СОДЕРЖАНИЕ

Введение

Обоснование темы диссертационной работы и ее актуальность.

Развитие информационно-коммуникационных технологий (ИКТ) является одним из основных факторов благосостояния и экономического роста страны. Сегодня ИКТ становится одним из основных приоритетов государственной политики Узбекистана [1].

В Постановлении Президента Республики Узбекистан "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий». (Собрание законодательства Республики Узбекистан, 2012 г., № 13, ст. 139) одной из основных задачи дальнейшего внедрения и развития информационно-коммуникационных технологий, в частности, является программа мер по коренному и качественному улучшению функционирования национальной информационно-поисковой системы, увеличению количества ее пользователей [2].

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних нарушителей, так и со стороны внутренних нарушителей.

В последнее время все больше и больше внедряются в нашу повседневную жизнь информационные технологии, пытаясь захватить в ней все: от важнейших государственных проектов до решения обычных бытовых проблем. Вместе с огромной пользой и, казалось бы, неограниченными возможностями новые технологии приносят и новые проблемы. Одной из них является проблема защиты информации от несанкционированного

посягательства теми, кто доступа к этой информации иметь не должен. В связи с этим почти одновременно с развитием информационных и компьютерных технологий начали развиваться и технологии защиты информации, развитие которых с некоторой точки зрения гораздо более критично, чем развитие непосредственно информационных технологий. Ведь с совершенствованием систем защиты, совершенствуются и методы взлома, обхода этих защит, что требует постоянного пересмотра и увеличения надежности защиты информации.

Способов защиты информации существует очень много, но каждый из них всегда можно отнести к одному из двух видов: физическое сокрытие информации от противника и шифрование информации. Зашифрованную информацию можно свободно распространять по открытым каналам связи без боязни ее раскрытия и нелегального использования.

Говоря о системах безопасности, нужно отметить, что они должны не только и не столько ограничивать допуск пользователей к информационным ресурсам, сколько определять и делегировать их полномочия в совместном решении задач, выявлять аномальное использование ресурсов, прогнозировать аварийные ситуации и устранять их последствия, гибко адаптируя структуру в условиях отказов, частичной потери или длительного блокирования ресурсов.

Параллельно с развитием средств вычислительной техники и появлением все новых способов нарушения безопасности информации развивались и совершенствовались средства защиты. Необходимо отметить, что более старые виды атак никуда не исчезают, а новые только ухудшают ситуацию. Существующие сегодня подходы к обеспечению защиты информации несколько отличаются от существовавших на начальном этапе. Главное отличие современных концепций в том, что сегодня не говорят о каком-то одном универсальном средстве защиты, а речь идет о комплексной системы защиты информации (КСЗИ), включающей в себя:

– нормативно-правовой базис защиты информации;

– средства, способы и методы защиты;

– органы и исполнителей.

Другими словами, на практике защита информации представляет собой комплекс регулярно используемых средств и методов, принимаемых мер и осуществляемых мероприятий с целью систематического обеспечения требуемой надежности информации, генерируемой, хранящейся и обрабатываемой на объекте АС, а также передаваемой по каналам. Защита должна носить системный характер, то есть для получения наилучших результатов все разрозненные виды защиты информации должны быть объединены в одно целое и функционировать в составе единой системы, представляющей собой слаженный механизм взаимодействующих элементов, предназначенных для выполнения задач по обеспечению безопасности информации.

Более того, КСЗИ предназначена обеспечивать, с одной стороны, функционирование надежных механизмов защиты, а с другой - управление механизмами защиты информации. В связи с этим должна предусматриваться организация четкой и отлаженной системы управления защитой информации.

Исходя из всего вышесказанного, можно сделать вывод об актуальности выбранной темы диссертационной работы.

Объектом исследования являются информационно-коммуникационные системы.

Предметом исследования являются систем защиты информации.

Методы исследования является методы и средства защиты информации, теория чисел и теория вероятности.

Публикация. По теме диссертации опубликована 1 работа.

Целью диссертационной работы является разработка методики оценки и повышение эффективности информационной безопасности деятельности организаций.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Анализ функционирования комплексной обеспечения защиты информации в деятельности организациях, а также исследование принципы и этапы проектирования защищенных автоматизированных систем.

2. Исследование степени защищенности автоматизированных систем с последующей оценкой эффективности информационной безопасности организаций в информационно-коммуникационных системах.

3. Выбор путей повышения эффективности информационной безопасности в деятельности организациях.

4. Разработка рекомендаций по использованию защищенности информации в организациях.

Краткий анализ литературы по теме диссертации.

Основные вопросы в области исследование методов и средств обеспечения информационной безопасности и методология создания систем защиты информации в работах ученых В.В. Домарева, А.А. Хорева, В.П. Мельникова, С.А. Клейменова, А.М. Петраков и др., а также зарубежных P.D.Coddington, D.Saad. В результате предлагается множество методов и средств защиты информации, и подходы к обеспечению решения проблем информационной безопасности деятельности организаций.

Научная новизна. В результате выполнения диссертационной работы получены следующие новые научные результаты:

1. Разработаны модель оценки эффективности систем защиты информации в организациях, позволяющая оценить степень защищенности информационные системы и осуществить возможных путей улучшения безопасности.

2. Предложен подход к определению номенклатуры контролируемых параметров с целью получения максимальной информации о техническом состоянии (защиты) канала в организациях.

Практическая значимость исследования заключается в том, что разработаны методики оценки эффективности информационной безопасности, позволяющие обеспечить защиту информации от внешних угроз в организациях.

Структура и объем диссертации.

Диссертационная работа состоит из введения, трех глав, заключения, списка использованной литературы и приложений. Основная часть содержит 58 страниц печатного текста, 10 рисунков и 8 таблиц.

Глава I. Анализ функционирования комплексных систем защиты информации в деятельности организаций

1. Этапы проектирования защищенных автоматизированных систем в организациях

Согласно одному из таких стандартов автоматизированных систем(АС) представляет собой систему, состоящую из персонала и комплекса средств автоматизации его деятельности, реализующую информационную технологию выполнения установленных функций.

В зависимости от вида деятельности выделяют следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др.

В зависимости от вида управляемого объекта (процесса) АСУ делят на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д.

В нашем случае АС представляет собой среду обработки информации, и также информационных ресурсов в информационно-телекоммуникационной системе. Поэтому в дальнейшем будем использовать понятие автоматизированная информационная система.

В свою очередь, защита информации в АС - деятельность, которая направлена на обеспечение безопасности обрабатываемой в АС информации и АС в целом, и позволяет предотвратить или осложнить возможность реализации угроз, а также снизить величину потенциальных убытков в результате реализации угроз.

Таким образом, автоматизированная информационная система(АИС) представляет собой сложную систему, которую целесообразно разделять на отдельные блоки (модули) для облегчения ее дальнейшего проектирования. В результате этого, каждый модуль будет независим от остальных, а в комплексе они будут составлять цельную систему защиты.

Выделение отдельных модулей АИС позволяет службе защиты информации:

– своевременно и адекватно реагировать на определенные виды угроз информации, которые свойственны определенному модулю;

– в короткие сроки внедрять систему защиты информации в модулях, которые только что появились;

– упростить процедуру контроля системы защиты информации в целом (под системой защиты информационной инфраструктуры предприятия в целом следует понимать совокупность модулей систем защиты информации).

Постепенно наращивая количество модулей, а также усложняя структуру защиты, АИС приобретает некую комплексность, которая подразумевает использование не одного типа защитных функций во всех модулях, а их произведение.

Таким образом, построение КСЗИ становится неотъемлемым фактором в разработке эффективной системы защиты от несанкционированного доступа.

Согласно КСЗИ – совокупность организационных и инженерных мероприятий, программно-аппаратных средств, которые обеспечивают защиту информации в АС.

Отсюда видно, что, например, простым экранированием помещения при проектировании КСЗИ не обойтись, так как данный метод предполагает лишь защиту информации от утечки по радиоканалу[3].

В общем случае понятие «комплексность» представляет собой решение в рамках единой концепции двух или более разноплановых задач (целевая комплексность), или использование для решения одной и той же задачи разноплановых инструментальных средств (инструментальная комплексность), или то и другое (всеобщая комплексность).

Целевая комплексность означает, что система информационной безопасности должна строиться следующим образом:

– защита информации, информационных ресурсов и систем личности, общества и государства от внешних и внутренних угроз;

– защита личности, общества и государства от негативного информационного воздействия.

Инструментальная комплексность подразумевает интеграцию всех видов и направлений ИБ для достижения поставленных целей.

Современная система защиты информации должна включать структурную, функциональную и временную комплексность.

Структурная комплексность предполагает обеспечение требуемого уровня защиты во всех элементах системы обработки информации.

Функциональная комплексность означает, что методы защиты должны быть направлены на все выполняемые функции системы обработки информации.

Временная комплексность предполагает непрерывность осуществления мероприятий по защите информации, как в процессе непосредственной ее обработки, так и на всех этапах жизненного цикла объекта обработки информации.

2. Классификация автоматизированных систем защиты информации

Нормативным документом предполагается деление АС на 3 класса:

Класс 1 — одномашинный однопользовательский комплекс, который обрабатывает информацию одной или нескольких категорий конфиденциальности. Пример — автономная персональная ЭВМ, доступ к которой контролируется с использованием организационных мероприятий.

Класс 2 — локализированный многомашинный многопользовательский комплекс, обрабатывающий информацию разных категорий конфиденциальности. Пример — локальная вычислительная сеть.

Класс 3 – распределенный многомашинный многопользовательский комплекс, который обрабатывает информацию разных категорий конфиденциальности. Пример — глобальная вычислительная сеть.

Особенности АС класса 1

Информация с ограниченным доступом, а именно: конфиденциальная информация, принадлежащая государству, и информация, содержащая государственную тайну, создается, обрабатывается и хранится в режимно-секретном (РСО) органе[4]. Такая информация, в большинстве случаев, обрабатывается с использованием АС класса 1, которые имеют следующие особенности:

– в каждый момент времени с комплексом может работать только один пользователь, хотя в общем случае лиц, которые имеют доступ к комплексу, может быть несколько, но все должны иметь одинаковые полномочия (права) относительно доступа к обрабатываемой информации;

– технические средства (носители информации и средства ввода/ вывода), с точки зрения, защищенности относятся к одной категории и все они могут использоваться для хранения и/ или ввода/ вывода всей информации.

Для проведения работ, связанных с построением КСЗИ, специалистам организации исполнителя должен быть оформлен допуск к государственной тайне.

При создании КСЗИ используются только те технические средства защиты информации, которые имеют экспертное заключение или сертификат соответствия государственной службы специальной связи и защиты информации, применение других технических средств защиты информации запрещено.

Методика проведения по построению КСЗИ АС класса 1 базируется на следующих исходных данных:

– объект защиты — рабочая станция;

– защита информации от утечки по техническим каналам осуществляется за счет использования рабочей станции в защищенном исполнении или специальных средств;

– защита от несанкционированного доступа к информации осуществляется специальными программными или аппаратно-программными средствами защиты от несанкционированного доступа;

– защита компьютера от вирусов, троянских и шпионских программ — антивирусное программное обеспечение.

Особенности АС класса 2 и 3

В основном в АС класса 2 и класса 3 обрабатывается конфиденциальная или открытая информация, которая принадлежит государству и к которой выдвигаются требования по обеспечению целостности и доступности.

Особенности АС класса 2: наличие пользователей с разными полномочиями по доступу и/или технических средств, которые могут одновременно осуществлять обработку информации разных категорий конфиденциальности. Особенности АС класса 3: необходимость передачи информации через незащищенную среду или, в общем случае, наличие узлов, которые реализуют разную политику безопасности. АС класса 3 отличается от АС класса 2 наличием канала доступа в Интернет. Так же, как и для создания КСЗИ, для создания КСЗИ АС класса 2 и класса 3 организация-исполнитель должна иметь лицензию на проведение работ в сфере технической защиты информации, а также использовать сертифицированные технические средства защиты информации. Методика проведения работ по построению КСЗИ АС класса 2 (3) базируется на следующих исходных данных:

– объектами защиты являются рабочие станции, каналы передачи данных, веб-серверы, периметр информационной системы и т. д;

– защита от несанкционированного доступа осуществляется с помощью базовых средств операционной системы или с использованием специальных программных, аппаратно-программных средств;

– защита каналов передачи данных через незащищенную среду — аппаратные, программные, аппаратно-программные средства шифрования информации;

– защита периметра — программные, аппаратные межсетевые экраны, системы обнаружения атак;

– защита компьютера (сети) от вирусов, троянских и шпионских программ — антивирусное программное обеспечение;

– защита электронного документооборота и электронной почты — использование средств электронной цифровой подписи.

Потребителями КСЗИ АС класса 2 и класса 3 являются органы государственной власти, а также организации, деятельность которых связана с обработкой конфиденциальной информации, принадлежащей государству.

Системы информационной безопасности

Выделяют еще один тип АС – системы информационной безопасности (СИБ).

СИБ представляют собой решение, направленное на обеспечение защиты критичной информации организации от разглашения, утечки и несанкционированного доступа. Как и КСЗИ, СИБ объединяет в себе комплекс организационных мероприятий и технических средств защиты информации.

СИБ в основном предназначены для защиты информации в АС класса 2 и класса 3. Однако между КСЗИ и СИБ есть принципиальные отличия.

Первое отличие заключается в том, что при построении СИБ нет необходимости выполнять требования нормативных документов в сфере технической защиты информации, так как основными потребителями СИБ являются коммерческие организации, которые не обрабатывают информацию, принадлежащую государству. Вторым принципиальным

отличием является отсутствие контролирующего органа, и, как следствие, спроектированная СИБ не требует проведения государственной экспертизы. Еще одно отличие от КСЗИ — свободный выбор технических средств, возможное применение любых аппаратных и программных средств защиты информации. СИБ можно рекомендовать коммерческим организациям, которые заботятся о сохранности своей коммерческой (критичной) информации или собираются принимать меры по обеспечению безопасности своих информационных активов[5]. Для определения необходимости построения СИБ и направления работ по защите информации, а также для оценки реального состояния информационной безопасности организации необходимо проводить аудит информационной безопасности.

Применительно к КСЗИ РСО и КСЗИ АС класса 2 и класса 3 проведение такого аудита тоже является первым этапом работ. Такие работы называются обследованием информационной инфраструктуры организации.

Важным моментом, который касается эксплуатации как КСЗИ АС класса 2 и класса 3, так и СИБ, является тот факт, что недостаточно просто построить и эксплуатировать эти системы защиты, необходимо постоянно их совершенствовать так же, как совершенствуются способы несанкционированного доступа, методы взлома и хакерские атаки.

Сравнительный анализ всех перечисленных систем защиты информации представлен в таблице 1.

Как видно, более жесткие требования выдвинуты к процессу построения КСЗИ и исполнителю этих работ по сравнению с требованиями к построению СИБ.

В дальнейшем, при проектировании системы защиты будем брать за основу АС класса 1 и 2, так как именно эти системы обработки информации представляют наиболее огромный интерес у злоумышленника с точки зрения ее хищения.

Сравнительный анализ систем защиты информации Таблица 1

Особенности	РСО КСЗИ	АС класса 2	СИБ

КСЗИ			
Потребители услуг	Органы государственной власти, коммерческие организации	Органы государственной власти, коммерческие организации	Коммерческие организации
Обрабатываемая информация	Конфиденциальная информация, которая принадлежит государству, или информация, которая содержит государственную тайну	Конфиденциальная информация, которая принадлежит государству (физическому лицу), или открытая информация, которая принадлежит государству	Критическая информация организации (персональная, финансовая, договорная информация, информация о заказчиках)
Субъекты	Заказчик Исполнитель Контролирующий орган	Заказчик Исполнитель Контролирующий орган	Заказчик Исполнитель
Наличие лицензии на проведение работ по построению	Лицензия на проведение работ по технической защите информации	Лицензия на проведение работ по технической защите информации	Не требуется
Проведение государственной экспертизы	Обязательно	Обязательно	Не требуется
Технические средства защиты информации	Только сертифицированные средства защиты информации	Только сертифицированные средства защиты информации	Любые средства защиты информации
Выполнение требований нормативной базы	Обязательно	Обязательно	Не требуется

Порядок создания комплексной системы защиты информации

Создание КСЗИ в ИТС осуществляется в соответствии с нормативным документом системы технической защиты информации на основании технического задания (далее - ТЗ), разработанного согласно требованиям нормативного документа системы технической защиты информации. Кроме того, при проектировании КСЗИ можно руководствоваться стандартом.

В состав КСЗИ входят мероприятия и средства, которые реализуют способы, методы, механизмы защиты информации от:

– утечки техническими каналами, к которым относятся каналы побочных электромагнитных излучений и наводок, акустоэлектрических и других каналов;

– несанкционированных действий и несанкционированного доступа к информации, которые могут осуществляться путем подключения к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, преодоление мероприятий защиты с целью использования информации или навязывания ошибочной информации, применение закладных устройств или программ, использование компьютерных вирусов и т.п.;

– специального влияния на информацию, которое может осуществляться путем формирования полей и сигналов с целью нарушения целостности информации или разрушения системы защиты.

