МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ.

С.С. Гулямов, А.А. Мусалиев, Б.А. Бегалов

ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

УЧЕБНО – МЕТОДИЧЕСКОЕ ПОСОБИЕ

ТАШКЕНТ – 2007

Содержание

Введение

Одной из важнейших составных частей национальной безопасности любой страны, в том числе и Республики Узбекистан, в настоящее время называют ее информационную безопасность.

Проблемы обеспечения информационной безопасности становятся все более сложными и концептуально значимыми в связи с массовым переходом информационно-коммуникационных технологий в управлении на безбумажную автоматизированную основу. Рождается новая современная технология – технология защиты информации в компьютерных информационных системах и системах передачи данных.

Объективными факторами повышенного интереса к данной проблеме послужили также высокие темпы роста вычислительной и коммуникационной техники, расширение областей использования ЭВМ, высокая степень концентрации информации в вычислительных системах и сетях, качественное и количественное совершенствование методов и средств доступа пользователей к информационным и вычислительным ресурсам. Кроме того, появление программных злоупотреблений, служащих основой компьютерных преступлений, значительно повысило требования к информационной безопасности, потребовало направить усилия на разработку систем по предотвращению несанкционированного доступа к информации.

При всей прогрессивности этого явления одновременно существенно расширяются и содержательно обновляются комплекс организационных, технических и технологических проблем (трудностей) в предотвращении преступного и достаточно простого вмешательства в информационные ресурсы, которые стали легкой добычей посторонних лиц.

Термин «информационная безопасность» имеет различные определения, общего или частного свойства, однако они все связывают безопасность именно с ее защитой, что в определенной степени сужает содержание этого понятия и не отражает ее глобального значения в современном управлении.

В общей трактовке под «информационной безопасностью» понимается защищенность информации на любых носителях от случайных и преднамеренных воздействий естественного или искусственного свойства, направленного на уничтожение тех или иных данных, изменение степени доступности ценных сведений.

Если раньше опасность состояла в основном в краже (воровстве, копировании) секретных или конфиденциальных сведений и документов, то в настоящее время получило развитие незаконное оперирование компьютерными базами данных (без фактической кражи), незаконное использование электронных массивов без согласия их собственника или владельца или даже извлечение материальной выгоды из таких действий.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего, вычислитель-

ных систем. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, а также программное обеспечение и базы данных, для которых технические средства являются окружением].

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, "безбумажного" документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике.

На сегодняшний день сформулировано два базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных - защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных.
- конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

1. Защита информации и информационная безопасность

Концептуальное содержание защиты информации. Защита информации в концептуальном понимании представляет собой жестко регламентированный и динамический технологический процесс, предупреждающий нарушение целостности, достоверности, доступности и конфиденциальности ценных информационных ресурсов организации и, в конечном счете, обеспечивающий реальную информационную безопасность управленческой и производственной деятельности.

Концепция находит практическое выражение в механизме (системе) защиты информации. Эта система всегда имеет в основе персональную ответственность руководителей различного уровня в соответствии с функциональными обязанностями.

Важно, что архитектура защиты должна охватывать не только компьютерные (электронные) информационные системы, а весь управленческий комплекс организации в единстве его реальных функциональных, структурных и традиционных документационных процессов. Отказаться от бумажных документов и, часто рутинной, сложившейся в организации управленческой технологии не всегда представляется возможным.

Основные понятия и определения. Учитывая, что предметом данной работы являются организация безопасности в области защиты информации прежде необходимо дать ряд основных понятий данной сферы деятельности.

Защита информации - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Эффективность защиты информации - степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

Контроль эффективности защиты информации - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

Безопасность информации (информационная безопасность) - состояние информации, информационных ресурсов и информационных и телекоммуникационных систем, в которой с требуемой вероятностью обеспечивается защита информации.

Требования по безопасности информации - руководящие документы, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности ее защиты.

Криптографическая защита - защита данных при помощи криптографического преобразования данных.

Криптографическое преобразование - преобразование данных при помощи шифрования и (или) выработки имитовставки.

Цели защиты информации. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб его собственнику, владельцу, пользователю и иному лицу. Целями защиты являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные системы;
- обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Система защиты информации. Система защиты информации (СЗИ) представляет собой комплекс организационных, технических, технологических и иных средств, методов и мер, снижающих уязвимость информации и препятствующих несанкционированному (незаконному) доступу к информации, ее утечке и утрате.

Собственники соответствующей информации, в том числе соответствующие государственные органы, лично определяют необходимую степень ее защищенности и тип системы, способы и средства защиты, исходя из ценности информации, размера ущерба от ее утраты или утечки и стоимости защитного механизма. Ценность информации и требуемая надежность ее защиты находятся в прямой зависимости.

