соответствующие нормальному и ошибочному функционированию:

- включение/выключение питания (первичного, вторичного, резервного);
- обслуживание крипто-офицером (например, управление ключами);
- ввод ключей и других критичных данных;
- пользовательские состояния (выполнение криптографических операций, предоставление сервисов безопасности);
- самотестирование ;
- ошибочные состояния (например, неудача самотестирования или попытка шифрования при отсутствии необходимого ключа), которые могут подразделяться на фатальные, требующие сервисного обслуживания (например, поломка оборудования), и нефатальные, из которых возможен возврат к нормальному функционированию (например, путем инициализации или перезагрузки модуля).

Могут быть предусмотрены и другие, дополнительные состояния:

- работа в режиме обхода (передача через модуль открытых данных);
- работа в инженерном режиме (например, физическое и логическое тестирование).

Вопросы обеспечения физической безопасности криптографических модулей исключительно важны и сложны. В стандарте FIPS 140-2 им уделено очень много внимания. Мы, однако, остановимся лишь на основных моментах.

Стандартом предусмотрены четыре разновидности криптографических

модулей:

- чисто программные (вопросы физической безопасности для них не рассматриваются);
- состоящие из одной микросхемы;
- состоящие из нескольких микросхем и встроенные в физически незащищенное окружение (например, плата расширения);
- состоящие из нескольких микросхем и обладающие автономной защитой (например, шифрующие маршрутизаторы).

Меры физической защиты структурированы в стандарте двумя способами. Во-первых, вводится деление на меры выявления свидетельств случившихся ранее нарушений (обнаружение нарушений) и меры выявления нарушений в реальном времени с выполнением соответствующих ответных действий (реагирование на нарушения).

Во-вторых, защитные меры подразделяются на общие и специфические для той или иной разновидности модулей.

И, наконец, в соответствии с принятым в стандарте подходом, меры группируются по четырем уровням безопасности.

Мы ограничимся рассмотрением общих требований физической безопасности, применимых ко всем аппаратным конфигурациям.

Если разрешено производить обслуживание модуля и поддерживается роль инженера, должен быть определен интерфейс обслуживания, включающий все маршруты физического доступа к содержимому модуля, в том числе все съемные оболочки и дверцы (которые необходимо снабдить подходящими средствами физической защиты). При доступе по интерфейсу обслуживания все хранящиеся в открытом виде секретные ключи и другие критичные ключи необходимо обнулить.

На втором уровне безопасности предусмотрено обнаружение нарушений, а начиная с третьего - реагирование на нарушения.

Для четвертого уровня предусмотрена защита от нештатных внешних условий (электрических или температурных), которая может быть реализована двояко:

- путем постоянного отслеживания электрических и температурных параметров с выключением модуля или обнулением данных, критичных для безопасности, при выходе параметров за допустимые границы;
- путем обеспечения устойчивости модуля к нештатным внешним условиям (например, модуль должен нормально работать при температурах от -100 до +200 градусов).

Требования безопасности. Часть 3. Эксплуатационное окружение, управление криптографическими ключами

Эксплуатационное окружение - это совокупность необходимых для функционирования модуля средств управления аппаратными и программными компонентами. В стандарте FIPS 140-2 рассматривается несколько видов окружения:

- универсальное, с коммерческой операционной системой, управляющей как компонентами модуля, так и другими процессами и приложениями;
- ограниченное, являющееся статическим, немодифицируемым (например, виртуальная Java-машина на непрограммируемой плате для персонального компьютера);
- модифицируемое, которое может быть реконфигурировано и включать средства универсальных ОС .

Ядро универсального и модифицируемого окружения - операционная система. На первом уровне безопасности к ней предъявляются следующие требования:

- используется только однопользовательский режим, параллельная работа нескольких операторов явным образом запрещается;
- доступ процессов, внешних по отношению к модулю, к данным, критичным для безопасности, запрещается, некриптографические процессы не должны прерывать работу криптографического модуля ;
- программное обеспечение модуля следует защитить от несанкционированного раскрытия и модификации;
- целостность ПО модуля контролируется утвержденными

средствами.

Для второго уровня безопасности требуется использование ОС, сертифицированных на соответствие определенным профилям защиты на основе "Общих критериев" с оценочным уровнем доверия не ниже второго. Для защиты критичных данных должно применяться произвольное управление доступом с определением соответствующих ролей. Необходимо протоколирование действий крипто-офицера.

Характерная черта третьего уровня безопасности - использование доверенного маршрута.

На четвертом уровне безопасности криптографического модуля нужна ОС с оценочным уровнем доверия не ниже четвертого.

Требования безопасного управления криптографическими ключами охватывают весь жизненный цикл критичных данных модуля. Рассматриваются следующие управляющие функции:

- генерация случайных чисел;
- генерация ключей ;
- распределение ключей ;
- ввод/вывод ключей ;
- хранение ключей ;
- обнуление ключей.

Секретные ключи необходимо защищать от несанкционированного раскрытия, модификации и подмены, открытые - от модификации и подмены.