Для каждой конкретной ИТС состав, структура и требования к КСЗИ определяются свойствами обрабатываемой информации, классом АС и условиями ее эксплуатации.

В общем случае, последовательность и содержание научно-исследовательской разработки КСЗИ можно предварительно разделить на 4 этапа (рис.1.).

Несмотря на простоту структуры разработки КСЗИ, большинство организаций придерживается именно этого алгоритма. Однако данный алгоритм – это лишь основа проектирования. Каждый представленный этап отражает множество уровней в ходе проектирования, в зависимости от структуры АС требования, предъявляемых к ее системе защиты. Рассмотрено эти этапы подробнее.

Рис.1 Этапы проектирования КСЗИ

Анализ структуры автоматизированной информационной системы

Данная стадия разработки включает в себя следующие работы:

– проведение предпроектного обследования;

– разработка аналитического обоснования по созданию КСЗИ;

– разработка технического задания на создание КСЗИ.

Для проверки способности информационной системы противостоять попыткам несанкционированного доступа и воздействия на информацию иногда целесообразно выполнять тесты на проникновение.

Существует несколько видов обследования:

– предпроектное диагностическое обследование, которое выполняется при модернизации или построении СЗИ;

– аудит СЗИ на соответствие требованиям внутрикорпоративным стандартам или международным/национальным стандартам. Примером может служить сертификационный аудит системы управления ИБ по ISO 27001;

– специальные виды обследования, например, при расследовании компьютерных инцидентов.

Мировой опыт создания систем защиты для различного рода объектов позволяет выделить три основных элемента, присутствующих практически на любом объекте и требующих обеспечения их безопасности:

– люди - персонал и посетители объекта;

– материальные ценности, имущество и оборудование;

– критичная информация - информация с различными грифами секретности.

Каждый из выделенных элементов имеет свои особенности, которые необходимо учесть при определении возможных угроз. По результатам анализа возможных угроз безопасности АС формируются требования к защите. Полная защита АС формируется из частных требований защиты элементов путем объединения функционально однородных требований по обеспечению защиты[6].

По результатам данного этапа определяются и формируются требования к защите. Полная защита АС формируется из частных требований защиты элементов путем объединения функционально однородных данных по обеспечению защиты. К таким данным относится защищаемая информация на основе документально оформленных перечней защищаемых сведений, угрозы безопасности информации и модель вероятного нарушителя, состав используемых технических средств и связи между ними, состав разработанной организационно-распорядительной документации, класс защищенности АС в защищенном исполнении. Принимаются решения, касающиеся состава технических средств и систем, предполагаемых к

использованию в разрабатываемой системе, и мероприятий по обеспечению конфиденциальности информации на этапе проектирования системы.

3. Принципы защиты информации от несанкционированного доступа в организациях

Проведя оценку необходимости защиты информации от НСД, становится вопрос о дальнейшем направлении проектирования системы защиты информации. Ведь именно по полученным результатам можно судить о сложности проектируемой системы. Имея такие результаты, необходимо оценить вероятность проявляемых угроз на информационную систему, а также сформировать модель нарушителя, после чего следует приступить к формированию защитных мероприятий. Опираясь на требования по защите информации от НСД, которые были рассмотрены ранее, можно привести основные принципы защитных мероприятий от НСД в АС.

Уточним, что одним из основных компонентов АС является автоматизированное рабочее место (АРМ) – программно технический комплекс АС (или средства вычислительной техники (СВТ)), предназначенный для автоматизации деятельности определенного вида. В простейшем случае АРМ представляется как ПЭВМ и работающий на ней пользователь[7].

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки промышленного шпионажа.

Тут же приводятся основные принципы защиты информации от НСД, которые включают в себя:

– обеспечение защиты СВТ комплексом программно-технических средств;

– обеспечение защиты АС комплексом программно-технических средств и поддерживающих их организационных мер.

Однако такие защитные мероприятия необходимо начинать непосредственно с организационных мероприятий. Последние, в рамках системы защиты информации от НСД (СЗИ НСД) в АС, которые обрабатывают или хранят информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

В свою очередь, предлагается закрытие каналов несанкционированного получения информации начинать с контроля доступа пользователей к ресурсам АС. Эта проблема решается путем ряда следующих принципов:

– *Принцип обоснованности доступа.* Данный принцип заключается в обязательном выполнении двух основных условий: пользователь должен иметь достаточную "форму допуска" для получения информации требуемого им уровня конфиденциальности, и эта информация необходима ему для выполнения его производственных функций. Заметим здесь, что в сфере автоматизированной обработки информации в качестве пользователей могут выступать активные программы и процессы, а также носители информации различной степени сложности. Тогда система доступа предполагает определение для всех пользователей соответствующей программно-аппаратной среды или информационных и программных ресурсов, которые будут им доступны для конкретных операций.

– *Принцип достаточной глубины контроля доступа*. Средства защиты информации должны включать механизмы контроля доступа ко всем видам информационных и программных ресурсов АС, которые в соответствии с принципом обоснованности доступа следует разделять между пользователями.

– *Принцип разграничения потоков информации*. Для предупреждения нарушения безопасности информации, которое, например, может иметь место при записи секретной информации на несекретные носители и в несекретные файлы, ее передаче программам и процессам, не предназначенным для обработки секретной информации, а также при передаче секретной информации по незащищенным каналам и линиям связи, необходимо осуществлять соответствующее разграничение потоков информации.

– *Принцип чистоты повторно используемых ресурсов*. Данный принцип заключается в очистке ресурсов, содержащих конфиденциальную информацию, при их удалении или освобождении пользователем до перераспределения этих ресурсов другим пользователям.

– *Принцип персональной ответственности*. Каждый пользователь должен нести персональную ответственность за свою деятельность в системе, включая любые операции с конфиденциальной информацией и возможные нарушения ее защиты, а также за случайные или умышленные действия, которые могут привести к несанкционированному ознакомлению с конфиденциальной информацией, ее искажению или уничтожению, либо исключению возможности доступа к такой информации законных пользователей.

– *Принцип целостности средств защиты*. Данный принцип подразумевает, что средства защиты информации в АС должны точно выполнять свои функции в соответствии с перечисленными принципами и быть изолированными от пользователей, а для своего сопровождения должны включать специальный защищенный интерфейс для средств контроля, сигнализации о попытках нарушения защиты информации и воздействия на процессы в системе

Реализация перечисленных принципов осуществляется с помощью так называемого "монитора обращений", контролирующего любые запросы к данным или программам со стороны пользователей (или их программ) по

установленным для них видам доступа к этим данным и программам. Схематично такой монитор можно представить в виде, показанном на рис.2.

Рис.2 Структура монитора обращений

Практическое создание монитора обращений, как видно из приведенного рисунка, предполагает разработку конкретных правил разграничения доступа в виде так называемой модели защиты информации.

Спроектировав модель защиты информации, необходимо проверить ее в действии. Однако реализация такой модели будет стоит заказчику больших затрат, если вдруг при ее реализации одна или несколько защитных функций системы не окажется эффективной. Поэтому целесообразно будет провести математический анализ эффективности защитных организаций.

Выводы по первой главе

Установлен перечень основных нормативно-правовых документов регламентирующих проектирование автоматизированных систем в защищенном исполнении. На основании этих документов, проведен анализ автоматизированных систем, в результате которого существует 3 класса таких систем по степени сложности и доступа к информации, циркулирующей в них. Проанализированы особенности каждого класса автоматизированных систем. Наиболее требовательными к защите являются 1-й и 2-й классы. Установлено, что для проектирования эффективной системы защиты необходимо АИС (Автоматизированная информационная система) представить в виде различных модулей. В результате этого, используемые защитные мероприятия для каждого модуля будут независимы друг от друга, а в целом система защиты будет являться комплексной. Формирован порядок создания КСЗИ(Комплексная система защиты информации). Установлено, что такая разработка обычно состоит из четырех этапов. Наиболее ответственным является третий этап, так как именно на данном этапе реализуются все защитные мероприятия по требованиям и техническому решению, принятым на предыдущих этапах. Были анализированы основные принципы защищенности организаций от несанкционированного доступа в АС, на основании которого установлено, что реализация таких принципов осуществляется с помощью так называемого "монитора обращений".

Глава II. Разработка методики оценки эффективности информационной безопасности информационно-коммуникационных систем в организациях

1. Подходы к оценке эффективности безопасности информационно-коммуникационных систем в деятельности организаций

Оценка эффективности является важным элементом разработки проектных и плановых решений, позволяющим определить уровень прогрессивности действующей структуры, разрабатываемых проектов или плановых мероприятий и проводится с целью выбора наиболее рационального варианта структуры или способа ее совершенствования. Эффективность защитных мероприятий (ЗМ) должна оцениваться на стадии проектирования, для получения наилучших показателей работоспособности системы в целом.

В общем случае эффективность ЗМ оценивается как на этапе разработки, так и в процессе эксплуатации системы защиты. В оценке эффективности ЗМ, в зависимости от используемых показателей и способов их получения, можно выделить три подхода:

- классический;
- официальный;
- экспериментальный.

Под классическим подходом к оценке эффективности понимается использование критериев эффективности, полученных с помощью показателей эффективности. Значения показателей эффективности получаются путем моделирования или вычисляются по характеристикам реальной ИКС. Такой подход используется при разработке и модернизации КСЗИ. Однако возможности классических методов комплексного оценивания эффективности применительно к ЗМ ограничены в силу ряда причин. Высокая степень неопределенности исходных данных, сложность формализации процессов функционирования, отсутствие общепризнанных методик расчета показателей эффективности и выбора критериев

оптимальности создают значительные трудности для применения классических методов оценки эффективности.

Большую практическую значимость имеет подход к определению эффективности ЗМ, который условно можно назвать официальным. Политика безопасности информационных технологий проводится государством и должна опираться на нормативные акты. В этих документах необходимо определить требования к защищенности информации различных категорий конфиденциальности и важности.

Под экспериментальным подходом понимается организация процесса определения эффективности существующих КСЗИ путем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников[8]. Такие исследования проводятся следующим образом. В качестве условного злоумышленника выбирается один или несколько специалистов в области информационной борьбы наивысшей квалификации. Составляется план проведения эксперимента. В нем определяются очередность и материально-техническое обеспечение проведения экспериментов по определению слабых звеньев в системе защиты. При этом могут моделироваться действия злоумышленников, соответствующие различным моделям поведения нарушителей: от неквалифицированного злоумышленника, не имеющего официального статуса в исследуемой ИКС, до высококвалифицированного сотрудника службы безопасности.

Принципиальное значение для оценок эффективности защитных мероприятий имеет выбор базы для сравнения или определение уровня эффективности, который принимается за нормативный. Здесь можно указать несколько подходов, которые могут дифференцированно использоваться применительно к конкретным случаям. Один из них сводится к сравнению с показателями, характеризующими эффективность организационной структуры эталонного варианта системы защиты. Эталонный вариант может быть разработан и спроектирован с использованием всех имеющихся

методов и средств проектирования систем защиты, на основе передового опыта и применения прогрессивных организационных решений. Характеристики такого варианта принимаются в качестве нормативных, при этом сравнительная эффективность анализируемой или проектируемой системы определяется на основе сопоставления нормативных и фактических (проектных) параметров системы с использованием преимущественно количественных методов сравнения. Может применяться также сравнение с показателями эффективности и характеристиками системы управления, выбранной в качестве эталона, определяющего допустимый или достаточный уровень эффективности организационной структуры.

Однако возникают некоторые трудности применения указанных подходов, которые обусловлены необходимостью обеспечения сопоставимости сравниваемых вариантов. Поэтому часто вместо них используется экспертная оценка организационно-технического уровня анализируемой и проектируемой системы, а также отдельных ее подсистем и принимаемых проектных и плановых решений, или комплексная оценка системы защиты, основанная на использовании количественно-качественного подхода, позволяющего оценивать эффективность ЗМ по значительной совокупности факторов. Экспертная оценка может являться составным элементом комплексной оценки эффективности системы защиты, включающей все перечисленные подходы как к отдельным подсистемам, так и к системе в целом.

Эффективность систем оценивается с помощью показателей эффективности. Иногда используется термин - показатель качества. Показателями качества, как правило, характеризуют степень совершенства какого-либо товара, устройства, машины. В отношении сложных человеко-машинных систем предпочтительнее использование термина показатель эффективности функционирования, который характеризует степень соответствия оцениваемой системы своему назначению.

Определение показателя эффективности возможно двумя общенаучными методами: экспериментом (испытанием) и математическим моделированием (в настоящее время часто называют вычислительным экспериментом).

Применительно к защите информации показатели по значимости ("снизу вверх") разделяются так: технические - информационные (датчиковые) - системные - надсистемные (ценностные). Физически, применительно к защите информации от утечки, этот ряд выглядит так: сигнал / шум - вероятность обнаружения объекта – источника информации - вероятность его вскрытия - ущерб от утечки информации. При этом все частные показатели между собой функционально связываются.

Для того чтобы оценить эффективность системы защиты информации или сравнить системы по их эффективности, необходимо задать некоторое правило предпочтения. Такое правило или соотношение, основанное на использовании показателей эффективности, называют критерием эффективности. Для получения критерия эффективности при использовании некоторого множества k-показателей используют ряд подходов. Обычно при синтезе системы возникает проблема решения задачи с многокритериальным показателем.

Так как определение эффективности систем защиты информации относится к задачам многокритериальной оценки, то такую сложную систему невозможно достаточно правильно охарактеризовать с помощью единственного показателя[9]. Соответственно применение при оценке эффективности защиты системы множества показателей будет характеризовать эффективность наиболее полно. При использовании известных методик оценки угроз есть определённые недостатки, которые не дают полной картины оценки эффективности защиты системы. К таким недостаткам относятся те оценки, которые имеют следующие характеристики методик:

а) Результаты характеристик представлены как шкалы оценок потенциальных угроз и их последствий. Такая методика имеет приближённые значения показателей, основанные на анализе имеющейся статистики нарушений или на экспертных оценках. Для определения значений показателя необходим значительный объём статистического материала, значит оценка не может быть использована для оценки эффективности и выбора мер защиты информации.

б) *Ri10(S□V-4)*, где показатель частоты возникновения угрозы S выбирается из интервала [0,7], 0 – соответствует случаю, когда угроза почти не возникает, 7 – угроза возникает тысячу раз в год, V – показатель ущерба, который назначается в зависимости от S и принимает значения от 1 до 1 млн. долл. Оценка очень приближённая, и для определения значений показателя необходим значительный объём статистического материала, показатель не может быть использован для оценки эффективности и выбора мер защиты информации.

в) $SR_{(s,r)} = \frac{1}{n} \sum_{i=1}^{n} W_i G_i$

где W_i – субъективный коэффициент важности j-ой характеристики СЗИ (системы защиты информации); G_i – назначенное экспертным путём значение каждой из характеристик; n – количество характеристик. Выражение позволяет получить приближённую оценку эффективности системы защиты информации. Может быть использован при отсутствии необходимых исходных данных для более точной и достоверной оценки, но имеет субъективный коэффициент важности, что не даёт возможности использования метода в системах, где мера степени безопасности системы указана явно.

г) Оценка угроз: L – средний показатель появления угроз (случайная величина с распределением вероятности f(L)). Для оценки ущерба: случайная величина m со средним отклонением V . L определяется на основе анализа статистики нарушений или экспертным путём; m – определяется на основе

анализа статистики нарушений или экспертным путём. Для оценки ущерба необходимо иметь статистику нарушений безопасности и измеренные значения ущерба в результате этих нарушений. Невозможно учесть влияние средств защиты информации на L и соответственно на m, а следовательно, и оценить эффективность мер защиты информации[10].

При использовании счётного множества показателей $W \square \{W_i\}, i \square 1,n$, где n – количество показателей, оценка эффективности будет наиболее полной с учётом правильности выбора критериев оценки и количества выбранных показателей.

Из основных подходов к многокритериальной оценке эффективности сложных систем видно, что они сводятся к свертыванию множества частных показателей W_i к единственному интегральному показателю W_0 или использованию методов теории многокритериального выбора и принятия решений при наличии значительного числа частных показателей эффективности, приблизительно одинаково важных.

При подходе к оценке эффективности, в которой эффективность выражается в нечётких показателях защиты информационной системы, в виде лингвистических переменных, таких, как: «абсолютно незащищённая», «недостаточно защищённая», «защищённая», «достаточно защищённая», «абсолютно защищённая», выстраивается необходимая и достаточная картина защищённости системы от НСД (несанкционированного доступа к информации) как в качественной, так и в количественной оценке, что в свою очередь является положительным свойством, имеющим превосходство над вышеперечисленными известными методиками.

В такой методике принадлежность определённого уровня безопасности будет определятся на промежутке [0, 1], и показатели надёжности будут функцией принадлежности $м^A (x_i)$, где x_i – есть элемент множества X – требования безопасности, а A – множество значений, определяющих выполнение требований безопасности в той или иной мере, и определяемое как:

$$A = \frac{\mu^{A}(x_1)}{x_1} + \frac{\mu^{A}(x_2)}{x_2} + \ldots + \frac{\mu^{A}(x_n)}{x_n} = \sum_{i=1}^{n} \frac{\mu^{A}(x_i)}{x_i},$$

где $\frac{\mu^{A}(x_i)}{x_i}$ пара «функция принадлежности \ элемент». Тогда возможно производить оценку эффективности по чётко определённым критериям безопасности следующим образом.