Система защиты информации должна быть непрерывной, плановой, централизованной, целенаправленной, конкретной, активной, надежной, комплексной, легко совершенствуемой и быстро видоизменяемой. Она должна быть эффективной как в обычных условиях, так и в экстремальных ситуациях.

В процессе разработки систем защиты информации выработались некоторые общие правила, которые были сформулированы Ж. Солцером и М. Шредером (США):

1. *Простота механизма защиты.* Так как средства защиты усложняют и без того сложные программные и аппаратные средства, обеспечивающие обработку данных в ЭВМ, естественно стремление упростить эти дополнительные средства. Чем лучше совпадает представление пользователя о системе защиты с ее фактическими возможностями, тем меньше ошибок возникает в процессе работы.
2. *Разрешения должны преобладать над запретами.* Нормальным режимом работы считается отсутствие доступа, а механизм защиты должен быть основан на условиях, при которых доступ разрешается. Допуск дается лишь тем пользователям, которым он необходим.
3. *Проверка полномочий любого обращения к любому объекту информации.* Это означает, что защита выносится на общесистемный уровень и предполагает абсолютно надежное определение источника любого обращения.
4. *Разделение полномочий* заключается в определении для любой программы и любого пользователя в системе минимального круга полномочий. Это позволяет уменьшить ущерб от сбоев и случайных нарушений и сократить вероятность преднамеренного или ошибочного применения полномочий.
5. *Трудоемкость проникновения в систему.* Фактор трудоемкости зависит от количества проб, которые нужно сделать для успешного проникновения. Метод прямого перебора вариантов может дать результат, если для анализа используется сама ЭВМ.

6. *Регистрация проникновений в систему.* Иногда считают, что выгоднее регистрировать случаи проникновения, чем строить сложные системы защиты.

Защита информации в небольших организациях. В некрупных организациях с небольшим объемом информации, подлежащей защите, наиболее целесообразны и эффективны простейшие методы ее защиты. Например: выделение в отдельную группу и маркирование ценных бумажных машиночитаемых и электронных документов, назначение и обучение служащего, работающего с этими документами, организация охраны здания, введение обязательства для сотрудников о неразглашении ценных сведений, контроль за посетителями, проведение простейших действий по защите ЭВМ, ведение аналитической и контрольной работы и другие методы. Как правило, применение простейших методов защиты дает значительный эффект.

Защита информации в крупных организациях. В крупных организациях со сложной структурой, множеством информационных систем и значительными объемами информации, подлежащей защите, формируются комплексные системы защиты информации, характеризующиеся многоуровневым построением и иерархическим доступом к информации. Однако эти системы, как и простейшие методы защиты, не должны создавать сотрудникам серьезные неудобства в работе.

2. Комплексность системы защиты информации

Элементы комплексной системы защиты информации. Комплексность системы защиты информации достигается наличием в ней ряда обязательных элементов – правовых, организационных, инженерно-технических и программно-математических. Соотношение элементов и их содержание обеспечивают индивидуальность системы защиты информации организации, и гарантирует ее неповторимость и трудность преодоления.

Структура комплексной системы защиты информации представлена на рис 1.

Конкретную систему можно представить из множества разнообразных элементов. Содержание элементов системы определяет не только ее индивидуальность, но и конкретный заданный уровень защиты с учетом ценности информации и стоимости системы.

Элемент правовой защиты информации. Элемент правовой защиты информации предполагает юридическое закрепление взаимоотношений организации и государства по поводу правомерности защитных мероприятий, а также организации и персонала по поводу обязанности персонала соблюдать порядок защиты ценной информации организации и ответственности за нарушение этого порядка. Элемент включает:

- наличие в организационных документах организации, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, и в должностных инструкциях положений и обязательств по защите ценной информации организации;

- разъяснения лицам, принимаемым на работу, связанную с защищаемой информацией фирмы, о добровольности принимаемых ими на себя ограничений, обусловленных соблюдением правил допуска, доступа к такой информации и, ее использования;
- формулирование и доведения до сведения всех сотрудников организации (в том числе не связанных в своей работе с защищаемой информацией) о правовой ответственности за разглашение, уничтожение или фальсификацию информации.