Компрометация методов генерации или распределения ключей (например, угадывание затравочного значения, инициализирующего детерминированный генератор случайных чисел) должна быть не проще определения значений ключей.

Для распределения ключей может применяться как ручная транспортировка, так и автоматические процедуры согласования ключей.

Допускается ручной (с клавиатуры) и автоматический (например, при помощи смарт-карты) ввод ключей. На двух нижних уровнях безопасности при автоматическом вводе секретные ключи должны быть зашифрованы; ручной ввод может осуществляться в открытом виде. На третьем и четвертом уровнях при ручном вводе ключей в открытом виде применяются процедуры разделения знаний.

Модуль должен ассоциировать введенный ключ (секретный или открытый) с владельцем (лицом, процессом и т.п.).

Требования безопасности. Часть 4. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации.

Мы приступаем к рассмотрению трех последних из одиннадцати предусмотренных стандартом FIPS 140-2 групп требований безопасности для криптографических модулей.

Криптографический модуль должен выполнять самотестирование при включении питания, при выполнении некоторых условий (когда вызывается функция безопасности, для которой предусмотрено тестирование), а также по требованию оператора.

Необходимо, чтобы тесты покрывали все функции модуля (зашифрование, расшифрование, аутентификацию и т.д.). Для определения правильности прохождения тестов может применяться как сравнение с заранее известными, эталонными результатами, так и анализ согласованности результатов двух независимых реализаций одной и той же функции.

Специфицированы следующие виды проверок:

- тесты криптографических алгоритмов;
- контроль целостности программного обеспечения;
- тесты функций, критичных для безопасности модуля.

В число проверок, выполняемых по условию, входят:

- проверка взаимной согласованности парных ключей ;
- контроль загружаемых программ;
- контроль ключей, вводимых вручную;
- тест генератора случайных чисел;
- тест режима обхода.

Меры доверия проектированию, заданные стандартом, распространяются на конфигурационное управление, процедуры безопасной установки, генерации и распространения, процесс разработки и документацию.

Документация, представляемая разработчиком на первом уровне безопасности, должна специфицировать соответствие между проектом криптографического модуля и его политикой безопасности, а комментарии в исходном тексте - между проектом и программными компонентами.

На втором уровне предусмотрена функциональная спецификация с неформальным описанием модуля, внешних портов и интерфейсов, их назначения.

На третьем уровне программные компоненты должны быть реализованы на языке высокого уровня, за исключением, быть может, небольшого числа ассемблерных вставок. Высокоуровневая спецификация требуется и для аппаратуры.

На четвертом уровне устанавливается формальная модель политики безопасности с обоснованием ее полноты и непротиворечивости и неформальной демонстрацией соответствия функциональным спецификациям. В исходных текстах программных компонентов должны быть представлены необходимые предусловия и ожидаемые постусловия.

Комплект документации состоит из руководства крипто-офицера (аналог руководства администратора) и пользователя.

Криптографические модули могут стать объектом самых разных атак, основанных, например, на анализе потребляемого электропитания или времени выполнения операций, на переводе модуля в сбойный режим, на анализе побочных электромагнитных излучений и наводок и т.д.

Для противодействия анализу потребляемого электропитания в модуль могут встраиваться конденсаторы, использоваться внутренние источники питания, вставляться специальные инструкции для выравнивания потребления электропитания в процессе выполнения криптографических функций.

Средство сдерживания атак, основанных на анализе времени выполнения операций, - вставка дополнительных инструкций, сглаживающих различия во времени работы.

Для противодействия атакам, основанным на переводе модуля в сбойный режим, стандарт рекомендует описанные выше меры физической защиты.

В качестве приложений стандарт FIPS 140-2 содержит рекомендации, дополняющие одиннадцать групп требований безопасности. К ним относятся:

- сводка требований к документации;
- рекомендуемые правила разработки программного обеспечения;
- рекомендуемое содержание политики безопасности криптографического модуля.

В заключение еще раз подчеркнем роль стандарта FIPS 140-2 как базового элемента других спецификаций в области информационной безопасности, включая профили защиты сервисов безопасности, их комбинаций и приложений. Очевидно, весьма желательна разработка российского аналога данного документа.

Заключение

Подводится итог курса, кратко суммируются полученные знания.

Основные идеи курса

Знание стандартов и спецификаций важно для специалистов в области информационной безопасности по целому ряду причин, главная из которых состоит в том, что стандарты и спецификации - одна из форм накопления знаний, в первую очередь о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами.

В статье 12 закона РФ "О техническом регулировании" определен принцип применения международного стандарта как основы разработки национального стандарта. Это означает, что знание международных стандартов требуется для понимания направлений развития отечественной нормативной базы, что, в свою очередь, важно для выработки стратегии построения и совершенствования информационных систем.

Количество стандартов и спецификаций в области ИБ велико. В курсе рассмотрены наиболее существенные из них, изучение которых необходимо всем или почти всем разработчикам, оценщикам, администраторам, руководителям, пользователям.