Пусть X={1, 2, 3, 4, 5} есть заданные наборы требований защиты системы, тогда нечёткое множество оценки защищённости системы, имеющей определённые критерии безопасности, будет:

A = 0,2/1 + 0,4/2 + 0,6/3 + 0,8/4 + 1/5.

Это следует интерпретировать так, что система, имеющая набор выполненных требований «1», относится к «абсолютно незащищённой», система, имеющая набор выполненных требований «2», относится к «недостаточно защищённой», система, имеющая набор выполненных требований «3», относится к «защищённой», система, имеющая набор выполненных требований «4», относится к «достаточно защищённой», система, имеющая набор выполненных требований «5», относится к «абсолютно защищённой». Причём набор «5» относится к «абсолютно защищённой» системе и т.д. Разные состояния безопасности системы выделяются в виде подмножеств нечёткого множества A. Вероятность взлома оцениваемой системы может соответствовать кардинальному числу (мощности) нечёткого множества, а именно: если X={1, 2, 3, 4, 5} и A = 0,2/1 + 0,4/2 + 0,6/3 + 0,8/4 + 1/5, то Card A = |A|= 3, т.е. вероятность взлома будет 3k, где k – коэффициент соответствия.

Каждый терм имеет определённые значения на промежутке [0, T], где T – максимальное количество требований, определённых в системе защиты информации. Так, набор требований может быть на промежутке [0, 20], и

соответственно набор «1» будет множеством выполненных требований, например, [0, 4].

Очевидно, что при таком подходе для оценки эффективности защищённости АС от НСД необходимы только данные о необходимых требованиях защищённости и данные о полноте выполнения этих требований. Предлагаемая методика даёт возможность её применения при оценке эффективности защищённости системы с помощью определённых нейросетевых приложений.

При использовании методики совместно с программно-аппаратным комплексом можно достичь:

– постоянного мониторинга состояния информационной безопасности АС;

– прогнозирования возможности осуществления атак путём имитации угроз (предполагается наличие множества Q[1, q], где q – максимальное количество угроз);

– существенного затруднения или предотвращения реализации угрозы или множества угроз, которые существуют при невыполнении некоторых требований из промежутка [0, T];

– изменения наборов требований для стремления системы защиты к лингвистической переменной «абсолютно защищённая».

Комплекс также может обладать возможностью перевода состояния системы безопасности к более высокому уровню эффективности защиты.

2. Построение алгоритма повышения эффективности системах защиты информации на основе математического анализа

Любая система безопасности представляет собой организационно оформленные кадровые и материально-технические ресурсы и действует всегда во времени и пространстве угроз. Пространство угроз образуют объекты защиты - люди, работающие в коммерческой структуре, имущество и

денежные средства предприятия, сведения, составляющие коммерческую или служебную тайну. Главная функция системы безопасности - противодействие угрозам с помощью людей и техники. Каждая угроза влечет за собой ущерб, а противодействие призвано снизить его величину, в идеале - полностью. Удается это далеко не всегда. Способность системы безопасности выполнять свою главную функцию всегда должна оцениваться количественно. К примеру, можно измерить относительный ущерб, предотвращенный на рис.1.

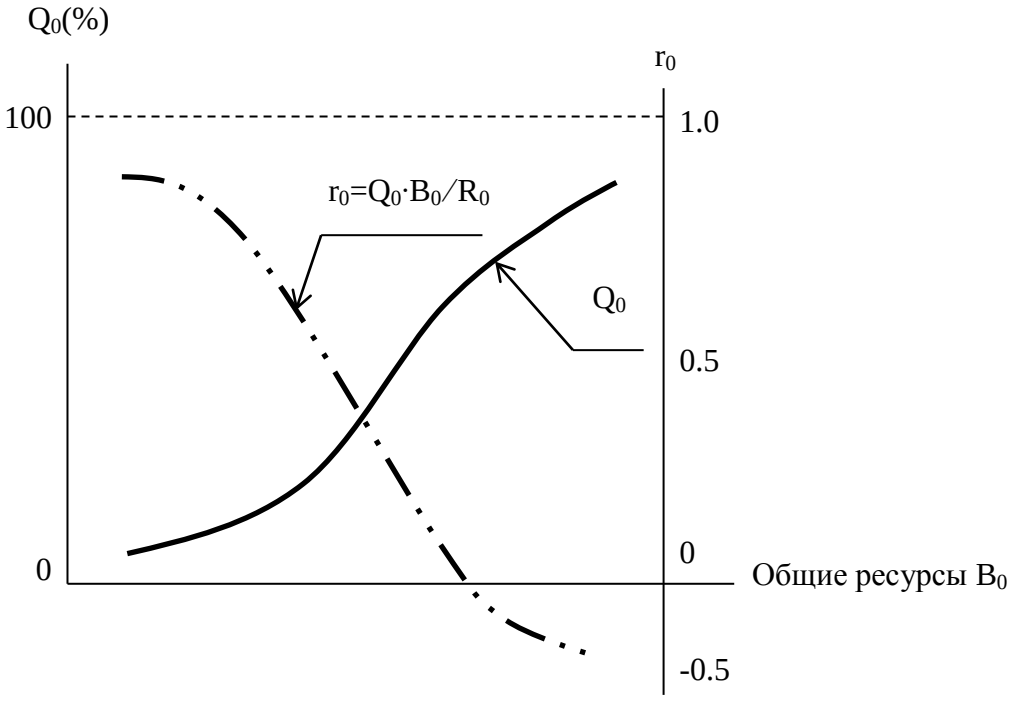


Рис.1 Типичная зависимость эффективности Q_0 и рентабельности r_0 защиты от общих ресурсов

Величина Q_0 - мера общей эффективности защиты. Чем больше Q_0, тем меньший ущерб создадут угрозы. Таким образом, мерой риска является величина$(1—Q_0)$. Стремление обеспечить высокоэффективную защиту, когда Q_0 близко к 1 (или 100%), вполне естественно, но это потребует значительных расходов на ресурсы. То есть чем выше совокупные ассигнования (B_0) на ресурсы, тем на большую эффективность защиты можно рассчитывать. Возникшая при этом зависимость видна на рис.2.3. Однако чрезмерные расходы на собственную безопасность не всегда оправданны

экономически. Можно столкнуться с ситуацией, когда стоимость защиты (B_0) превысит уровень (R_0) максимального ущерба от реализации угроз. В этом случае возникает опасность угрозы «саморазорения» от защиты. Ее уровень также можно оценить, к примеру, величиной r разности относительного «защищенного» ущерба Q_0 и относительных затрат B_0/P_0 на ресурсы. Назовем эту величину рентабельностью защиты. Если она положительная (т.е. $B_0<=P_0Q_0$), то защита рентабельна. В отличие от эффективности, чем больше затраты (B_0), тем меньше рентабельность[11]. Эта противоположность создает неоднозначную ситуацию в выборе стратегии защиты.

Рассмотрим типовую зависимость эффективности защиты (Q_0) и ее рентабельности (r_0) от максимального ущерба R_0 (рис.2.).

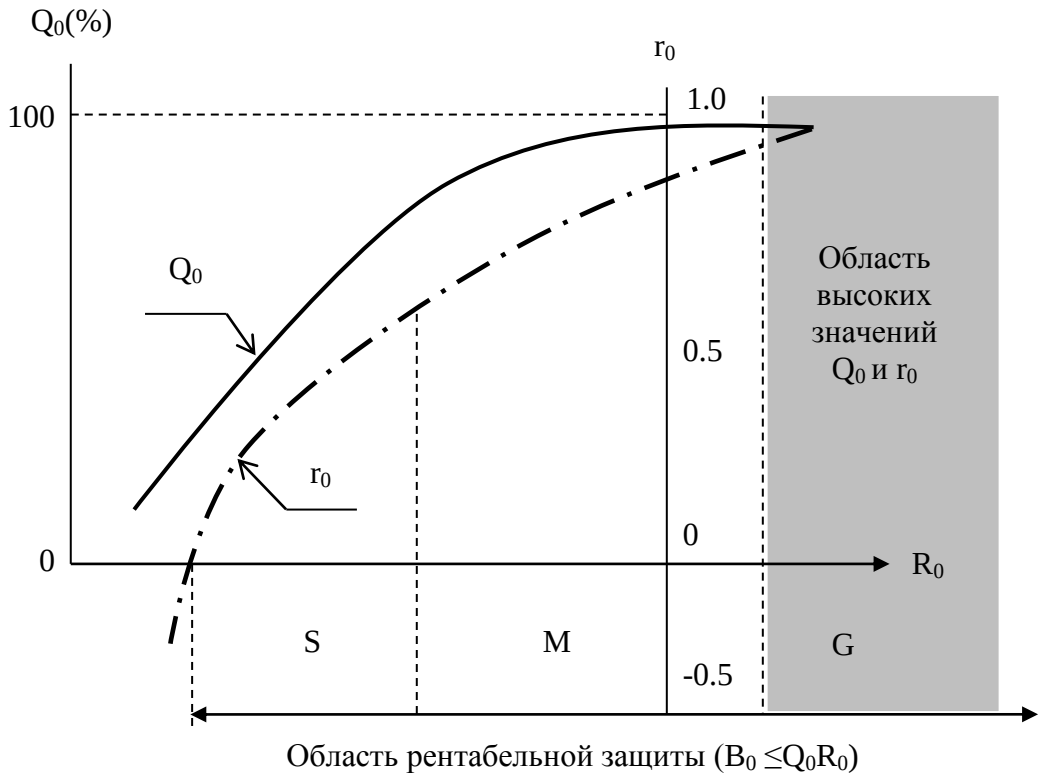


Рис.2 Зависимость эффективности и рентабельности защиты от максимального ущерба R_0

По сути, это является мерой масштабности бизнеса. Нетрудно увидеть, что сделать защиту одновременно и высокоэффективной, и высокорентабельной под силу лишь крупным коммерческим структурам (область G), для которых характерны большие величины максимального ущерба. Достаточно, например, чтобы $B_0=R_0(l-Q_0)$.Тогда при $r\rightarrow l, Q_0\rightarrow l$. В худшем положении оказываются

интересы среднего (область M) и малого (область S) бизнеса, поскольку из-за ограниченности ресурсов выбор стратегии защиты более сложен. Здесь рекомендации просты. Надо обеспечить максимально возможную эффективность при положительном показателе рентабельности защиты. То есть в первую очередь следует противодействовать наиболее вероятным и опасным угрозам. В любом случае нельзя забывать об экономии ресурсов. Совершенно ясно, что выбор стратегии защиты облегчается, если при меньших затратах удастся обеспечить равную или даже большую эффективность защиты.

Очевидны и источники экономии затрат: использование более экономичных средств и решений универсального характера; рациональное распределение ресурсов и более совершенные формы управления ими; привлечение кооперативных форм обеспечения безопасности и др. В противном случае защита может себя не оправдать. Поэтому надо иметь в виду, что экономии ресурсов в этих условиях будут способствовать кооперативные формы защиты в рамках единой местной или региональной системы безопасности.

Выгоду кооперативных форм противодействия угрозам иллюстрирует рис.3.

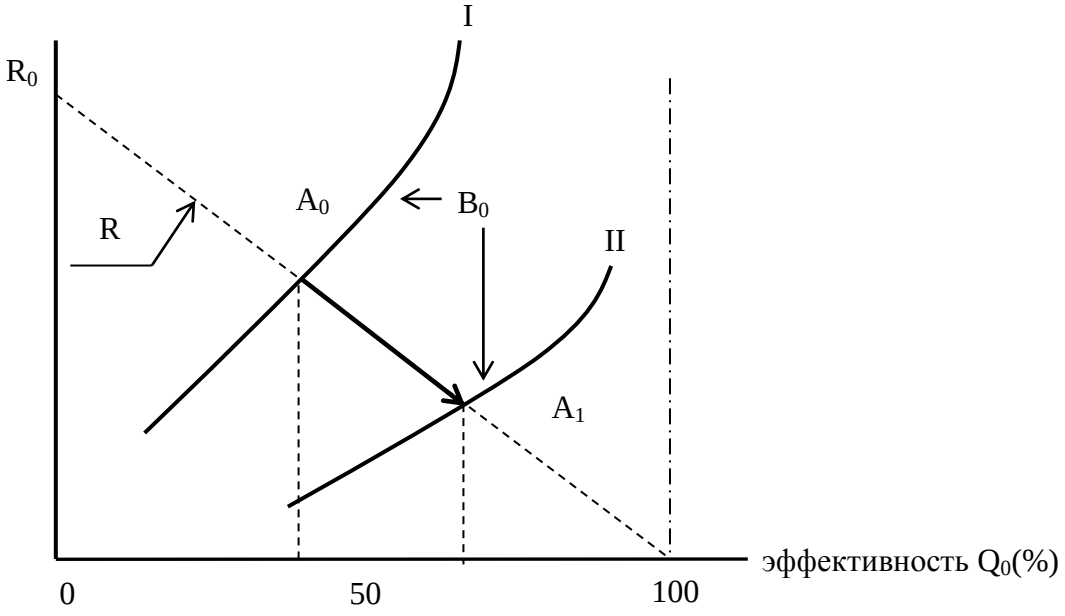


Рис.3 Характерные зависимости риска R и расходов на ресурсы B_0 как функций от эффективности защиты Q_0

На нем представлены характерные зависимости величины риска ($R=R_0(1-Q_0)$ и общих затрат (B_0) на ресурсы от эффективности автономной (I)

и кооперативной (II) защиты. Точка пересечения (A_0) зависимостей R(Q) и B(Q) для автономной защиты соответствует примерно области минимальных общих потерь

$R_0(1-Q_0)+B_0$. Экономия ресурсов выразится в том, что исходная зависимость (I) окажется «выше» новой зависимости (II), которая отображает кооперацию в использовании ресурсов. Соответственно новая точка пересечения кривых (A_1) окажется правее прежней (A_0). Практически это означает, что при сохранении рентабельности защиты увеличивается ее эффективность. Причем выигрыш тем существенней, чем больше экономия. На практике в основном кооперируются по двум формам - материально-техническим и кадровым ресурсам, которые и являются составными частями общего. Что касается первой формы, то она характерна для ситуаций, когда пространство угроз не расширяется. Иными словами, объединяются лишь материально-технические средства одного и того же предприятия, но предназначенные для различных целей.

В качестве примера можно назвать комплексную систему имущественной и информационной защиты. К общим средствам можно отнести контрольно-пропускную систему, средства ограничения доступа, телевизионные и другие системы выявления и верификации угроз, средства пожаротушения и др. Эта форма эффективна лишь для крупного бизнеса. Вторую форму, то есть кооперацию по кадровым ресурсам, используют в основном при решении проблемы безопасности на региональном уровне, когда пространство угроз намеренно расширяется (рассматриваются несколько коммерческих предприятий в одном регионе). В этом случае объединение происходит лишь на уровне сил так называемого быстрого реагирования. Именно такие силы противодействуют несанкционированным и силовым проникновениям, терроризму, пожару и т.п.

Любая угроза и противодействие ей происходят, естественно, во времени и характеризуются определенными его масштабами. Исходя из этого ущерб от реализации угроз будет определяться тем, насколько полно данные

события пересекаются во времени[12]. Самый нежелательный вариант - запаздывающее противодействие, когда реакция системы защиты начинается к моменту завершения угрозы или после нее. Он характерен для систем информационной защиты. Несколько лучший вариант - одновременное противодействие, то есть оно начинается с появлением угрозы. И, наконец, наилучший - противодействие, носящее опережающий характер: реакция системы защиты начинается до начала реализации угрозы. Основанием для реакции могут быть оперативные данные, сигналы тревоги раннего оповещения и т.п.

На рис.4. представлена характерная зависимость эффективности защиты от относительного времени реакции системы (T_p/T_y) для всех трех вариантов противодействия.