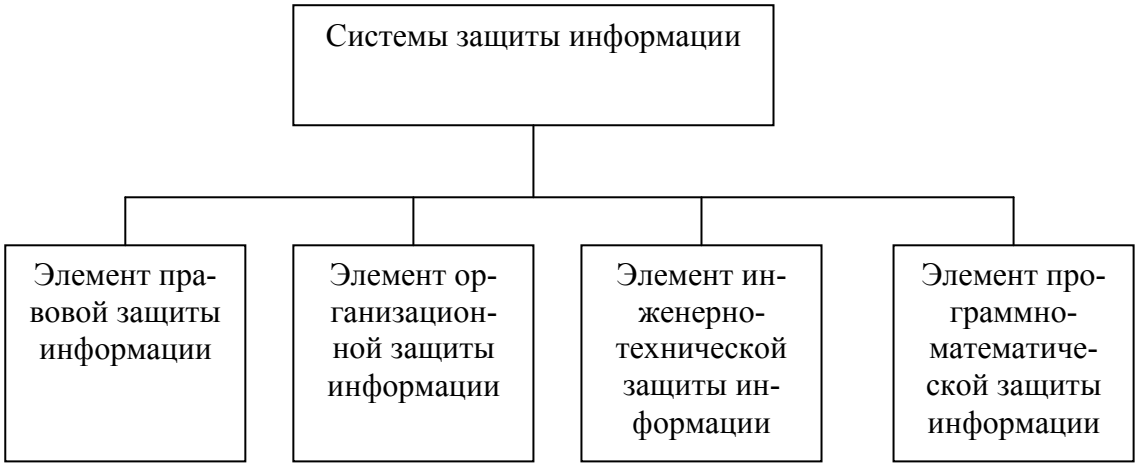

Рис 1. Структура комплексной системы защиты информации.

Элемент организационной защиты информации. Элемент организационной защиты информации содержит меры управленческого и ограничительного характера, устанавливающего технологию защиты и, побуждающего персонал соблюдать правила защиты ценной информации организации. Элемент включает в себя:

- формирование и регламентацию деятельности службы безопасности организации (или менеджера по безопасности), обеспечение этой службы нормативно-методическими документами по организации и технологии защиты информации;
- регламентацию и регулярное обновление состава (перечня, списка, матрицы) ценной информации организации, подлежащей защите, составление и ведения перечня (описи) бумажных, машинно-читаемых и электронных ценных документов организации;
- регламентацию системы (иерархической схемы) разграничения доступа персонала к ценной информации;
- регламентацию методов отбора персонала для работы с закрытой информацией, методике обучения и инструктирования сотрудников;
- регламентацию технологии защиты и обработки бумажных, машинно-читаемых и электронных документов организации (делопроизводственной, автоматизированной и смешанной технологии);

- регламентацию порядка защиты ценной информации организации от случайных или умышленных несанкционированных действий персонала;
- регламентацию порядка защиты информации при проведении совещаний, заседаний, проведения переговоров, приеме посетителей, работе с представителями средств массовой информации;
- регламентацию аналитической работы по выявлению угроз ценной информации и каналов разглашения, утечки информации;
- оборудование и аттестацию помещений и рабочих зон, выделенных для работы с ценной информацией, лицензирование технических средств и средств защиты информации и охраны, сертификацию информационных систем, предназначенных для работы с закрытой информацией;
- регламентацию пропускного режима на территории, в зданиях и помещениях организации, идентификация посетителей и персонала;
- регламентацию системы охраны территории, здания, помещений, оборудования, транспорта и персонала организации;
- регламентацию организационных вопросов эксплуатации технических средств защиты информации и охраны;
- регламентацию организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;
- регламентацию действий службы безопасности и персонала организации в экстремальных ситуациях;
- регламентацию работы по управлению системой защиты информации;
- регламентацию критериев и порядка проведения оперативных мероприятий по установлению степени эффективности системы защиты информации.

Элемент организационной защиты является стержнем, который связывает в единую систему все другие элементы. По мнению большинства специалистов, меры организационной защиты информации составляют 50-60% в структуре большинства систем защиты информации. Это связано с рядом факторов и также тем, что важной стороной организационной защиты информации является подбор, расстановка и обучение персонала, который будут осуществлять на практике принципы и методы защиты.

Организационные методы защиты информации отражаются в нормативно-методических документах службы безопасности организации. В этой связи часто используется единое название двух рассмотренных выше элементов системы защиты информации – элемент организационно-правовой защиты информации.

Элемент инженерно – технической защиты информации. Элемент инженерно – технической защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, зданий, помещения и оборудования с помощью комплексов технических средств. При защите информационных систем этот элемент имеет важное значение, хотя стоимость средств технической защиты информации и охраны очень велика. Элемент включает в себя:

- сооружение физической защиты от проникновения посторонних лиц на территорию, в здания, помещения и т.п. (заборы, решетки, стальные двери, сейфы и др.);
- средства защиты технических средств утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов, других приборов и офисного оборудования;
- средства защиты помещений от визуальных и акустических способов технической разведки;
- средства обеспечения охраны территорий, зданий и помещений (средства наблюдения, оповещения, сигнализации, информирования и идентификации);
- средства противопожарной охраны;
- средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной звукозаписывающей и телевизионной аппаратуры и т.п.);
- технические средства контроля, предотвращающие вынос персоналом специально маркированных предметов, документов, дискет, книг и т.п.