В курсе выделены две группы стандартов и спецификаций:

- оценочные стандарты, направленные на оценивание и классификацию информационных систем и средств защиты по требованиям безопасности ;
- спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Обе группы дополняют друг друга. Оценочные стандарты выделяют важнейшие понятия и аспекты ИС, играя роль организационных и архитектурных спецификаций. Другие спецификации определяют, как

строить ИС предписанной архитектуры и выполнять организационные требования.

Из числа рассмотренных в курсе оценочных стандартов необходимо выделить международный стандарт "Критерии оценки безопасности информационных технологий" (точнее, его первоисточник - " Общие критерии ") и разработанные на его основе профили защиты . Это - основа современной системы сертификации по требованиям безопасности, системы, к которой стремится присоединиться и Россия.

Основным источником технических спецификаций, применимых к современным распределенным ИС, является Internet-сообщество, уделяющее внимание не только программно-техническому, но также административному и процедурному уровням информационной безопасности. Комплексность подхода Internet-сообщества к проблемам ИБ проявляется и в том, что в спецификациях рассматриваются как профилактические меры, направленные на предупреждение нарушений ИБ, так и меры реагирования на нарушения. Вероятно, среди многих международных стандартов, затрагивающих вопросы сетевой безопасности, наиболее часто цитируется документ X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов". Этот стандарт важен и как образец тщательной проработки и продуманного развития простой, но весьма глубокой идеи - идеи цифрового сертификата, способного хранить атрибуты произвольной природы.

Очень ценно, когда стандарт не просто что-то требует, но предлагает образцы, помогающие выполнить те или иные требования. К числу таких конструктивных стандартов принадлежит BS 7799 (ISO/IEC 17799), дающий возможность справиться с проблемами административного и процедурного уровней информационной безопасности.

Общие критерии" и профили защиты на их основе

"Проект ОК", результатом которого стали " Общие критерии оценки безопасности информационных технологий", носит не только технический, но и экономико-политический характер. Его цель состоит, в частности, в том, чтобы упростить, удешевить и ускорить путь сертифицированных изделий информационных технологий на мировой

рынок.

Эта цель близка и понятна российским специалистам. В 2002 году был официально издан ГОСТ Р ИСО/МЭК 15408-2002 "Критерии оценки безопасности информационных технологий" с датой введения в действие первого января 2004 г. Таким образом, и Россия фактически живет по " Общим критериям " со всеми вытекающими из данного факта последствиями.

В рамках " Проекта ОК ", помимо " Общих критериев ", разработан целый ряд документов, среди которых выделяется "Общая методология оценки безопасности информационных технологий", облегчающая и унифицирующая применение ОК.

Согласно подходу, принятому в " Общих критериях ", на основании предположений безопасности, при учете угроз и положений политики безопасности формулируются цели безопасности для объекта оценки. Для их достижения к объекту и его среде предъявляются требования безопасности.

" Общие критерии " в главной своей части являются каталогом (библиотекой) требований безопасности. Спектр стандартизованных требований чрезвычайно широк, что способствует универсальности ОК. Высокий уровень детализации делает их конкретными, допускающими однозначную проверку, способствует повторяемости результатов оценки. Требования параметризованы, что обеспечивает их гибкость.

" Общие критерии " содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности объекта оценки и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации объекта оценки.

Библиотека функциональных требований составляет вторую часть "

Общих критериев ", а каталог требований доверия - третью часть (первая содержит изложение основных концепций ОК).

После того как сформулированы функциональные требования, требования доверия и требования к среде, возможна оценка безопасности изделия ИТ. Для типовых изделий " Общие критерии " предусматривают разработку типовых совокупностей требований безопасности - профилей защиты.

Рассматриваемые в курсе профили делятся на следующие категории:

- профили защиты для отдельных сервисов безопасности ;
- профили защиты для комбинаций и приложений сервисов безопасности.

Кроме того, выделяются общие требования к сервисам безопасности. К числу важнейших видов функциональных требований принадлежат:

- идентификация (FIA_UID) и аутентификация (FIA_UAU);
- определение атрибутов пользователя (FIA_ATD);
- связывание пользователь-субъект (FIA_USB);
- политика управления доступом (FDP_ACC);
- функции управления доступом (FDP_ACF);
- генерация данных аудита безопасности (FAU_GEN);
- анализ аудита безопасности (FAU_SAA);
- управление криптографическими ключами (FCS_CKM);
- криптографические операции (FCS_COP);
- базовая защита внутренней передачи (FDP_ITT);
- защита остаточной информации (FDP_RIP);
- целостность экспортируемых данных (FPT_ITI);
- управление отдельными функциями безопасности (FMT_MOF);
- управление данными функций безопасности (FMT_MTD);
- безопасность при сбое (FPT_FLS);
- надежное восстановление (FPT_RCV);
- посредничество при обращениях (FPT_RVM);
- разделение доменов (FPT_SEP);
- доверенный канал передачи между функциями безопасности (FTP_ITC);
- доверенный маршрут (FTP_TRP).