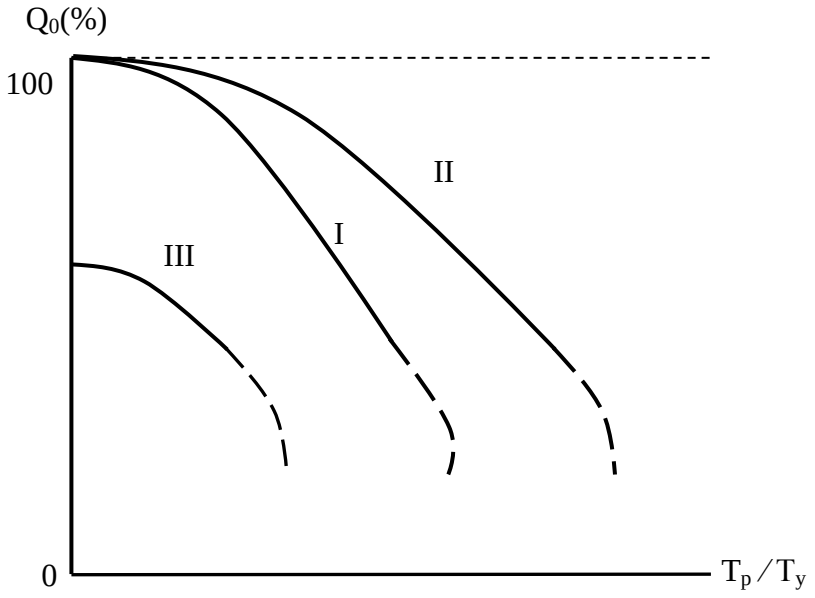


Рис.4 Зависимость эффективности защиты Q_0 от относительного времени T_p/T_y реакции системы с одновременным (I), опережающим (II) и запаздывающим (III) противодействием

Основные выводы и рекомендации очевидны. Одновременное противодействие будет достаточным для высокоэффективной защиты от угрозы, если реакция на нее будет быстрой. Эта задача вполне реальна для объектов большого бизнеса. Кооперативные же формы противодействия в условиях медленной реакции на угрозы не принесут эффекта, если отсутствуют средства задержки и блокирования угроз. Говоря о тактических вопросах системы безопасности бизнеса в части технических каналов связи,

прежде всего имеют в виду скорость ее реакции, надежность решений, блокирование развития угроз и их ликвидацию. Особенно важно обеспечить жесткие требования к надежности всех систем защиты, которая зависит от времени их функционирования и периодичности обновления ресурсов. Если это время превышает 5 лет, то требование надежности реализуется несколькими способами, среди которых - резервирование решений, многорубежность защиты, автоматизация первичных решений, централизованное управление ресурсами в кризисных ситуациях и т.п. Прежде чем определиться в вопросах тактики, надо помнить, что она должна соответствовать стратегии и опираться на точный количественный анализ. Для объектов среднего и малого бизнеса такой анализ вполне реален даже без средств автоматизации. Однако необходимо привлечь специалистов и экспертов, которые бы проанализировали обстановку и свойства защищаемого объекта, разработали модель угроз, изучили рынок существующих средств и методов. Эти данные и помогли бы оценить саму систему и при необходимости модернизировать ее.

3. Разработка моделей оценки эффективности системах защиты информации в организациях

Насколько важна любая информация, относящаяся к бизнесу понятно многим. Пользуясь собранной и обработанной информацией, можно успешно конкурировать на своем рынке и захватывать новые. Информация помогает в поиске партнеров и способствует четкому определению позиции по отношению к ним. Кроме того, при переходе к рыночной экономике информация становится товаром и должна поэтому подчиняться специфическим законам товарно-рыночных отношений. В этих условиях проблема защиты информации весьма актуальна и для организаций любой формы собственности. Вопросы безопасности - важная часть концепции внедрения новых информационных технологий во все сферы жизни

общества. Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально-распределенной сети, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Системный подход обеспечивает адекватную многоуровневую защиту информации, рассматриваемую как комплекс организационно-правовых и технических мероприятий. Кроме того, при реализации механизмов защиты должны использоваться передовые, научно обоснованные технологии защиты, обеспечивающие требуемый уровень безопасности, приемлемость для пользователей и возможность наращивания и модификации СЗИ в дальнейшем.

Следовательно, при моделировании информационной системы (ИС) организация необходимо учитывать угрозы защиты информации и методы противодействия угрозам. Для этого следует разработать модель системы защиты информации, отвечающую определенным требованиям в зависимости от потребностей ИС. Для этого разумно будет использовать системный подход, анализ существующих систем и их недостатки.

Анализ подходов к моделированию систем защиты информации показал, что ни одна из представленных моделей не удовлетворяет в полной мере основным критериям. Таким образом, анализ моделей средств защиты информации показывает, что ни один из подходов в полной мере не отвечает предъявляемым требованиям. Модели в основном используются на этапе эксплуатации и сопровождения. Также некоторые модели используются и на этапе проектирования ИС, но только для получения частных оценок уровня защищенности ИС.

Разработка комплекса моделей

Для решения всех задач поставленных перед разрабатываемой моделью СЗИ организации, предлагается реализовывать её в виде комплекса моделей.

Архитектура разработанного комплекса моделей представляет собой иерархическую структуру, отображенную на рис.5.

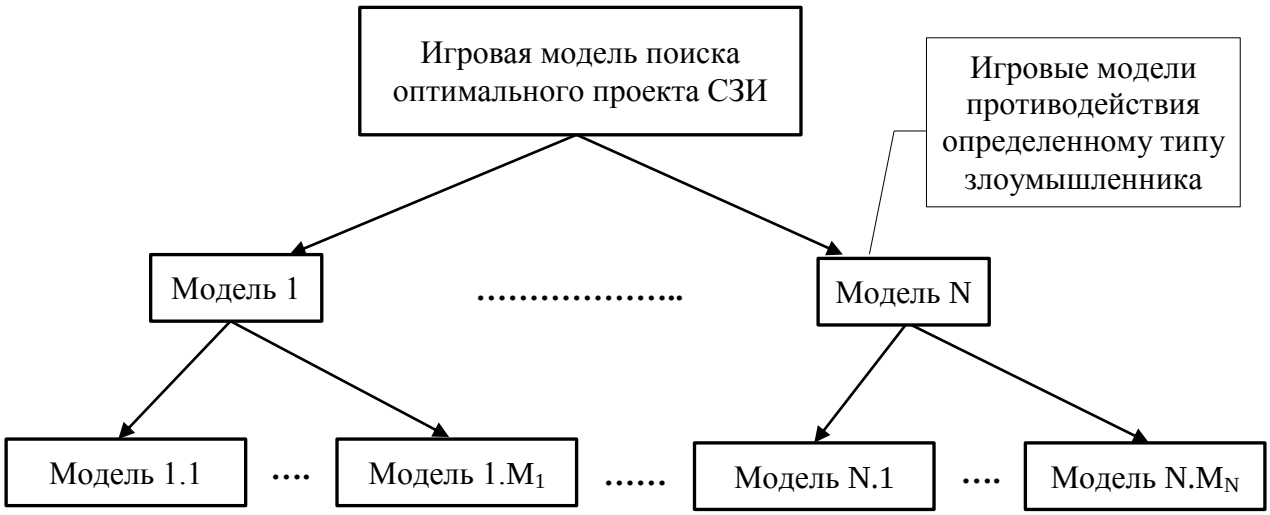


Рис.5 Иерархическая структура комплекса моделей

Во главе иерархии находится игровая модель поиска оптимального проекта. Исходными данными для данной модели являются показатели обобщенных рисков при противодействии определенному типу злоумышленника и вероятности атаки со стороны того или иного типа злоумышленника. Вероятности атаки должны быть определены отдельно, а показатели обобщенных рисков поставляют модели, лежащие на среднем уровне иерархии - игровые модели противостояния определенному типу злоумышленника, для которых, в свою очередь, исходными данными являются риски, связанные с реализацией злоумышленником той или иной угрозы, и вероятности того, что злоумышленник будет пытаться осуществить именно эту угрозу. Вероятности нацеленности злоумышленника на реализацию угрозы определяются отдельно, а значения рисков поставляются моделями низшего уровня - полумарковскими моделями реализации угроз.

Разработка модели злоумышленника

Модель исследования оптимальности проекта системы защиты информации предполагает построение модели злоумышленника. Как известно злоумышленники могут быть разных типов[13]. Они могут быть внутренними и внешними, они могут отличаться по уровню подготовки, по

уровню оснащения, по целям, которые они перед собой ставят и т.д. Следовательно, необходимо разработать модель злоумышленника, которая формально описывала бы все разнообразие существующих типов злоумышленников.

В рамках описанного комплекса моделей для исследования оптимальности проекта системы защиты информации - модель злоумышленника представляет собой множество

$$\mathrm{M} = \{\{\mathrm{T}\}, \{M^{param}\}, P_k\},$$

где: $\{\mathrm{T}\} -$ множество угроз доступных злоумышленнику. При этом элемент Т из множества {Т} представляет собой следующее

$$\mathrm{T}; = \{\mathrm{Pт}, \{\mathrm{VI}\}, \{\mathrm{E}\}\},$$

где: Рт - вероятность выбора данной угрозы злоумышленником для эксплуатации; $\{\mathrm{VI}\}$ −множество уязвимостей системы защит информации, причем элемент $\mathrm{VI}_j -$ из множества {VI} представляет собой следующее

$$\mathrm{VI}_j = \{P_{init}, S_{param}\},$$

где: $P_{init}, -$ вероятность инициализации; S_{param} − ножество требований к злоумышленнику. $\{\mathrm{E}\} -$ множество переходов между уязвимостями защиты информации, причем элемент E_j из множества {Е} представляет собой следующее

$$E_i = \{P_i^{\text{перех}}, P_i^{\text{усп}}, \mu, \sigma\},$$

где: $P_i^{\text{перех}} -$ вероятность выбора пути по данному переходу; $P_i^{\text{усп}}$ −вероятность успеха; $\mu,\ \sigma -$ параметры логнормального закона распределения вероятности пребывания в предыдущем состоянии при выборе пути по данному переходу; S_{param} −множество требований к злоумышленнику. $\{S_{param}\} -$ множество параметров злоумышленника; P_k −вероятность столкновения системы защиты именно с данным типом злоумышленника.

Выводы по второй главе

Исследованы основные подходы к оценки эффективности защитных организаций в АС. К их числу относятся:

– классический;

– официальный;

– экспериментальный.

Установлено, что для оценки эффективности защитных организаций в ИКС наиболее целесообразно выбирать многокритериальные показатели. Разработан подход к оценке эффективности информационной безопасности организаций АС от НСД, для реализации которого достаточно иметь только данные о необходимых требованиях защищённости и данные о полноте выполнения этих требований. Для повышения эффективности используемых защищенности организаций был проведен их математический анализ. На основании такого анализа установлено, что реализация защищённых организаций для каждого объекта различна, соответственно и эффективность таких мероприятий от НСД для одних объектов будет выше (объекты большого бизнеса), а для других ниже (объекты малого бизнеса). Приведен сравнительный анализ различных моделей СЗИ, выявлены основные плюсы и минусы каждой.

Глава III. Выбор уровня защищенности системах защиты информации и разработка рекомендации по повышению эффективности работы пользователей в деятельности организации

1. Выбор контролируемых параметров по максимальным значениям с учетом защиты канала и по заданному коэффициенту готовности

Выбор параметров для контроля по информативным признакам достаточно сложен и требует обширных фактических данных.

Для инженерных расчетов приемлемыми являются методы линейного и динамического программирования.

Рассмотрено применение линейного программирования для определения номенклатуры контролируемых параметров с целью получения максимальной информации о техническом состоянии (защиты) канала при заданном коэффициенте готовности и выполнении ряда ограничений (например, стоимость контроля, масса, габариты и т.д.).

Решение этой задачи возможно при определенных допущениях. Поставим задачу в терминологии линейного программирования.

Найти подмножество контролируемых параметров ω множества Щ, максимизирующее при соблюдении ограничений линейную функцию В или

$$B_{\omega} = \max_{\omega \in \Omega} \left\{ B \,/\, g_s \le G_s ; s = 1,2 \ldots \right\}, \qquad (1)$$

где G_s - ограничение на выбор состава контролируемых параметров;

g_s - достигнутое значение по s-му ограничению.

Применение в качестве максимизируемой функции критерия объективности контроля в виде

$$B_{\omega} = \sum_{i \in \omega} b_i , \quad (4.1.2)$$

где

$$b_i = \frac{I_i}{\sum_{i \in \omega} I_i} \qquad (2)$$

$$I_i = -\frac{\lambda_i}{\Lambda}\log_2\frac{\Lambda}{\lambda_i} - \left(1-\frac{\lambda_i}{\Lambda}\right)\log_2\frac{1}{\left(1-\frac{\lambda_i}{\Lambda}\right)}. \quad (3)$$

Здесь λ_i - интенсивность проникновений в i-ый параметр;

Λ - интенсивность проникновений в канал - $\Lambda = \sum_{i\in\omega} \lambda_I$.

Не меняя, практически, сути рассуждений, можно принять $b_i = \lambda_i / \Lambda$, что значительно упрощает вычисления[14].

Принимаются следующие допущения, пригодные для широкого класса каналов:

– надежность параметров не изменяется при введении КУ;

– параметры взаимонезависимые; для всех параметров выполняется

$\lambda_i << \Lambda$. (4)

В среднем время отыскания неисправного элемента $\tau_{от\ i}$ (без КУ) больше, чем время устранения неисправности или проникновения $\tau_{ус\ i}$ этого элемента; $\tau_{от\ i} + \tau_{ус\ i} = \tau_{в\ i}$ - время восстановления i-го элемента; для всех элементов выполняется условие

$\tau_{от\ ку\ i} << \tau_{ус\ i}$. (5)

Выбор контролируемых параметров по заданному коэффициенту готовности

В качестве обязательного ограничения можно потребовать получение какой-либо характеристики надежности заданного значения, например, коэффициента готовности в виде

$$\sum_{i\in\omega} Z_i\gamma_i + \sum_{j\in\omega} Z_j\gamma_j \le \frac{1-K_{гз}}{K_{гз}}, \quad 6)$$

$\overline{\omega} \cup \omega = \Omega$, $\overline{\omega} \cap \omega = \varnothing$,

где $Z_i \neq Z_j$

$$Z_i, Z_j = \begin{cases} 0 \\ 1 \end{cases} \qquad (7)$$

$$\gamma_i = \lambda_i(\tau_{\text{от ку } i} + \tau_{\text{ус } i})$$
$$\gamma_j = \lambda_j(\tau_{\text{от ку } j} + \tau_{\text{ус } j}). \qquad (8)$$
$$\lambda_i \approx \lambda_j;\ \tau_{\text{ус } i} \approx \tau_{\text{ус } j}$$

В качестве λ_i можно использовать вероятность отказа, в предположении $q_i \equiv \lambda_i$.

Формализуем условие задачи.

Определить набор $Z = (z_1, z_2, \ldots, z_n)$ максимизирующий функцию

$$\sum_{i\in\omega} Z_i b_i + \sum_{j\in\omega} Z_j b_j,\ \omega \cap \bar{\omega} = \varnothing,\ \omega \cup \bar{\omega} = \Omega. \qquad (9)$$

При условиях

$$\sum_{i\in\omega} Z_i \gamma_i + \sum_{j\in\omega} Z_j \gamma_j \le \frac{1 - K_{\text{гз}}}{K_{\text{гз}}},$$

$$\sum_{i\in\omega} Z_i g_{S\,i} + \sum_{j\in\omega} Z_j g_{S\,j} \le G_s,$$

$$Z_i, Z_j = \begin{cases} 0 \\ 1 \end{cases};\ Z_i \ne Z_j. \qquad (10)$$

Показано применение расчетных соотношений на простом примере.

Пример. В коммуникационном устройстве имеется 10 определяющих параметров. Необходимый $K_{гз}$ = 0,978, максимальная стоимость КУ G_2 = 150 усл.единиц, максимальная масса КУ G_2 = 80 усл.единиц. Данные о параметрах сведены в таблица 1.

Все параметры канала контролировать нельзя, так как нарушаются условия (4). Определяются величины I_i и $\sum_{i\in\omega} I_i$

$$\sum_{i=1}^{10} I_i = 0,45 + 0,23 + 0,71 + 0,4 + 0,6 + 0,45 + 0,23 + 0,23 + 0,05 + 0,71 = 4,06,$$

Таблица 1

№	1	2	3	4	5	6	7	8	9	10	
$л_i$ (1/ч)	1	0,5	2	0,8	1,5	1	0,5	0,5	0,2	2	10^{-2}
$ф_{bi}$ (ч)	2	4	6	2	1	0,2	4	2	2	2	10^{-1}
$ф_{усi}$	1,6	1	4,8	1,4	0,8	0,16	1	0,5	0,6	1,6	10^{-1}

(ч)											
g_{1i} (усл.ед)	10	20	10	30	20	10	10	10	20	40	
g_{2i} (усл.ед)	5	10	20	20	20	10	5	10	5	5	

после чего находятся коэффициенты b_i по формуле (3) и ε_i, ε_j по формулам (3). Все показатели сводятся в таблица 2.