В качестве важнейших общих требований доверия безопасности выделяются:

- анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации;
- независимое тестирование;
- наличие проекта верхнего уровня ;
- анализ стойкости функций безопасности ;
- поиск разработчиком явных уязвимостей ;
- контроль среды разработки;
- управление конфигурацией.

Профили защиты и их проекты, рассматриваемые в курсе, применимы к следующим сервисам безопасности:

- (биометрическая) идентификация и аутентификация ;
- управление доступом (произвольное, принудительное, ролевое);
- (межсетевое) экранирование ;
- (активный) аудит;
- анализ защищенности.

Изучаются также инфраструктурные элементы информационной безопасности:

- анонимизаторы;
- выпуск и управление сертификатами.

Выделим представленный в курсе профиль защиты для одной из разновидностей анонимизаторов. Он поучителен по крайней мере по двум причинам:

- в нем продемонстрирована важность архитектурных требований для обеспечения информационной безопасности и недостаточность соответствующих средств " Общих критериев ";
- он характеризует становление так называемой многоаспектной информационной безопасности, когда делается попытка учесть весь спектр интересов (порой конфликтующих) всех субъектов информационных отношений.

В свою очередь, изучение упорядоченного семейства из четырех профилей защиты для аппаратно-программных компонентов, реализующих выпуск, аннулирование и управление сертификатами открытых ключей, способствует активному овладению идеями и понятиями стандарта X.509. Кроме того, данное семейство может служить примером при построении классификационных схем в Руководящих документах Гостехкомиссии России.

Важнейшей (и наиболее привычной) комбинацией сервисов безопасности являются операционные системы. Как таковые они содержат лишь небольшое число специфических требований, среди которых выделяются:

- максимальные квоты (FRU_RSA.1);
- дополнительный элемент FAU_GEN.1-CSPP.3, предписывающий предоставление прикладного программного интерфейса для добавления собственных данных к общему регистрационному журналу и/или для ведения приложениями собственных журналов;
- ряд дополнительных требований, направленных на обеспечение конфиденциальности (FPT_ITC.1.1-CSPP), целостности (FPT_ITI.1.1-CSPP), согласованности (FPT_SYN-CSPP.1.1) критичных данных функций безопасности в распределенных конфигурациях.

Анализ профиля защиты для систем управления базами данных показывает, что при использовании стандартных требований " Общих критериев " существует опасность оставить за рамками рассмотрения специфические свойства приложений и присущие им угрозы.

Весьма поучителен профиль защиты для смарт-карт, при его изучении можно усмотреть множество аналогий со стандартом FIPS 140-2 " Требования безопасности для криптографических модулей". И профиль, и стандарт - хорошие примеры систематического подхода к вопросам собственной защищенности средств безопасности.

Из числа специфических функциональных требований профиля особого внимания заслуживают:

- автоматическая реакция аудита безопасности (FAU_ARP);
- противодействие физическому нападению (FPT_PHP.3).

Отметим также выделение двух функциональных пакетов: для интегральной схемы и базового ПО. Это - пример модульности, важной не только для программирования, но и вообще для работы с большими системами.

" Общие критерии " - исключительно мощное, гибкое средство разработки требований безопасности для изделий информационных технологий. В то же время, сама гибкость " Общих критериев " является источником сложных проблем, в первую очередь относящихся к методологии разработки профилей защиты.

По результатам рассмотрения ОК можно наметить следующие направления дальнейших исследований и разработок:

- создание новых профилей защиты, охватывающих все сервисы безопасности ;
- разработка дисциплины и инструментальных средств для работы с множеством профилей защиты ;
- развитие " Общих критериев ", разработка новых стандартных требований безопасности, как "точечных", так и концептуальных, архитектурных.

Спецификации Internet-сообщества для программно-технического уровня ИБ

Из множества спецификаций Internet-сообщества, относящихся к программно-техническому уровню информационной безопасности, для данного курса были выбраны три: IPsec, TLS и GSS-API.

Выбор IPsec и TLS основан на том, что как на сетевом, так и на транспортном уровне эталонной семиуровневой модели могут быть реализованы практически все функции безопасности, выделенные в спецификации X.800 (см. курс "Основы информационной безопасности" [91]). (Исключение составляют избирательная конфиденциальность и неотказуемость ; кроме того,

конфиденциальность трафика реализуется на сетевом, но не на транспортном уровне, а целостность с восстановлением - наоборот, на транспортном, но не на сетевом уровне .)

Протоколы IPsec обеспечивают управление доступом, целостность вне соединения, аутентификацию источника данных, защиту от воспроизведения, конфиденциальность и частичную защиту от анализа трафика.

Основными элементами архитектуры средств безопасности для IP-уровня являются протокол аутентифицирующего заголовка и протокол инкапсулирующей защиты содержимого, а также механизмы управления криптографическими ключами.

Протокол аутентифицирующего заголовка служит в IPsec для обеспечения целостности пакетов и аутентификации источника данных, а также для защиты от воспроизведения ранее посланных пакетов. Он защищает данные протоколов более высоких уровней и те поля IP-заголовков, которые не меняются на маршруте доставки или меняются предсказуемым образом.

Протокол инкапсулирующей защиты содержимого предоставляет три вида сервисов безопасности:

- обеспечение конфиденциальности (шифрование содержимого IP-пакетов, а также частичная защита от анализа трафика путем применения туннельного режима);
- обеспечение целостности IP-пакетов и аутентификации источника данных ;
- обеспечение защиты от воспроизведения IP-пакетов.

Протоколы обеспечения аутентичности и конфиденциальности могут использоваться в двух режимах: транспортном и туннельном. В первом случае защищается только содержимое пакетов и, быть может, некоторые поля заголовков. В туннельном режиме защищается весь пакет.

При взаимодействии средствами IPsec стороны должны выработать общий контекст безопасности и затем применять элементы этого

контекста, такие как алгоритмы и их ключи. За формирование контекстов безопасности в IPsec отвечает особое семейство протоколов.

Формирование контекстов безопасности в IPsec разделено на две фазы. Сначала создается управляющий контекст, назначение которого - предоставить доверенный канал для выработки (в рамках второй фазы) протокольных контекстов.

Протокольный контекст безопасности в IPsec - это однонаправленное "соединение" (от источника к получателю), предоставляющее обслуживаемым потокам данных набор защитных сервисов. Пользователями протокольных контекстов, как правило, являются прикладные процессы.

Системы, реализующие IPsec, должны поддерживать две базы данных:

- базу данных политики безопасности ;
- базу данных протокольных контекстов безопасности.

Все IP-пакеты (входящие и исходящие) сопоставляются с упорядоченным набором правил политики безопасности. При сопоставлении используется фигурирующий в каждом правиле селектор - совокупность анализируемых полей сетевого и более высоких протокольных уровней. Первое подходящее правило определяет характер обработки пакета.

Таким образом, системы, реализующие IPsec, функционируют в духе межсетевых экранов, фильтруя и преобразуя потоки данных на основе предварительно заданной политики безопасности.

Протокол безопасности транспортного уровня (TLS) - развитие версии 3.0 протокола SSL. Посредством протокола TLS приложения, построенные в архитектуре клиент/сервер, могут защититься от пассивного и активного прослушивания сети и подделки сообщений .

TLS имеет двухуровневую организацию. На первом уровне, опирающемся на надежный транспортный сервис, располагается протокол передачи записей, на втором - протокол установления соединений.

Протокол передачи записей обеспечивает конфиденциальность и целостность передаваемых данных. Представим его функционирование в общем виде. Сообщение разбивается на блоки (записи), сжимается, снабжается имитовставкой, шифруется, после чего выполняется передача результата. На стороне получателя принятые данные расшифровываются, верифицируются, подвергаются декомпрессии и сборке, и затем сообщение доставляется клиенту на вышележащем протокольном уровне.

Протокол установления соединений позволяет серверу и клиенту провести взаимную аутентификацию, согласованно выбрать алгоритм шифрования и криптографические ключи, прежде чем прикладной протокол начнет передачу данных. При выработке совместных секретов обеспечивается конфиденциальность, целостность и защита от нелегального посредника.

В спецификациях TLS фигурируют четыре криптографические операции: цифровая подпись, потоковое шифрование, блочное шифрование и шифрование открытым ключом.

Компьютерная криптография - это большая и сложная тема, для которой особенно важно разбиение на относительно независимые аспекты. Мы выделим три из них:

- алгоритмический ;
- интерфейсный ;
- собственной защищенности.

Алгоритмического аспекта мы не касаемся. Вопросам собственной защищенности криптографических средств посвящены стандарт FIPS 140-2 и профиль защиты для смарт-карт. Интерфейсный аспект - предмет спецификации Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности" (некоторое внимание этому аспекту уделено и в стандарте FIPS 140-2).

Интерфейс GSS-API преследует цель защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Он предоставляет услуги по взаимной аутентификации общающихся партнеров и по контролю целостности и обеспечению

конфиденциальности пересылаемых сообщений.

Основными понятиями обобщенного прикладного программного интерфейса службы безопасности являются:

- удостоверение ;
- контекст безопасности;
- токен безопасности ;
- механизм безопасности ;
- имя;
- канал передачи данных.

Интерфейс GSS-API предоставляет следующие основные виды функций:

- работа с удостоверениями ;
- создание и уничтожение контекстов безопасности;
- защита сообщений;
- вспомогательные функции.

Обобщенный интерфейс безопасности не зависит от языковой среды и механизмов безопасности, обеспечивающих реальную защиту. Приложения, использующие GSS-API, на уровне исходного текста мобильны по отношению к смене механизмов безопасности. Тем самым реализуется открытость прикладных систем и соответствующих средств защиты.

Спецификации Internet-сообщества для административного и процедурного уровней ИБ

В курсе рассматривается три спецификации Internet-сообщества для административного и процедурного уровней информационной безопасности:

- "Руководство по информационной безопасности предприятия";
- "Как реагировать на нарушения информационной безопасности";
- "Как выбирать поставщика Интернет-услуг ".