Таблица 2

№	1	2	3	4	5	6	7	8	9	10	
b_i	0,11	0,06	0,17	0,1	0,15	0,11	0,06	0,06	0,11	0,17	
ε_i	1,6	0,5	9,6	1,12	1,2	0,16	0,5	0,25	0,12	3,2	10^{-3}
ε_j	2	2	12	1,6	1,5	0,2	2	1	0,4	4	10^{-3}

Требуется найти набор $Z = (z_1, z_2, \ldots, z_{10})_{\omega \in \Omega}$ максимизирующий линейную функцию

$$0{,}11\, z_1 + 0{,}06\, z_2 + 0{,}17\, z_3 + 0{,}1 z_4 + 0{,}15\, z_5 + 0{,}11\, z_6 + 0{,}06\, z_7 + 0{,}06\, z_8 + 0{,}01\, z_9 + 0{,}17\, z_{10}$$

(6) при условиях

$$\begin{aligned} &(1{,}6 z_1 + 0{,}5 z_2 + 9{,}6 z_3 + 1{,}12\, z_4 + 1{,}2 z_5 + 0{,}16\, z_6 + 0{,}5 z_7 + 0{,}25\, z_8 + 0{,}12\, z_9 + 3{,}2 z_{10})_{i \in \omega} + \\ &+ (2 z_1 + 2 z_2 + 12\, z_3 + 1{,}6 z_4 + 1{,}5 z_5 + 0{,}2 z_6 + 2 z_7 + z_8 + 0{,}4 z_9 + 4 z_{10})_{j \in \omega} \le 22{,}5; \\ &10\, z_1 + 20\, z_2 + 10\, z_3 + 30\, z_4 + 20\, z_5 + 10\, z_6 + 10\, z_7 + 10\, z_8 + 20\, z_9 + 40\, z_{10} \le 150; \\ &5 z_1 + 10\, z_2 + 20\, z_3 + 20\, z_4 + 20\, z_5 + 10\, z_6 + 5 z_7 + 10\, z_8 + 5 z_9 + 5 z_{10} \le 80 \end{aligned} \qquad (6)$$

Решая задачу методом направленного полного перебора, получаем оптимальный набор контролируемых параметров (1,3,4,5,6,10), при выполнении условий (6) и максимальном $B_\omega = 0{,}81$. (7)

Предложенная методика при ее наглядности и универсальности обладает следующими недостатками:

– большой объем вычислений при увеличении числа параметров (более 10), особенно при близости их характеристик;

– сложность приведения к задаче линейного программирования (из-за зависимости значения величины г от выбора z в выражении (7);

– трудности разработки вычислительного алгоритма для ЭВМ.

В связи с этими недостатками приведенные соотношения целесообразно применять только для каналов с малым числом параметров (единицы).

Однако преобразуя выражение (5) к виду

$$\sum_{i \in \Omega} Z_i \gamma_{\text{ст i}} \geq \frac{K_{\text{гз}} - K_{\text{г}}}{K_{\text{гз}} K_{\text{г}}}, \qquad (8)$$

или

$$\sum_{i \in \Omega} \sum Z_i \gamma_{\text{ст i}} \geq \Lambda (\tau_{\text{в}} - \tau_{\text{вз}}), \qquad (9)$$

или

$$\sum_{i \in \Omega} Z_i \gamma_{\text{ст i}} \geq \Lambda \tau_{\text{в}} - \frac{(1 - K_{\text{гз}})}{K_{\text{гз}}}, \qquad (10)$$

где Л- интенсивность отказов канала;

$\phi_{\text{в}}$ - среднее время устранения одной неисправности или проникновения;

$\phi_{\text{вз}}$ — заданное время восстановления;

$$\gamma_{\text{ст i}} = \lambda_i \tau_{\text{ст i}} \approx q_i \tau_{\text{ст i}}, \qquad (11)$$

добиваемся отсутствия зависимости г от выбора z. Поэтому сравнительно просто можно придти к задаче линейного программирования с булевыми переменными в следующей математической постановке.

Определить набор $Z = (Z_1, Z_2, \ldots, Z_n)$, максимизирующий функцию

$$\sum_{i \in \Omega} Z_i B_i,$$

при условиях

$$\begin{cases} \sum_{i \in \Omega} Z_i \gamma_{\text{ст i}} \geq \dfrac{(1 - K_{\text{гз}})}{K_{\text{гз}}} \\ \sum_{i \in \Omega} Z_i g_{S_i} \leq G_s \\ Z_i = \begin{cases} 0 \\ 1 \end{cases} \\ B_i > 0;\ \gamma_{\text{ст i}} > 0;\ g_{S_i} > 0. \end{cases}$$

При такой постановке задача может быть решена методами линейного программирования с булевыми переменными, в том числе и на ЭЦВМ.

2. Выбор контролируемых параметров по максимальному значению вероятности безотказной работы после проведения диагностики

Методика выбора контролируемых параметров, может эффективно применяться только при независимости параметров (каждый параметр зависит только от одного элемента или каждый элемент имеет только один параметр). Рассмотрено задачу выбора для случая, когда параметры взаимозависимы. Причем оптимальным считается такой набор, при контроле которого достигается максимальная апостериорная вероятность безотказной работы и соблюдается условие ограничения (стоимость контроля, время и т.д.). Задачу выбора оптимального набора контролируемых параметров при ограничении можно решить методами сокращенного перебора. Сокращение перебора достигается использованием специальных правил, позволяющих исключать заведомо неоптимальные наборы. Рассмотрено более простой алгоритм , пригодный для определения набора контролируемых параметров канала.

Постановка задачи

Система состоит из N элементов. В каждый момент времени возможно только одно проникновение (возможен отказ лишь одного элемента). Работоспособность каждого элемента не зависит от состояния других. Отказ любого элемента вызывает выход из зоны допуска значения, по крайней мере, одного из M параметров.

Известные априорные вероятности q_i при отказе i-го элемента и для каждого к-го параметра $p_к$ определено подмножество $S_к$ элементов, охваченных контролем этого параметра. Другими словами, величиной $S_к$ можно характеризовать ненадежность к-го параметра.

Известны затраты $g_к$ на контроль каждого параметра. При этом предполагается, что затраты g(w) на контроль любой совокупности w параметров слагаются из суммы затрат на контроль каждого параметра из этой совокупности.

Требуется из всех совокупностей (наборов) w, у которых $g(w)<G_s$ - допустимых планов, (где G_s - s-ое ограничение на проведение контроля) выбрать ту совокупность, при которой вероятность безотказной работы устройства после проведения контроля (диагностики) была бы наибольшей.

Решение

Обозначим: $p_к$ - вероятность безотказной работы тех элементов, у которых контролируется к-й параметр ($q_к = 1 – p_к$). Вероятность безотказной работы устройства перед контролем

$$P^{(0)} = \prod_{i=1}^{N} P_i = \prod_{i=1}^{N} (1 - q_i) \approx \sum_{i=1}^{N} q_i , \quad (1)$$

при

$$\sum_{i=1}^{N} q_i < 1 . \quad (2)$$

Взаимосвязь параметров и элементов задается матрицей вида

$$\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1K} & \dots & a_{1M} \\ a_{21} & a_{22} & \dots & a_{2K} & \dots & a_{2M} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{iK} & \dots & a_{iM} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{N1} & a_{N2} & \dots & a_{NK} & \dots & a_{NM} \end{Vmatrix}$$

элементы которой определяются из условия

$$a_{iK} = \begin{cases} 0, & \text{если } i \notin \pi_к \\ 1, & \text{если } i \in \pi_к \end{cases} , (4)$$

где i - номер элемента;

к - номер параметра.

При этом параметры нумеруются так, чтобы соответствующие им затраты составляли неубывающий ряд

$$g_1 \le g_2 \le \dots \le g_M .$$

(Впоследствии предпочтительно начинать выбор параметров слева).

При продолжительном результате контроля к-го параметра, вероятность безотказной работы всех элементов, от которых зависит к-й

параметр, принимается равной единице. В этом случае вероятность безотказной работы всей системы определится выражением

$$P^{(к)} = \frac{P^{(10)}}{P_к},$$

где

$$P_к = \prod_{i \in \pi_к} P_i \approx 1 - \sum_{i \in \pi_к} q_i = 1 - S_к. \quad (3)$$

При этом вероятность безотказной работы системы возрастет на величину

$$\Delta P^{(к)} = P^{(к)} - P^{(0)} = \frac{P^{(0)} S_к}{1 - S_к}.$$

Предполагается, что затраты $q_к$ и ограничение G_s таковы, что сумма любых двух значений затрат больше G_s. Тогда для контроля, очевидно, надлежит выбирать лишь один параметр. Этим параметром будет тот, у которого сумма $S_к$ будет наибольшей. Если таких параметров несколько, то из них надо выбрать тот, у которого произведение $(1 - S_к)q_к$ - наименьшее и, следовательно, приращение вероятности, приходящееся на единицу затрат – наибольшее

$$V^{(к)} = \frac{\Delta P^{(к)}}{g_к} = \frac{P^{(0)} S_к}{g_к (1 - S_к)}.$$

Если систему проконтролировать некоторой совокупностью w приборов (p_w) и затраты при этом $g(w) < G_s$, то вероятность безотказной работы системы примет значение

$$P^{(w)} = \frac{P^{(0)}}{P_w},$$

где

$$P_w = \prod_{i \in uк \in w} P_i \approx 1 - \sum_{i \in uк \in w} q_1 = 1 - S_w. \quad (4)$$

При этом общий множитель p_i (или общее слагаемое q_i) берется лишь один раз. Вероятность безотказной работы системы увеличится при этом на величину

$$\Delta P^{(w)} = P^{(0)} - P^{(w)} = \frac{P^{(0)} S_w}{1 - S_w}.$$

Если при фиксированном числе параметров все наборы w таковы, что $g(w) + g_1 > G_s$ и $1 \notin w$, то из всех наборов оптимальным будет тот, у которого сумма S_w - наибольшая, а, следовательно, и приращение вероятности будет наибольшим[15]. Если окажется несколько наборов с одинаковой наибольшей суммой S_w, то оптимальным из них будет тот, у которого величина

$$V^{(w)} = \frac{\Delta P^{(w)}}{g_w} = \frac{P^{(0)} S_w}{g(w)(1 - S_w)}$$

наибольшая. Таковым будет набор, у которого произведение $g(w)(1 - S_w)$ - наименьшее.

Алгоритм определения рационального набора контролируемых параметров реализуется в следующей последовательности:

1-й шаг. Параметры, у которых $g_к > G_s$ не рассматриваются. Для оставшихся параметров вычисляются $S_к$ и находится наибольшая из них $S_к^{(0)}$. Если таких параметров несколько, то из них выбирается тот, у которого $R_к = g_к(1 - S_к)$ - наименьшее. Обозначим этот параметр p_1^0.

2-й шаг. Исключаются из дальнейшего рассмотрения все параметры, у которых $g_к = G_s$ (кроме p_1^0, если $g_1^0 = G_s$). Из оставшихся параметров формируются наборы по два параметра: $(p_1,p_2)(p_1,p_3) \ldots (p_{м-1},p_м)$. Все пары $(p_к,p_1)$, у которых $g_2 = g_к + g_1 > G_s$ не рассматриваются. Вычисляются

$$S_{к1} = \sum_{i \in \pi_к^u \pi_1} q_1 \left[(1, к) = 1,2, \ldots, M, 1 \neq к\right]$$

и находится наибольшая из них $S_{к1}^{(0)}$. Если таких пар несколько, то из них выбирается та, у которой $R_{к1} = (g_к+g_1)(1 - S_{к1})$ - наименьшее. Обозначим эту пару p_2^0.

m-й ш а г . Процесс продолжается до сочетаний по $m \leq M$ параметров, если еще $g_{w \to M} < G_s$. Из полученных наивыгоднейших наборов p_1^0, p_2^0, …, p_m^0 выбирается тот, у которого наименьшее

$$R_w = \sum_{к \in w} q_к (1 - S_w).$$

Соответствующий набор параметров есть решение поставленной задачи. При этом вероятность безотказной работы системы после проведения диагностики достигает наибольшего значения

$$P_{max} = \frac{P^{(0)}}{1 - \max S_w}.$$

Точное решение задачи по предлагаемому алгоритму при больших M и N (несколько десятков) становится весьма громоздким. Можно использовать приближенные методы, которые позволяют получить вполне приемлемую для инженерной практики точность. К ним относятся:

А. Метод выбора рационального набора по числу максимально допустимых в наборе элементов.

Определяется среднее значение затрат на контроль одного параметра

$$g_c = \frac{\sum_{к=1}^{n} q_к}{M}.$$

Предполагается, что затраты $g_к = g_c = const$ и рациональный набор контролируемых параметров находится среди наборов с максимально допустимым числом параметров. За максимально допустимое число принимается

$$n = \left\lceil \frac{G_s}{g_s} \right\rceil + 1.$$

Затем рассматриваются все наборы по n параметров, у которых $g_{s\,w \to n} \le G_s$ и из них выбирается оптимальный p_n^0 по алгоритму, изложенному ранее.

Применение этого приближенного метода эффективно при близких значениях затрат на контроль параметров.

Б. Метод приближения к рациональному набору по наборам с наибольшим приращением вероятности, приходящейся на единицу затрат (Метод наискорейшего спуска).

Предполагается, что из всех сочетаний по два наилучшим является сочетание из таких параметров $p_{к1}^{0}$ и $p_{к2}^{0}$, что значение $V^{(к1\ 0)}$ — наибольшее из всех $V^{(к)}$ и $V^{(к1\ 0\ к2\ 0)}$ - наибольшее из всех $V^{(кl\ к2)}$. Из всех сочетаний по три параметра наилучшим является сочетание $p_{кl}^{0}\ p_{к2}^{0}\ p_{к3}^{0}$ у которого значение $V^{(к1\ 0\ к2\ 0\ к3\ 0)}$ наибольшее. Таким образом, за оптимальный набор принимается набор $p_{кl}^{0}\ p_{к2}^{0}\ldots p_{кn}^{0}$. При этом присоединение к этому набору любого из оставшихся приборов не удовлетворяет условию ограничения на затраты

$$\sum_{j=1}^{n} g_{К_j^0} \le G_s \quad \text{и} \quad \sum_{j=1}^{n} g_{К_j^0} + g_{К_1} > G_s \quad \left(1 \notin к_j^0\right).$$

В этом методе получается наименьшее число переборов. Его применение наиболее эффективно при резком отличии параметров друг от друга.

В. Комбинированный метод, в котором применены предыдущие приближенные методы и основные идеи метода ветвей и границ. По методу А определяется базовый набор $w_Б^0$, состоящий их n параметров при $g(w_Б^0) < G_s$. В наборах $w_Б^0$ и $w_Б^0\left(w_Б^0 \cap \overline{w}_Б^0 = \varnothing \ \text{и}\ w_Б^0 \cup \overline{w}_Б^0 \subseteq \overline{М}\right)$ отыскиваются такие параметры, чтобы

$$V^{\left(к \in w_Б^0\right)} > \overline{V}^{\left(1 \in w_Б^0\right)}. \qquad (5)$$

Комбинированный метод, очевидно, самый эффективный из рассмотренных и позволяет наиболее быстро подойти к решению задачи при

$$\begin{aligned} &g\left(w_Б^1\right) \le G_s; \\ &к \in w_Б^1; \\ &1 \in \overline{w}_Б^1. \end{aligned} \qquad (6)$$

Такие операции проводятся до тех пор пока находятся параметры, удовлетворяющие условиям (4.3.6 и 7). При этом оптимальным набором w_0 из $\{w_Б^0, w_Б^1, w_Б^2, ..., w_Б^m\}$ считается тот, у которого

$$P(w_0) = \max\left\{P\left(w_Б^0\right), P\left(w_Б^1\right), P\left(w_Б^2\right), \ldots, P\left(w_Б^m\right)\right\}.$$

Следует отметить, что число шагов решения при использовании алгоритма Р.Р. Убара, реализованного с помощью метода ветвей и границ

[28]. (при учете допустимости и перспективности) несколько больше, чем при методе В, и логика алгоритма и элементарные вычисления сложнее приведенных выше.

Приведено характеристики числа переборов вариантов без учета допустимости и перспективности планов (таблица 3).

Следует отметить, что с ростом М и n различие в числе переборов для этих методов быстро возрастает. При учете допустимости и перспективности наборов число переборов в трех последних методах резко падает (метод А грубее остальных и может применяться только при сильных ограничениях).

Таблица 3

Метод (алгоритм)	Максимальное число переборов	n=5 M=7
Полный перебор	$\leq \sum_{i=1}^{M} C_{M}^{i}$	127
А	$< C_{M}^{n}$	21
Б	$\leq \left(nM - \sum_{i=1}^{n-1} i \right)$	25
Алгоритм Р.Р.Убара	$< \left(C_{M}^{]M/2[} + C_{M}^{]M/2[+1} \right)$	70

По простоте алгоритма и по элементарности вычислений, а также по быстроте решения наиболее предпочтительным является метод Б. Используя понятие веса (важности) параметра можно заменить в матрице (3) величину $a_{iк}$ на $h_{iк}$.

При этом

$$\sum_{i=1}^{M} h_{iк} = 1,$$

а $h_{iк}$ показывает (относительно) как сильно влияет i-ый элемент (точнее параметры элемента) на к-ый параметр. Такая замена особенно эффективна при преобладающем количестве параметрических отказов[16]. Заметено, что не меняя сущности метода, можно заменить величину q_i на $л_i ф_{bi}$ или на $ф_{bi}/ф_{cpi}$, (где $л_i$ –интенсивность отказов i-го элемента; $ф_{cpi}$ - среднее время восстановления i-го элемента). При этом в выражении (1) $P^{(0)}$ будет иметь смысл коэффициента готовности. Проиллюстрируем методы на примерах.

Примеры: Объект контроля задан матрицей вида (3)

$$\left\| a_{ik} \right\| = \begin{Vmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{Vmatrix}$$

элементы которой определяются из условия (4).

Исходные данные приведены в таблица 4 ограничение G_y=7.