Центральную роль играет "Руководство по информационной безопасности предприятия". В Руководстве перечисляются вопросы и факторы, которые следует проанализировать при формировании политики безопасности, оно отвечает на вопросы о том, что входит в политику безопасности, какие процедуры необходимы для обеспечения безопасности, что нужно делать в ситуациях, угрожающих безопасности.

Формирование политики и процедур безопасности означает выработку плана действий по информационной защите, для чего необходимо:

- выяснить, что следует защищать;
- выяснить, от чего следует защищаться;
- определить вероятность угроз ;
- реализовать меры, которые позволят защитить активы экономически оправданным образом;
- постоянно возвращаться к предыдущим этапам и совершенствовать защиту после выявления новых уязвимых мест.

В Руководстве основной упор делается на два последних этапа.

Когда политика выработана, можно приступать к созданию процедур, решающих проблемы безопасности.

Системные администраторы и руководители должны знать современные угрозы, связанные с ними риски, размер возможного ущерба, а также набор доступных мер для предотвращения и отражения нападений.

Очень важны рассматриваемые в Руководстве меры реагирования на нарушения, а также действия, предпринимаемые после ликвидации нарушений безопасности. Следует помнить, что планирование защитных действий - это непрерывный циклический процесс.

Тема реагирования развивается в спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности".

Цель данной спецификации - сформулировать ожидания Internet-сообщества по отношению к группам реагирования на нарушения информационной безопасности. Потребители имеют право понимать

правила и процедуры работы своей группы реагирования и нуждаются в этих знаниях.

Коллектив, называющий себя группой реагирования, должен реагировать на выявленные нарушения безопасности и на угрозы своим подопечным, действуя в интересах конкретного сообщества и способами, принятыми в этом сообществе.

Чтобы считаться группой реагирования, необходимо:

- предоставлять защищенный канал для приема сообщений о предполагаемых нарушениях;
- оказывать помощь членам опекаемого сообщества в ликвидации нарушений ;
- распространять информацию, относящуюся к нарушению, в пределах опекаемого сообщества и другим заинтересованным сторонам.

Группа реагирования должна объяснить, кого она опекает, и определить предоставляемые услуги, опубликовать свои правила и регламенты, порядок доклада о нарушениях.

С практической точки зрения, очень важно "Дополнение к Руководству по информационной безопасности предприятия: Как выбирать поставщика Internet-услуг ", призванное помочь в выработке политики и процедур безопасности в тех организациях, информационные системы которых подключены к Internet, а также служить для потребителей контрольным перечнем при обсуждении вопросов информационной безопасности с поставщиками Internet-услуг.

В заключение еще раз подчеркнем важность внимательного изучения и активного овладения знаниями, заложенными в стандарты и спецификации в области информационной безопасности. Это необходимо как отдельным специалистам для получения базовой квалификации, так и организациям, выстраивающим долгосрочную стратегию и заботящимся о защите своих интересов.

Список литературы

1. Безопасность информационных технологий. Контролируемый доступ. Профиль защиты (первая редакция), Центр безопасности информации, 2002.

2. Безопасность информационных технологий. Меточная защита. Профиль защиты (первая редакция), Центр безопасности информации, 2002.

3. Безопасность информационных технологий. Многоуровневые операционные системы в средах, требующих среднюю робастность. Профиль защиты (вторая редакция), Центр безопасности информации, 2002.

4. Безопасность информационных технологий. Одноуровневые операционные системы в средах, требующих среднюю робастность. Профиль защиты (вторая редакция), Центр безопасности информации, 2002.

5. Безопасность информационных технологий. Система управления базой данных. Профиль защиты (первая редакция), Центр безопасности информации, 2002.

6. Бетелин В.Б., Галатенко А.В., Галатенко В.А., Кобзарь М.Т., Сидак А.А., Классификация средств активного аудита в терминах "Общих критериев", В сб. "Информационная безопасность. Инструментальные средства программирования. Базы данных" под ред. чл.-корр. РАН В.Б. Бетелина. - М.: НИИСИ РАН, 2001, с. 4-26.

7. Браунли Н., Гатмэн Э., Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21), Jet Info, 2000, 5.

8. Галатенко А.В., О скрытых каналах и не только, Jet Info, 2002, 11.

9. Галатенко В., Макстенек М., Трифаленков И., Сетевые протоколы нового поколения, Jet Info, 1998, 7-8.

10. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель, ГОСТ Р ИСО/МЭК 15408-1-2002 М.: ИПК Издательство стандартов, 2002

11. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности, ГОСТ Р ИСО/МЭК 15408-2-2002 М.: ИПК Издательство стандартов, 2002

12. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности, ГОСТ Р ИСО/МЭК 15408-3-2002 М.: ИПК Издательство стандартов, 2002

13. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации, Москва, 1992

14. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения, Москва, 1992

15. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, Москва, 1992

16. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники, Москва, 1992

17. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности

от несанкционированного доступа к информации, Москва, 1992

18. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, Москва, 1997

19. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий, Москва, 2002

20. Гостехкомиссия России. Руководство по разработке профилей защиты и заданий по безопасности (проект), Москва, 2002

21. Гостехкомиссия России. Руководящий документ. Руководство по регистрации профилей защиты (проект), Москва, 2002

22. Дебопюи Т. (редактор), Дополнение к Руководству по информационной безопасности предприятия: Как выбирать поставщика Интернет-услуг, Jet Info, 2000, 3

23. Профиль защиты для межсетевых экранов корпоративного уровня, Инфосистемы Джет, 2002

24. Профиль защиты для межсетевых экранов провайдерского уровня, Инфосистемы Джет, 2002

25. Управление информационной безопасностью. Практические правила, Приложение к информационному бюллетеню Jet Info

26. Холбрук П., Рейнольдс Дж. (редакторы), Руководство по информационной безопасности предприятия, Jet Info, 1996, 10-11

27. Bainer C., Hines J., Shah S., U.S. Department of Defense Biometric System Protection Profile For Medium Robustness Environments. Version 1.01, DoD Biometrics Management Office, June 29, 2001

28. British Standard. Code of practice for information security management, British Standards Institution, BS 7799:1995

29. British Standard. Information security management systems - Specification with guidance for use, British Standards Institution, BS 7799-2:2002

30. Brownlee N., Guttman E., Expectations for Computer Security Incident Response, Request for Comments: 2350, BCP: 21, June 1998

31. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 2.1, CCIMB-99-031, August, 1999

32. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements. Version 2.1, CCIMB-99-032, August, 1999

33. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements. Version 2.1, CCIMB-99-033, August, 1999

34. Common Methodology for Information Technology Security Evaluation. Part 2: Evaluation Methodology. Version 1.0, CEM-99/045, August, 1999

35. Controlled Access Protection Profile. Version 1.d, U.S. Information Systems Security Organization. U.S. National Security Agency, 8 October 1999

36. Cryptographic Module Validation Program, http://csrc.nist.gov/cryptval/

37. Debeaupuis T. (Editor), Site Security Handbook Addendum for ISPs, Internet Draft, August 1999

38. Department of Defense Trusted Computer System Evaliation Criteria, DoD 5200.28-STD, December 26, 1985

39. Dierks T., Allen C., The TLS Protocol. Version 1.0, Request for Comments: 2246, January 1999

40. Dolan K., Wright P., Montequin R., Mayer B., Gilmore L., Hall C., Final U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments. Version 1.4, U.S. National Security Agency, May 1, 2000

41. FIPS PUB 140-2: Security Requirements for Cryptographic Modules, U.S. Department of Commerce, NIST, May, 25, 2001

42. Fraser B. (Editor), Site Security Handbook, Request for Comments: 2196, FYI: 8, September 1997

43. Harkins D., Carrel D., The Internet Key Exchange (IKE), Request for Comments: 2409, November 1998

44. Holbrook P., Reynolds J. (Editors), Site Security Handbook, Request for Comments: 1244, FYI: 8, July 1991

45. Iachello G., User-Oriented Protection Profile for Unobservable Message Delivery using MIX networks, Revision 2.4, June 6, 1999. http://www.iig.uni-freiburg.de/~giac/User_MIX_PP.pdf

46. Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services., ISO/IEC International Standard 9594-1:2001, ITU-T Recommendation X.500 (2001 E)

47. Information technology - Open Systems Interconnection - The Directory: Models, ISO/IEC International Standard 9594-2:2001, ITU-T Recommendation X.501 (2001 E)

48. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, ISO/IEC International Standard 9594-8:2000, ITU-T Recommendation X.509 (2000 E)

49. Information technology - Open Systems Interconnection - The Directory: Abstract service definition, ISO/IEC International Standard 9594-3:2001, ITU-T Recommendation X.501 (2001 E)

50. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, ISO/IEC 15408-1.1999

51. Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements, ISO/IEC 15408-2.1999

52. Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements, ISO/IEC 15408-3.1999

53. Information technology - Security techniques - Guide for Production of Protection Profiles and Security Targets. Version. 0.9, ISO/IEC PDTR 15446, January 4, 2000

54. Intrusion Detection System Analyser Protection Profile. Draft 3, U.S. National Security Agency. Science Applications International Corporation. Center for Information Security Technology, September 15, 2000

55. Intrusion Detection System Sensor Protection Profile. Draft 3, U.S. National Security Agency. Science Applications International Corporation. Center for Information Security Technology, September 15, 2000

56. Jansen W., Walsh J., Draft U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments. Version 1.b, September, 1998

57. Jansen W., Walsh J., Dolan K., Wright P, Final U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments. Version 1.1, April, 1998

58. Kent S., Atkinson R., IP Authentication Header, Request for Comments: 2402, November

1998

59. Kent S., Atkinson R., IP Encapsulating Security Payload (ESP), Request for Comments: 2406, November 1998

60. Kent S., Atkinson R., Security Architecture for the Internet Protocol, Request for Comments: 2401, November 1998

61. Kohl J., The Kerberos Network Authentication Service (V5), Request for Comments: 1510, September 1993

62. Labeled Security Protection Profile. Version 1.b, U.S. Information Systems Security Organization. U.S. National Security Agency, 8 October 1999