Таблица 4.

№	q_i x 10^3	p_1	p_2	p_3	p_4	p_5
		затраты на контроль				
		2	2	2	3	3
1	3		3			
2	5			5	5	5
3	4	4				4
4	4			5		
5	4				4	
$S_к$ x $l0^3$	20	4	3	9	9	9
1 - $S_к$	0,980	0,996	0,997	0,991	0,991	0,991
$R_к = g_к(l - S_к)$		-	-	1,882	-	-

Пример 1. Из таблица 4 видно, что предпочтительным для контроля является параметр p_3, то есть

$$\pi_{1^\circ} = \pi_3; \quad P^{(3)} = \frac{0,980}{0,991} = 0,998 \ .$$

Сочетания по два параметра для определения p_{2° представлены в таблица 5. Из нее следует, что предпочтительным для контроля является сочетание параметров $p_3p_4 = p_{2^\circ}$;

$$P^{(34)} = \frac{0,980}{1 - 0,013} = 0,993 \ .$$

Таблица 5

№	q_i x 10^3	12	13	14	15	23	24	25	34	35	45
		затраты на контроль $g_{(2)}$									
		4	4	5	5	4	5	5	5	5	6
1	3					3	3	3			
2	5		5	5	5	5	5	5	5	5	5
3	4	4	4	4	4			4		4	4

4	4					4			4		
5	4								4		4
$S_{k1} \times 10^3$		7	9	9	9	12	8	12	13	9	13
$(1 - S_{k1}) \times 10^3$		993	991	991	991	988	992	988	987	991	987
$(1 - S_{k1}) \times g(2)$		3,952									

Сочетания по три параметра для определения p_{3^o} представлены в табл.6.

Таблица 6

№	$q_i \times 10^3$	123	124	125	134	135	145	234	235	245	345
		затраты на контроль $g_{(3)}$									
		6	7	7	7	7	8	7	7	8	8
1	3	3	3	3		5		3	3		
2	5	5	5	5	5	4		5	5		
3	4	4	4	4	4				4		
4	4	4			4			4	4		
5	4		4		4			4			
$S_3 \times 10^3$		16	16	12	17	9	-	16	16	-	-
$(1 - S_3) \times 10^3$		984	984	988	983	991		984	984		

Примечание: наборы 145, 245 и 345 не рассматриваются, так как для них g(3) = 8>7. Из табл.4 получаем рациональный набор $p3^o$=p1p3p4.

При этом

$$P^{(134)} = \frac{0,980}{1 - 0,017} = 0,997$$

Любое сочетание по 4 прибора дает g(w)>7.

Сравнивая P(3), P(34) и P(134), получаем оптимальный набор ($p_1p_3p_4$).

Пример 2. Для тех же числовых данных решим задачу 1-ым приближенным методом. В нашем случае

$$M = 5; g_c = \frac{12}{5} = 2,4$$

$$n = \left\lceil \frac{7}{2,4} \right\rceil + 1 = 3$$

Составляется таблица 4 и из нее находится $p_{3^o}=p_1p_3p_4$.

Пример 3. Решаем 2-м приближенным методом. Из таблица 2 имеем $p_{k1^o}=p_3$. После этого объем табл.3. сократится, то есть в ней рассматриваются лишь сочетания с параметром p_3 [(31), (32), (34) и (35)].

Минимум произведения (l - $S_{к1}$)g(2) дает максимум $V^{(к1)}$. Таким образом, как это следует из табл.3, сочетание $p_{к1^{o}}$ $p_{к2^{o}}$= p_3p_2.

По этим же причинам уменьшается и объем таблица 4, так как в ней рассматриваются лишь сочетания с параметрами p_3 и p_2 [(231), (234) и (235)].

Наименьшее произведение (1 - S_3) g(3) соответствует сочетанию $p_2p_3p_1$ Для этого сочетания величина $V^{(к1\,0\,к2\,0\,к3\,0)}$ – наибольшая.

Приближенно определенный набор незначительно отличается от ранее найденного и при затратах $g_1 + g_2 + g_3 = 6 < 7$, вероятность безотказной работы $P^{(123)} = 0{,}996$.

3. Оценка оптимального времени между проведением функциональных проверок информационного канала

Если вероятность выявления отказов канала или проникновений в него с помощью непрерывного контроля $P_{нк}$, а с помощью контроля $P_{фк} = 1 - P_{нк}$, то значение стационарного коэффициента готовности можно выразить соотношением

$$K_{г} = \frac{T_0}{T_0 + \tau_{в} + P_{фк} + T_{фк}/2} \quad \frac{T_{фк}}{T_{фк} + \tau_{фк}}, \quad (1)$$

где T_0 - среднее время работы канала между отказами;

$ф_{в}$ - среднее время существования отказа ($ф_{в} = ф_{от} + ф_{ус}$);

$T_{фк}$ - среднее время между проведением функционального контроля;

$ф_{фк}$ - среднее время проведения функционального контроля.

Оптимальное значение времени между проведением функционального контроля, при котором обеспечивается максимальный коэффициент готовности, определяется формулой

$$T_{фк} = \sqrt{\frac{2\tau_{фк}(\tau_0 + \tau_{в})}{P_{фк}}}. \qquad (2)$$

Оптимизация блоков контролируемой аппаратуры. Очевидно, что чем на большее число блоков разделен канал, тем лучше ее ремонтопригодность и, следовательно, коэффициент готовности. В то же время возрастает

сложность аппаратуры контроля и увеличивается влияние ее погрешности (и проникновения в канал).

Отсюда вытекает требование целесообразного разбиения канала на блоки с контролируемыми параметрами. Получена формула для определения оптимального количества блоков с контролируемой работоспособностью, при условии

$$\tau << t << T_0 << T_{кi}, \qquad (3)$$

где ф - средняя длительность нерабочих периодов;

t – текущий момент времени работы РЭА;

$T_{кi}$ - среднее время безотказной работы одного блока аппаратуры диагностики.

Легко видеть, что условие (3) выполняется для широкого класса РЭА и аппаратуры контроля[17]. Оптимальное количество блоков для достижения максимального коэффициента готовности находится по формуле

$$M = \frac{-B + \sqrt{B^2 - 4AC}}{2A}, \quad (4)$$

где

$$A = (\tau_{ус} + P_и \tau)(\tau + \tau_{ус});$$

$$B = 2\tau_{от}(P_и \tau + \tau_{ус})$$

$$C = \tau_{от}\left[\tau_{от} - \frac{\tau T_{ки}(1 - P_и)}{P_{ло} T_o}\right].$$

Здесь $P_и$ - вероятность того, что канал используется в любой произвольный момент времени t (не зависит от t);

$ф_{от}$ - среднее время отыскания неисправности или проникновения в аппаратуре, не разделенной на блоки;

$P_{ло}$ - вероятность того, что отказ блочного узла аппаратуры диагностики выражается в выдаче неправильной информации об исправном блоке

($P_{ло} = 1 - P_{прав}$, где $P_{прав}$ - вероятность того, что блочный узел выдает правильную информацию о неисправном блоке при условии, что отказ или проникновение произошли).

4. Рекомендации по устранению несанкционированного использования подслушивающими устройствами

Инженерно-технические мероприятия — совокупность специальных технических средств и их использование для защиты информации. Выбор инженерно-технических мероприятий зависит от уровня защищенности информации, который необходимо обеспечить.

Инженерно-технические мероприятия, проводимые для защиты информационной инфраструктуры организации, могут включать использование защищенных подключений, межсетевых экранов, разграничение потоков информации между сегментами сети, использование средств шифрования и защиты от несанкционированного доступа.

В случае необходимости, в рамках проведения инженерно-технических мероприятий, может осуществляться установка в помещениях систем охранно-пожарной сигнализации, систем контроля и управления доступом.

Отдельные помещения могут быть оборудованы средствами защиты от утечки акустической (речевой) информации.

Рекомендуемые современные устройства поиска и защиты приведены в Приложении Б.

Рассмотрим некоторые технические средства, используемые в защищаемых АС.

Рекомендации по устранению несанкционированного использования диктофона

Проблема устранения нежелательных записей на диктофон на расстояниях ближе 1,5-2м решается многими методами.

Однако, в некоторых случаях это расстояние может потребоваться увеличить до 3-10м, что не позволяют сделать скрытно известные методы.

Предложим использовать для этого интерференционный метод. Поскольку звуковой диапазон (до 20кГц) не может быть применен для постановки помехи из-за восприятия его человеческим слухом, используем два излучателя в ультразвуковом диапазоне (30-50кГц). Их частоты *F1* и *F2* выбираем таким образом, чтобы *ДF= /F1-F2/*<(1-3) кГц.

Располагается аппаратура как показано на рис.1.

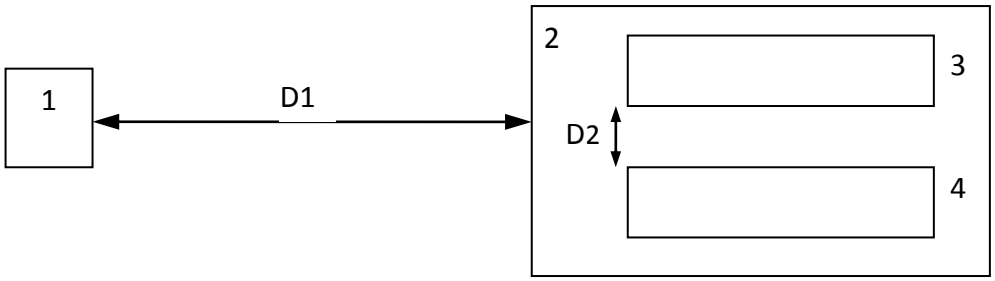


Рис.1 Схема расположения аппаратуры блокирования утечки информации с использованием диктофона

Здесь: 1-диктофон (предполагаемый);

2-аппаратура устранения записи (скрытно);

3-генератор гармонического сигнала частоты *F1* с ультразвуковым излучателем;

4- то же на частоте *F2;*

D1 – расстояние предполагаемого диктофона от аппаратуры устранения записи (постановщика гармонической интерференционной помехи), может быть более 1,5-2м;

D2 – расстояние между излучателями (выбирается в пределах от нескольких сантиметров до десятков).

Принцип работы следующий: излучения гармонических ультразвуковых колебаний каждого в отдельности не прослушиваются человеческим слухом (однако тренированная собака их может уловить). Человеческое ухо достаточно линейно в амплитудном отношении и поэтому интерференционных явлений не будет.

Микрофон диктофона сугубо нелинейный элемент и поэтому на входе диктофона возникнет интерференционный процесс, который приведет к

подавлению записи речи сигналом разностной частоты. Уровень ультразвуковых колебаний используется в пределах 80-100дБ и лучше, если он будет подобран опытным путем в аналогичном помещении и с диктофоном похожим на предполагаемый.

Этот метод может использоваться также и в автомобилях и в самолетах.

Рекомендации по защите информации постановкой помех

Рассмотрено несколько устройств и методов, которые могут быть использованы для улучшения постановки помех с целью защиты от несанкционированного доступа к информации.

Первое устройство может быть применено при решении различных задач постановки помех и повышения периода случайности в постановщиках помех.

Функциональная схема содержит генератор 1 равномерно распределенных случайных чисел, выход которого соединен со входом цифроаналогового преобразователя 2, блок 3 усреднения, выход которого соединен со входом сумматора 4, выход которого соединен со входом блока 5 сравнения, второй вход которого соединен с выходом цифроаналогового преобразователя 2, а выход - через прерыватель 6 и формирователь 7 импульсов соединен со входами генератора 1 равномерно распределенных случайных чисел и генератора 8 экспоненциального напряжения, выход которого соединен со входами блока 3 усреднения и сумматора 4.

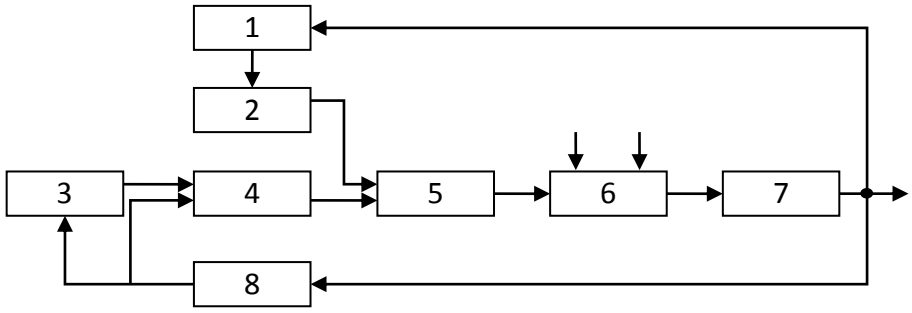


Рис.2 Структурная схема устройства постановки помех

Генератор пуассоновского потока импульсов работает следующим образом.

Генератор 1 случайных чисел вырабатывает случайное число, равномерно распределенное в некотором фиксированном интервале. На выходе цифроаналогового преобразователя 2 образуется аналоговый сигнал, амплитуда которого пропорциональна сформированному случайному числу.

Синхронно с генератором 1 случайных чисел включается и генератор 8, амплитуда выходного сигнала которого возрастает по экспоненциальному закону. Сигнал с выхода генератора 8 поступает на один из входов сумматора 4 и вход блока 3 усреднения, на выходе которого образуется сигнал пропорциональный разности теоретического и текущего средних значений непрерывного случайного напряжения с равномерным распределением амплитуд с выхода генератора 8. Этот сигнал поступает на другой вход сумматора 4. Напряжение на выходе сумматора 4 с помощью блока 5 сравнивается с аналоговым напряжением цифроаналогового преобразователя 2, и в момент равенства этих напряжений блок 5 выдает сигнал, который, проходя через прерыватель 6, поступает на вход формирователя 7 импульсов.

Сигнал с выхода формирователя 7 вновь запускает генератор 8 экспоненциального напряжения и считывает с генератора 1 вновь сформированное равномерно распределенное число.

Сигнал с выхода блока 3 усреднения выполняет функцию сигнала обратной связи, который автоматически поддерживает интенсивность пуассоновского потока на заданном уровне. Если текущее среднее случайное напряжение с выхода генератора 8 совпадает с теоретическим, то сигнал на выходе блока 3 отсутствует. При дрейфе параметров устройства на выходе блока 3 появляется разностный сигнал полярности, соответствующий отклонению интенсивности потока на выходе устройства от заданной. Этот сигнал, суммируясь с экспоненциально изменяющимся напряжением, компенсирует дрейф.

Использование новых блоков — сумматора и блока усреднения позволяет повысить точность результатов исследований систем массового обслуживания, в которых применяется датчик потока электрических

импульсов, распределенных по закону Пуассона; снизить требования к стабильности и температурной устойчивости источников питания и узлов датчика, что упростит конструктивные и схемные решения; устранить дополнительную погрешность, вызываемую усечением экспоненциального закона распределения, так как в предлагаемом устройстве устраняется необходимость выделения запаса по напряжению на случай дрейфа параметров.

Следующее устройство может быть использовано для создания специализированных моделирующих устройств, применяемых, в частности, для моделирования потоков сбоев при передаче дискретной информации по каналу связи в том числе и при несанкционированном доступе к информации.

Поставленная цель достигается тем, что в генератор случайного импульсного потока, содержащий последовательно соединенные генератор псевдослучайной последовательности импульсов, нелинейный цифроаналоговый преобразователь, компаратор, формирователь импульсов, выход которого соединен со входом генератора псевдослучайной последовательности импульсов, дополнительно введены блок задания закона распределения и последовательно соединенные управляемый генератор импульсов, счетчик импульсов, цифроаналоговый преобразователь, интегратор и сумматор, второй вход которого подключен к выходу дополнительного цифроаналогового преобразователя, выход сумматора соединен со вторым входом компаратора, причем выход формирователя импульсов соединен со вторым входом счетчика импульсов, в выход блока задания закона распределения подключен ко второму входу нелинейного цифроаналогового преобразователя.

Генератор случайного импульсного потока содержит генератор 1 псевдослучайной последовательности импульсов, блок 2 задания закона распределения, нелинейный цифроаналоговый преобразователь 3, интегратор 4, сумматор 5, компаратор 6, формирователь 7 импульсов, цифроаналоговый

преобразователь 8, управляемый генератор 9 импульсов, счетчик 10 импульсов, шину и выхода случайного импульсного потока, шину 12 входа управления интенсивностью случайного потока.