63. Lee A., et. al., Certificate Issuing and Management Components Family of Protection Profiles. Version 1.0, U.S. National Security Agency, October 31, 2001

64. Linn J., Generic Security Service Application Program Interface. Version 2, Update 1, Request for Comments: 2743, January 2000

65. Madson C., Glenn R., The Use of HMAC-MD5-96 within ESP and AH, Request for Comments: 2403, November 1998

66. Madson C., Glenn R., The Use of HMAC-SHA-1-96 within ESP and AH, Request for Comments: 2404, November 1998

67. Maughan D., Schertler M., Schneider M., Turner J., Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments: 2408, November 1998

68. National Computer Security Center. Trusted Network Interpretation, NCSC-TG-005, 1987

69. Protection Profile for Multilevel Operation Systems in Environments Requiring Medium Robustness. Version 1.22, Information Systems Assurance Directorate. U.S. National Security Agency, 23 May 2001

70. Protection Profile For Single-level Operating Systems In Environments Requiring Medium Robustness. Version 1.22, Information Systems Assurance Directorate. U.S. National Security Agency, 23 May 2001

71. Rannenberg K., Iachello G., Protection Profiles for Remailer Mixes, Do the New Evaluation Criteria Help. - Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC'00). - IEEE Press, 2000, pp. 107-118

72. Rational for RBAC Protection Profile. Version 1.0, July 30, 1998

73. Rescorla E. HTTP Over TLS, Request for Comments: 2818, May 2000

74. Reynolds J., Chandramouli R., Role-Based Access Control Protection Profile. Version 1.0, July 30, 1998

75. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, CCITT, Geneva, 1991

76. Sheridan M., Sohmer E., Varnum R., A Goal VPN Protection Profile For Protecting Sensitive Information. Release 2.0, U.S. National Security Agency, 10 July, 2000

77. Smart Card Protection Profile (SCSUG-SCPP). Version 3.0, Smart Card Security User Group, 9 September 2001

78. Smith H., Database Management System Protection Profile (DBMS PP). Version 2.1, Oracle Corporation, May, 2000

79. Stoneburner G., CSPP - Guidance for COTS Security Protection Profiles. Version 1.0. NISTIR 6462, U.S. Department of Commerce, NIST, December, 1999

80. Stoneburner G., CSPP-OS - COTS Security Protection Profile - Operating Systems. Draft Version 0.4, U.S. Department of Commerce, NIST, February 5, 2001

81. Stoneburner G., Rationale for CSPP - COTS Security Protection Profile - Operating Systems. Draft Version 0.4, U.S. Department of Commerce, NIST, February 5, 2001

82. Wray J., Generic Security Service API Version 2: C-bindings, Request for Comments: 2744, January 2000

83. Галатенко В.А., Информационная безопасность - практический подход, Под ред. В.Б. Бетелина. - М.: Наука, 1998. - 301 с.

84. Трубачев А.П. и др., Оценка безопасности информационных технологий, Под общ. ред. В.А. Галатенко. - М.: СИП РИА, 2001. - 356 с.

85. Гайкович В., Першин А., Безопасность электронных банковских систем, М.: "Единая Европа", 1994

86. Russel D., Gangemi G.T. Sr., Computer Security Basics, O'Reilly & Associates, Inc., 1992

87. Буч Г., Объектно-ориентированный анализ и проектирование с примерами приложений на C++, 2-е изд./Пер. с англ. - М.: "Издательство Бином", СПб.: "Невский диалект", 2001. - 560 с.

88. Web-сервер Международной организации по стандартизации, URL: http://www.iso.ch/

89. Web-сервер Международного телекоммуникационного союза, URL: http://www.itu.int/

90. Сервер Тематической группы по технологии Internet, на котором располагаются стандарты и проекты стандартов Internet-сообщества, URL: http://www.ietf.org/

91. Web-сервер с материалами по "Общим критериям", URL: http://www.commoncriteria.org/

92. Web-сервер Федерального агентства правительственной связи и информации при Президенте Российской Федерации, URL: http://www.fstec.ru/

93. Сервер Государственной технической комиссии при Президенте Российской Федерации, URL: http://www.infotecs.ru/gtc/

94. Информационный бюллетень "Jet Info" уделяет много внимания стандартам и спецификациям в области информационной безопасности, URL: http://www.jetinfo.ru/

95. Раздел на сервере Национального института стандартов США, содержащий много материалов по информационной безопасности, в частности, по стандартам и спецификациям в этой области, URL: http://csrc.nist.gov/ , По адресу [MCC] http://csrc.nist.gov/cc/ располагаются материалы по "Общим критериям"

96. Web-сервер Британского института стандартов, URL: http://www.bsi-global.com/

97. Web-сервер с материалами по "Общим критериям", URL: http://csrc.nist.gov/cc/

Содержание