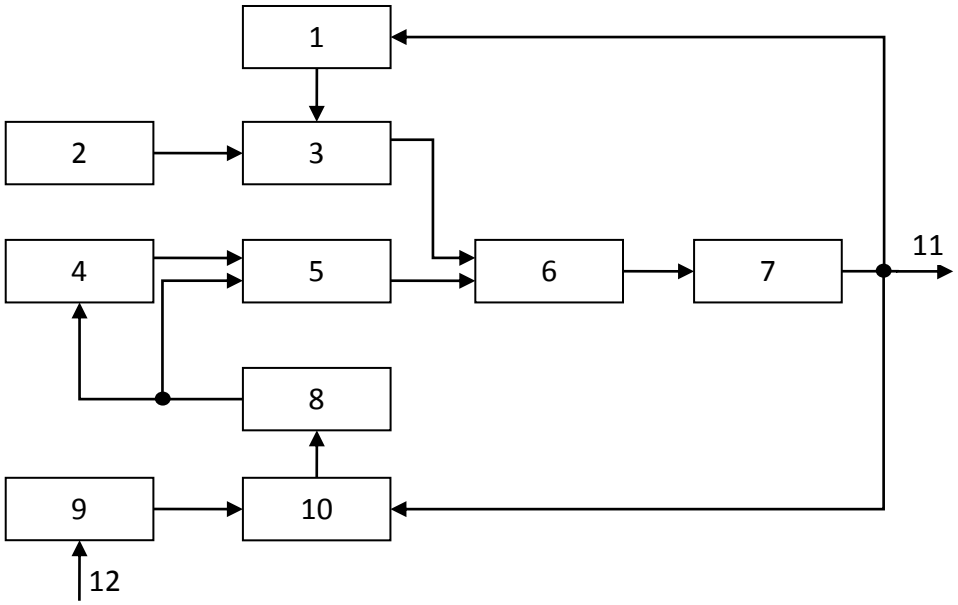


Рис.3 Структурная схема устройства 2

Генератор работает следующим образом.

На выходе генератора 1 псевдослучайной последовательности импульсов формируется n-разрядное двоичное равномерно распределенное случайное число, поступающее на входы нелинейного цифроаналогового преобразователя 3, на выходе которого устанавливается уровень напряжения пропорциональный функции, обратной функции распределения, задаваемой блоком 2 задания закона распределения. Напряжение с выхода нелинейного цифроаналогового преобразователя 3 поступает на один из входов компаратора 6, на другой вход которого поступает напряжение с выхода сумматора 5, на входы которого подается линейно изменяющееся напряжение с выхода цифроаналогового преобразователя 8 и напряжение с выхода интегратора 4, представляющее разность между напряжениями, соответствующими теоретическому и текущему среднему, линейно изменяющемуся напряжению с выхода цифроаналогового преобразователя 8, подключенного ко входу интегратора 4. На разрядные входы цифроаналогового преобразователя 8 поступают числа с выхода счетчика 10,

содержимое которого увеличивается по мере поступления на счетный вход импульсов с выхода управляемого генератора 9 импульсов, период поступления которых регулируется по требуемому закону путем подачи соответствующего управляющего воздействия на шину 12 входа управления интенсивностью случайного потока. При сравнении напряжений компаратор 6 изменяет свое состояние, что вызывает появление импульса на выходе формирователя 7 импульсов, который, поступая на шину сдвига генератора 1, вызывает формирования на выходе нового случайного числа, и, поступая на вход установки нуля счетчика 10, устанавливает его в нулевое состояние. Затем процесс формирования импульса случайного потока повторяется.

Интегратор 4 и сумматор 5 служат для стабилизации интенсивности случайного потока в процессе работы генератора случайного импульсного потока в процессе работы генератора случайного импульсного потока. Так, например, в результате температурного дрейфа параметров изменилась интенсивность потока на выходе устройства. Интегратор 4 формирует напряжение смещения, равное разности напряжений, соответствующих теоретическому и текущему среднему линейно изменяющемуся напряжению.

Напряжение смещения, поступая на один из входов сумматора 5, складывается с линейно изменяющимся напряжением с выхода цифроаналогового преобразователя 8, поступающим на другой вход с сумматора 5. Результирующее напряжение с выхода сумматора 5 поступает на один из входов компаратора 6, где происходит компенсация температурного дрейфа.

С помощью нелинейного цифроаналогового преобразователя 3, представляющего из себя полиномиальный цифроаналоговый преобразователь с регулируемыми коэффициентами полинома, возможна аппроксимация с требуемой точностью широкого класса функция распределения, что позволяет формировать на выходе генератора различные случайные потоки.

Предлагаемый генератор позволяет также генерировать нестационарные случайные потоки с произвольным законом изменения интенсивности. Это существенно расширяет область использования генератора случайного импульсного потока и устраняет необходимость разработки ряда специализированных генераторов.

Выводы по третьей главе

Предложен подход к определению номенклатуры контролируемых параметров с целью получения максимальной информации о техническом состоянии (защиты) канала АС при заданном коэффициенте готовности и выполнении ряда ограничений (например, стоимость контроля, масса, габариты и т.д.). Разработан выбор контролируемых параметров по максимальному значению вероятности безотказной работы после проведения диагностики. С целью дальнейшей оптимизации защиты выполнена оценка оптимального времени между проведением функциональных проверок информационного канала в деятельности организациях. Для достижения максимальной эффективности системы защиты необходимо использовать ряд организационных и инженерно-технических мероприятий в комплексе. Разработаны рекомендации по устранения несанкционированного использования диктофона, а также несколько эффективных устройств и методов для постановки помех с целью устранения несанкционированного доступа к информации.

Заключение

В заключении представлены основные результаты диссертационного исследования:

1. Рассмотрен перечень основных нормативно-правовых документов регламентирующих проектирование АИС в защищенном исполнении.

2. Проанализированы особенности каждого класса АС. Наиболее требовательными к защите являются 1-й и 2-й классы. Рассмотрение 3-го класса АС было опущено. Однако проектирование системы защиты в такой АС не значительно отличается от рассмотренных подходов.

3. Формирован порядок создания КСЗИ. Установлено, что такая разработка обычно состоит из четырех этапов. Наиболее ответственным является третий этап, так как именно на данном этапе реализуются все защищенные организации по требованиям и техническому решению, принятым на предыдущих этапах.

4. Были установлены основные требования к защите как конфиденциальной, так и секретной информации от несанкционированного доступа. Требования были сформированы в результате условно разделенных подсистем АС, в состав которых входит:

– подсистема управления доступом;

– подсистема регистрации и учета;

– подсистема обеспечения целостности.

5. Были анализированы основные принципы защиты информации в организациях от несанкционированного доступа, на основании которых установлено, что реализация таких принципов осуществляется с помощью так называемого "монитора обращений".

6. Исследованы основные подходы к оценке эффективности безопасности деятельности организаций в информационно-коммуникационных системах. К числу таковых относятся:

– классический;

– официальный;

– экспериментальный.

7. Для повышения эффективности защищенности информации в организациях был построен алгоритм на основе математического анализа. На основании такого алгоритма установлено, что реализация защищенности информации для каждого организация различна.

8. Разработана модель оценки эффективности систем защиты информации в организациях, позволяющая оценить степень защищенности информационные системы и осуществить возможных путей улучшения безопасности.

9. Предложены возможные пути оптимизации защитных мероприятий в АС путем выбора контролируемых параметров по различных показателям эффективности.

10. Предложен простой способ скрытного устранения несанкционированного использования диктофона.

11. Рассмотрено несколько эффективных устройств и методов для постановки помех с целью устранения несанкционированного доступа к информации.

12. Для повышения уровни эффективности систем защиты информации в организациях предложена программа, позволяющая шифровать и дешифровать информации между клиент-сервера на основе алгоритм Диффи-Хелмана.

Список использованные литературы

1. Доклад Президента Республики Узбекистан Ислама Каримова на заседании кабинета министров, посвященном итогам социально-экономического развития страны в 2012 году и важнейшим приоритетным направлениям экономической программы на 2013 год.

2. Постановление Президента республики Узбекистан «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий» (Собрание законодательства Республики Узбекистан, 2012 г., № 13, ст. 139).

3. Кельтон В., Лоу А. Имитационное моделирование. Классика CS. / Пер. с англ. / В. Кельтон, А. Лоу - 3-е изд. - СПб.: Питер; Киев: Издательская группа BHV, 2012. 847 с.

4. Бугайский К. Проблемы построения систем информационной безопасности //"Information Security/ Информационная безопасность" – 2008. – №2

5. Арьков П.А. Подход к проектированию системы защиты информации автоматизированной системы // XI Региональная конференция молодых исследователей Волгоградской области: тезисы докладов / ВГТУ Волгоград 2006, с. 198.

6. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия-Телеком, 2001. – 148 с.: ил.

7. Масюк М.И. НСД: теория и практика // "Специальная Техника". – 2003. – №3

8. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ООО «ТИД «ДС». 2001. – 688 с.

9. Ю.Г. Бугров Системные основы оценивания и защиты информации: Учеб. пособие / Воронеж: Воронеж. гос. техн. ун-т, 2005. 354 с.

10. Духан Е.И., Синадский Н.И., Хорьков Д. А. Применение программно-аппаратных средств защиты компьютерной информации. Учебное пособие / Е.И. Духан, Н.И. Синадский, Д.А. Хорьков; науч. ред. д-р техн. наук, проф. Н.А. Гайдамакин. Екатеринбург: УГТУ-УПИ, 2008. – 182 с.

11. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. – М.: ФОРУМ: ИНФРА-М, 2010. - 368 с.: ил.

12. Сидорин Ю.С. Технические средства защиты информации**:** Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005. 141 с.

13. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005. – 960 с.: ил.

14. Хорев А.А. Способы и средства зашиты информации. - М.: МО РФ, 2000. - 316 с.

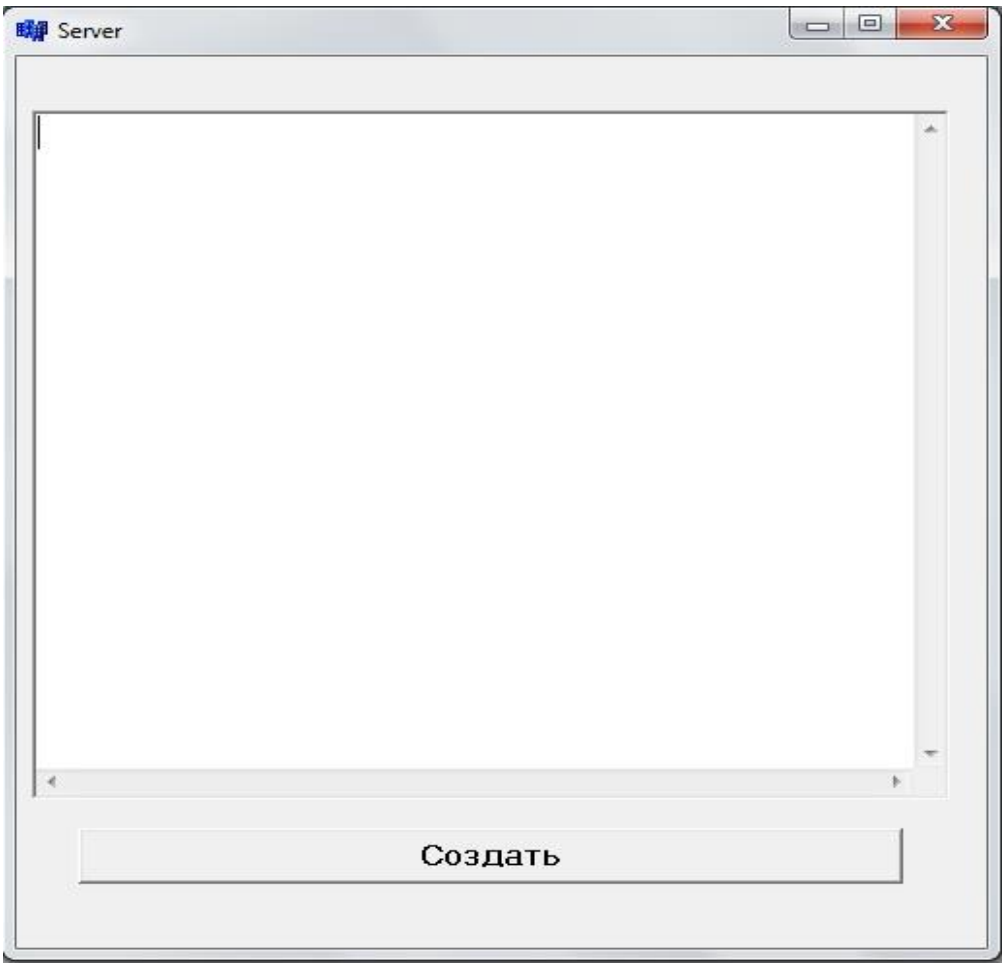
15. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. - К. : Арий, 2008. - Том I. Несанкционированное получение информации. - 464 с, ил.

16. Измалкова С.А., Тарасов А.В. Принципы построения эффективной системы информационной безопасности // Управление общественными и экономическими системами. – 2006. – № 2

17. http://all-safety.ru/ Подходы к оценке эффективности КСЗИ

ПРИЛОЖЕНИЕ

Серверное приложение

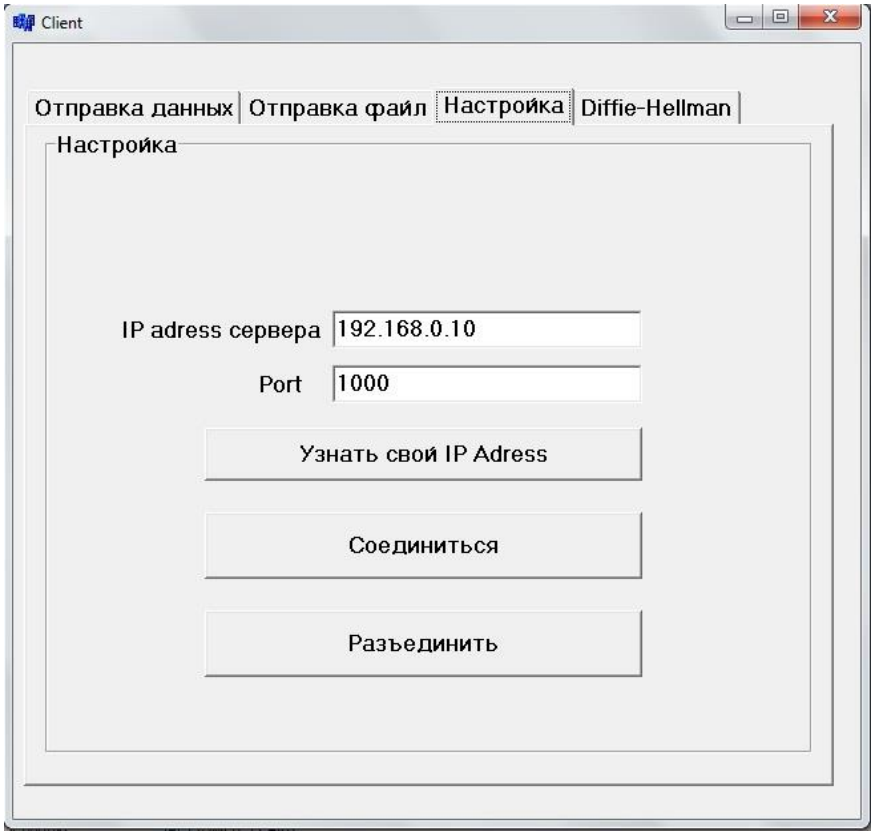


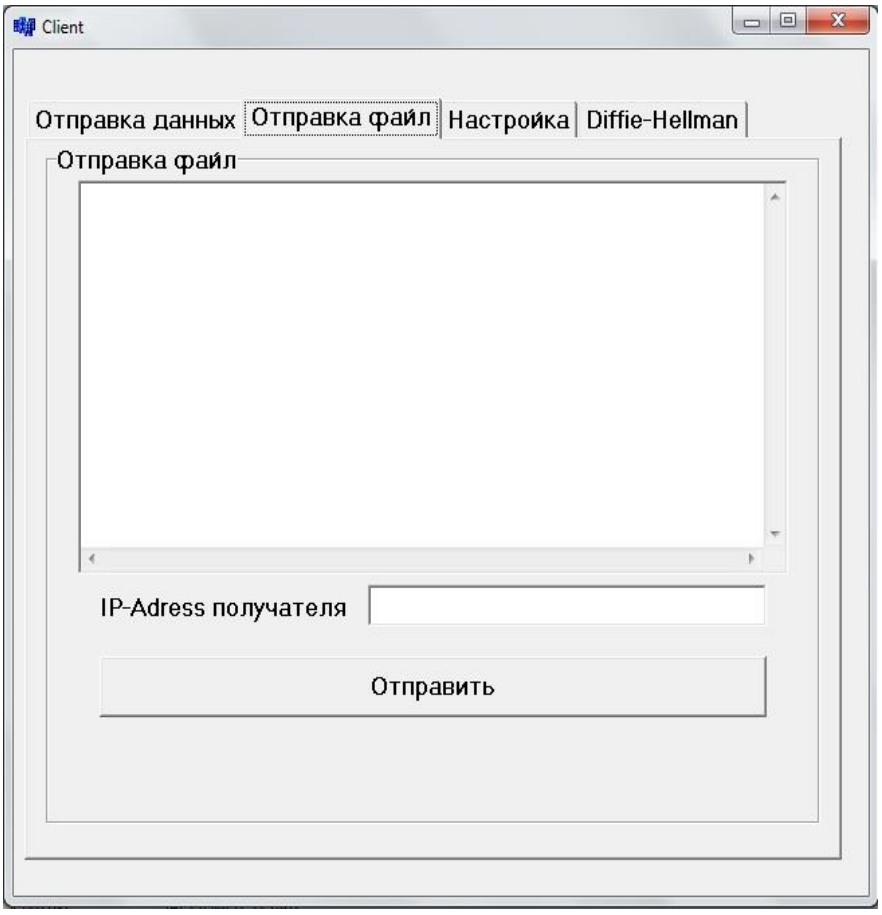
Исходный код серверного приложения

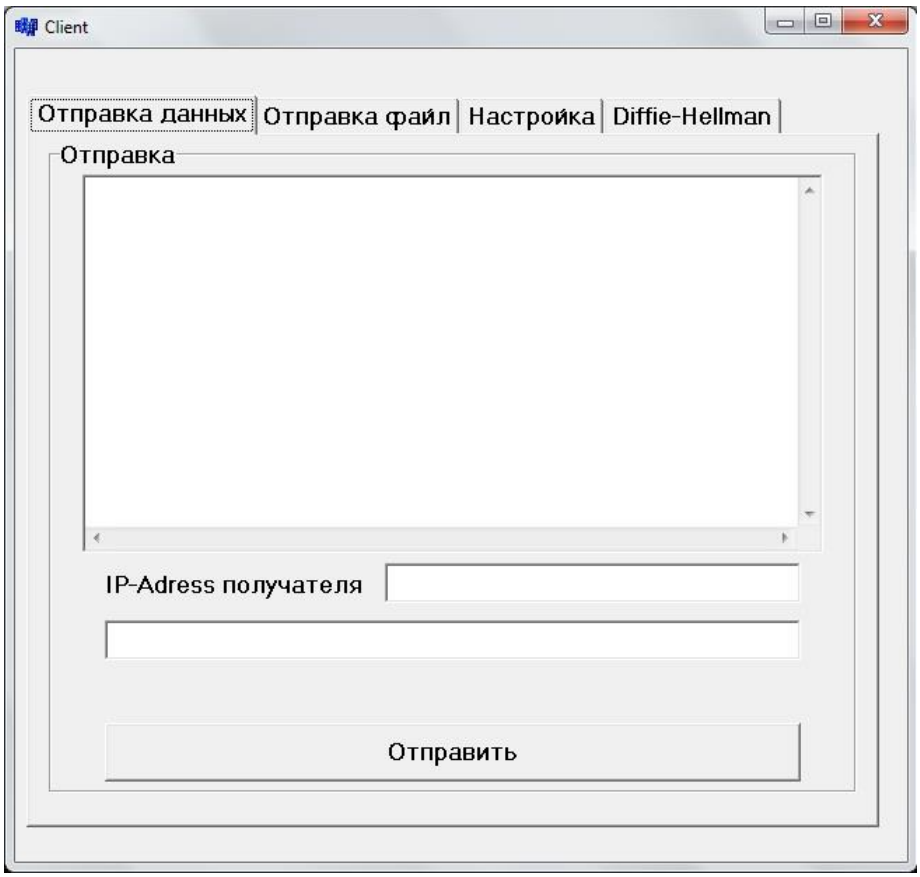
```
#include <vcl.h>
#pragma hdrstop
#include <winsock2.h>
#include <stdio.h>
#include <string.h>
#include <iostream.h>
#include "Unit1.h"
#pragma package(smart_init)
#pragma resource "*.dfm"
TForm1 *Form1;
String IPFile="";
__fastcall TForm1::TForm1(TComponent* Owner)
        : TForm(Owner)
```

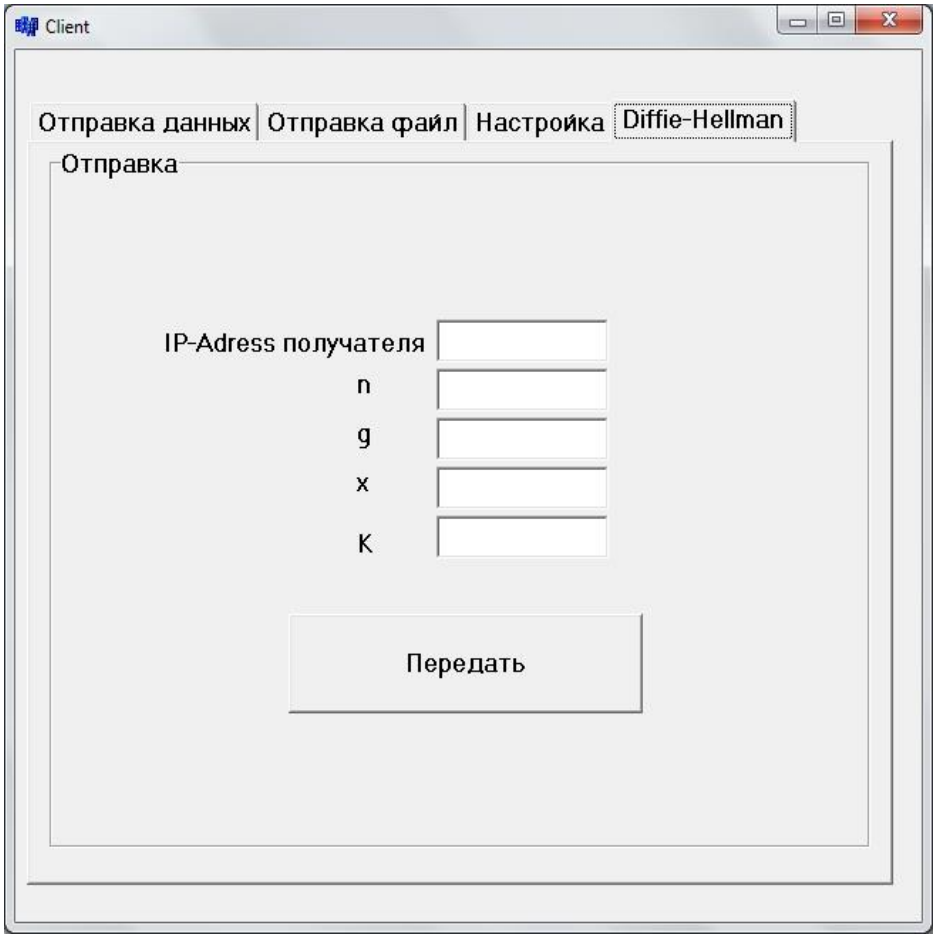
```
{
}
String getIP();
String getTYPE(String);
String getIP(){
AnsiString out = "WinSock ERR";
WSADATA wsaData;
if (!WSAStartup(WINSOCK_VERSION, &wsaData)){char chInfo[64];
if (!gethostname(chInfo, sizeof(chInfo)))
{
hostent *sh;
sh=gethostbyname((char*)&chInfo);
if (sh!=NULL)
{
int nAdapter = 0;
while (sh->h_addr_list[nAdapter])
{
struct sockaddr_in adr;
memcpy(&adr.sin_addr, sh->h_addr_list[nAdapter], sh->h_length);
out = inet_ntoa(adr.sin_addr);
nAdapter++;
}
}
}
}
WSACleanup();
ShowMessage(out);
return out;
}
```

Клиентское приложение






Client
Отправка данных
Отправка файл
Настройка
Diffie-Hellman
Отправка
IP-Adress получателя
Отправить


Client
Отправка данных
Отправка файл
Настройка
Diffie-Hellman
Отправка
IP-Adress получателя
n
g
x
K
Передать

Исходный код клиентского приложения

```
#include <vcl.h>
#pragma hdrstop
#include <winsock2.h>
#include <stdio.h>
#include <iostream.h>
#include <math.h>
#include "Unit1.h"
#pragma package(smart_init)
#pragma resource "*.dfm"
TForm1 *Form1;
TMemoryStream *MS = new TMemoryStream;
void Write(AnsiString Text);  // o-y caiene eiou a iioie
int Size; // ?acia? ii?aaaiiiai oaeea
bool Receive; // ia?aaaai ee iu ia aaiiue iiiaio oaee
AnsiString FileName;  // eiy oaeea
int X=0,Y=0,K=0;
void Write(AnsiString Text)
{
     if(MS->Size < Size)  // anee iu aua i?eieiaai oaee e ?acia? iioiea iaiuoa ?acia?a
oaeea
   {
    MS->Write(Text.c_str(),Text.Length()); // caienuaaai a iioie
    Form1->Memo1->Lines->Add("I?eieiaai aaiiua..."); //
    Form1->Memo2->Lines->Add("Polu4eno: " + IntToStr(Size)+" ec "+
IntToStr(MS->Size));
   }
  if(MS->Size == Size) // anee oaee i?eiyo e ?acia? iioiea niioaaonoaoao ?acia?o
oaeea
  {   Receive = false ; // inoaiaaeeaaai ?a?ei ia?aaa?e
     MS->Position = 0 ;   // ia?aaiaei ea?aoeo iioiea a ia?aei
     Form1->ClientSocket1->Socket->SendText("0:=>end"); // ionueaai na?aa?o
?oi iu i?eiyee oaee
     CreateDir("Downloads"); // nicaaai iaieo aey nio?aiaiiuo oaeeia
     MS->SaveToFile("Downloads\\"+FileName); // nio?aiyai ooaa iao oaee
     MS->Clear() ; // inaiai?aaai iioie
     Size = 0 ;
     Form1->Memo2->Lines->Add("Oaee i?eiyo !");
  }
}
__fastcall TForm1::TForm1(TComponent* Owner)
      : TForm(Owner)
{
```

```
}
String getIP();
String getTYPEC(String);
String getIP(){
AnsiString out = "WinSock ERR";
WSADATA wsaData;
if (!WSAStartup(WINSOCK_VERSION, &wsaData)){char chInfo[64];
if (!gethostname(chInfo, sizeof(chInfo)))
{
hostent *sh;
sh=gethostbyname((char*)&chInfo);
if (sh!=NULL)
{
int nAdapter = 0;
while (sh->h_addr_list[nAdapter])
{
struct sockaddr_in adr;
memcpy(&adr.sin_addr, sh->h_addr_list[nAdapter], sh->h_length);
out = inet_ntoa(adr.sin_addr);
nAdapter++;
}
}
WSACleanup();
return out;
}
String getTYPEC(String BufMess){
if(BufMess.Pos(":->")>0) return ":->";
if(BufMess.Pos(":*>")>0) return ":*>";
if(BufMess.Pos(":%>")>0) return ":%>";
if(BufMess.Pos("#")>0)   return "#";
}
void __fastcall TForm1::Button3Click(TObject *Sender)
{
  if((Edit3->Text!="")&&(Edit4->Text!="")){
        ClientSocket1->Port = StrToInt(Edit4->Text);
        ClientSocket1->Host = Edit3->Text; // I?enaaeaaai Eeeaioo Ae-Ie ec Yaeoa
        ClientSocket1->Active = true ;
        // Aaeaai iaainooiio? "Nicaaou" (oae eae iu eiiiaeoeiny)
        Edit3->Enabled = false;
        Edit4->Enabled = false;
        Button3->Enabled = false;
        Button5->Enabled = false;
        Button2->Enabled = true;
  }else{ ShowMessage("Maydonlarni to'ldiring!"); }
```

```
}
void __fastcall TForm1::ClientSocket1Connect(TObject *Sender,
     TCustomWinSocket *Socket)
{
  Memo1->Lines->Add("Au i?eniaaeiaiu");
  //ClientSocket1->Socket->SendText(ClientSocket1->Socket-
>LocalAddress+":=>"+Edit3->Text);
}
void __fastcall TForm1::Button1Click(TObject *Sender)
{
 int i;
 if(Edit5->Text == ""){
    ShowMessage("Aaaaeoa IP-adress eioi?ue eiio iaai ioi?aaeou");
    return;
 }
 if(Edit1->Text == "") {
    ShowMessage("Aaaaeoa oaeno eioi?ue iaai ioi?aaeou");
    return;
 }
 ClientSocket1->Socket->SendText(Edit5->Text+":=>"+Edit1->Text);
// Edit1->Text = "";
}
void __fastcall TForm1::Button5Click(TObject *Sender)
{
    Edit3->Text = getIP();
}
void __fastcall TForm1::TabControl1Change(TObject *Sender)
{
if(Form1->TabControl1->TabIndex==0) Form1->GroupBox2->Visible=true;  else
Form1->GroupBox2->Visible=false;
if(Form1->TabControl1->TabIndex==1) Form1->GroupBox4->Visible=true;  else
Form1->GroupBox4->Visible=false;
if(Form1->TabControl1->TabIndex==2) Form1->GroupBox1->Visible=true;  else
Form1->GroupBox1->Visible=false;
if(Form1->TabControl1->TabIndex==3) Form1->GroupBox3->Visible=true;  else
Form1->GroupBox3->Visible=false;
}
void __fastcall TForm1::Button2Click(TObject *Sender)
{
   ClientSocket1->Close();
   Edit3->Enabled = true;
   Edit4->Enabled = true;
   Button3->Enabled = true;
   Button5->Enabled = true;
```

```
   Button2->Enabled = false;
}
void __fastcall TForm1::ClientSocket1Read(TObject *Sender,
      TCustomWinSocket *Socket)
{ int i; String Mess, n1,g1, index;
  Mess = Socket->ReceiveText();
  index = getTYPEC(Mess);
  AnsiString Rtext,Names ;  // oaeno, eioi?ue iinueaao na?aa?
  Form1->Memo2->Lines->Add("++++-"+Mess);
//Memo2->Lines->Add("I?eiyee oaeno :" + Mess);
if((index=="#")||(Receive == true)){
  if(Receive == true) // anee iu a ?a?eia ia?aaa?e oaeea, oi
  {
    Write(Mess); // caienuaaai aai a iioie
  }
  else // anee iao , oi
  {
    Memo2->Lines->Add("I?eiyee oaeno :" + Mess);
    if(Mess.SubString(0,Mess.Pos("#")-1) == "file") // Anee yoi oaee, oi...
    {
      Mess.Delete(1,Mess.Pos("#")) ;    // oaaeyai neiai file
      Names = Mess.SubString(0,Mess.Pos("#")-1); // Ii?aaaeyai eiy oaeea
      FileName = Names.SubString(Names.LastDelimiter("\\")+1,Names.Length());
; // Auaaeyai ?enoia eiy oaeea , iai?eia? n c:\\test.txt , aa?ai test.txt
      Mess.Delete(1,Mess.Pos("#")) ;  // Oaaeyai iineaaiee ?acaaeeoaeu
      Size = StrToInt(Mess.SubString(0,Mess.Pos("#")-1)) ; // Ii?aaaeyai ?acia?
oaeea
      Mess.Delete(1, Mess.Pos("#")); // Oaaeyai iineaaiee ?acaaeeoaeu
      Memo2->Lines->Add("?acia? oaeea: "+IntToStr(Size)+" aaeo"); // Auaiaei
?acia? oaeea
      Memo2->Lines->Add("Eiy oaeea: "+Names); // Auaiaei eiy oaeea
      Receive = true; // Ia?aaiaei na?aa? a ?a?ei i?e?ia oaeea
      if(Receive == true)
      {
        Memo2->Lines->Add("?a?ei i?eaia aooa?a");
      }
    }
  }
 }else{
       if(index==":->") {
         Edit6->Text = Mess.SubString(0,Mess.Pos(index)-1);
         Mess        = Mess.SubString(Mess.Pos(index)+3,Mess.Length());
         Edit8->Text = Mess.SubString(0,Mess.Pos(index)-1);
         Y           = StrToInt(Mess.SubString(Mess.Pos(index)+3,Mess.Length()));
```

```
        Edit11->Text = IntToStr(Y);
        return;
       }
       Memo1->Lines->Add(Mess);
}
}
void __fastcall TForm1::Button4Click(TObject *Sender)
{
//X = gx mod n
 if(X==0){
   X = fmod(pow(StrToInt(Edit8->Text),StrToInt(Edit9->Text)),StrToInt(Edit6->Text));
   ClientSocket1->Socket->SendText(Edit7->Text+"::>"+Edit6->Text+":->"+Edit8->Text+":->"+IntToStr(X));
 }else{
 //Z'=Zx mod n
//   if(K)
   K = fmod(pow(Y,StrToInt(Edit9->Text)),StrToInt(Edit6->Text));
   ClientSocket1->Socket->SendText(Edit7->Text+"::>"+Edit6->Text+":->"+Edit8->Text+":->"+IntToStr(K));
 }
}
void __fastcall TForm1::Button6Click(TObject *Sender)
{
 int i;
 void *P;
 int Size;
 if(Edit10->Text == ""){
    ShowMessage("Aaaaeoa IP-adress eioi?ue eiio iaai ioi?aaeou");
    return;
 }
  if(OpenDialog1->Execute())
  {
    MS->LoadFromFile(OpenDialog1->FileName);
    Memo1->Lines->Add("Caa?oceee o?aaoaiue oaee a iioie...");
    ClientSocket1->Socket->SendText(Edit10->Text+":=>file#"+OpenDialog1->FileName+"#"+IntToStr(MS->Size)+"#");
    Memo2->Lines->Add("Iineaee caaieiaie");
  }
    MS->Position = 0;
    Size = ClientSocket1->Socket->SendBuf(P,MS->Size);
    Memo2->Lines->Add("Ioi?aaeaii: " + IntToStr(Size)+" ec "+ IntToStr(MS->Size));
}
```