Элемент программно-математической защиты информации. Элемент программно-математической защиты информации предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, локальных сетях и различных информационных системах. Однако фрагменты этой защиты могут применяться как сопутствующие средства в инженерно- технической и организационной защите. Элемент включает в себя:

- регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;
- регламентацию специальных средств и продуктов программной защиты;
- регламентацию криптографических методов защиты информации в ЭВМ и сетях, криптографирование (шифрования) текста документов при передаче их по каналам обычной и факсимильной связи, при пересылке почтой.

3. Информационные ресурсы ограниченного распространения и угрозы ресурсам

Информационные ресурсы. Предметом информационной безопасности в единстве сформированной политике безопасности и обеспечивающей комплексной системы защиты информации рассматриваются информационные ресурсы организации. Информационные ресурсы включают в себя отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банка данных, других информационных системах).

Информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы страны и

защищаются законом наряду с другими ресурсами. Правовой режим информационных ресурсов определяются нормами, устанавливающими:

- порядок документирования информации;
- право собственности на документы и массивы документов;
- категорию информации по уровню доступа к ней;
- порядок правовой защиты информации.

Документирование информации. Документирование информации (создание официального документа) является обязательным условием включение информации в информационные ресурсы. При этом тип используемой технологической системы создания, обработки и хранения документов (делопроизводственная, ручная или автоматизированная локальная, комплексная) не имеет никакого значения. Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в установленном порядке.

С точки зрения защиты информации процесс ее документирования предусматривает объективное распространение информации во времени и пространстве и соответствующее возрастания числа опасных источников ее разглашения, подлежащих учету и контролю. Сам факт запечатления ценной информации на каком-либо носителе предполагает наличие защитных мер в отношении информации и носителя от различных рисков.

Право собственности на документы и массивы документов. По принадлежности к тому или иному виду собственности информационными ресурсы могут быть государственными или негосударственными и как элемент состава имущества находится в собственности граждан, органов местного самоуправления, организации и общественных объединений. Субъекты, предоставляющие в обязательном порядке документированную информацию в органы государственной власти и организации, не утрачивают своих прав на эти документы и на использование информации, содержащихся в них.

Государственные информационные ресурсы. Формирование государственных информационных ресурсов осуществляются гражданами, органами государственной власти, органами самоуправления, организациями и общественными объединениями.

Персональные данные. Информация о гражданах (персональные данные) также включаются в состав информационных ресурсов. Под персональными данными понимаются сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Уровень доступа к информации. В соответствии с интересами обеспечения национальной безопасности и степени ценности для государства, государственного учреждения, организации или предприятия информационные ресурсы (информация, документы) могут быть:

- открытыми, т.е. общедоступными (публикуемые в средствах массовой информации, оглашенными на конференциях, в выступлениях, интервью и т.п.);
- ограниченного доступа, т.е. защищаемыми, охраняемыми.

Следовательно, информационные ресурсы при любой технологической системе их документирования, обработки и хранения (традиционной или автоматизированной) объективно подразделяются на два самостоятельных (автономных) информационных банков: банк общедоступной информации и банк защищаемой информации регламентированного доступа. Однако, оба из указанных банков информации постоянно подвергаются объективным и субъективным угрозам разрушения носителя или самой информации.

Угроза или опасность разрушения информации. Под угрозой или опасностью понимается потенциально возможное или реальное нарушение нормального использования информационных ресурсов, их соответствие целям и задачам эффективного управления. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованное и незаинтересованное в возникновении угрозы лица. Сюда относятся также: кражи или уничтожение документов, угасание (старение) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и многое другое.

Диапазон угроз для документов ограниченного доступа значительно шире, что связано, прежде всего, с тем, что к этим документам проявляются повышенный интерес со стороны иностранных спецслужб, криминальных структур, отдельных преступных элементов, часто незаконных детективных организации, которые в совокупности именуются злоумышленниками.

Несанкционированный доступ. Основной угрозой безопасности информационным ресурсам ограниченного распространения, резко повышающим их уязвимость, является несанкционированный (незаконный) доступ постороннего лица (или работающего в организации злоумышленника) к защищаемой документированной информации, и как результат этого – овладение информацией и противоправное ее использование. Обязательным условием для осуществления попытки несанкционированного доступа к этой информации является интерес к ней со стороны определенных лиц, служб и организаций. Результатом несанкционированного доступа к защищаемой информации может быть не только владение ценными сведениями и их использование, но и их видоизменение, уничтожение, подмена и т.п.

Основным виновником несанкционированного доступа к ценной документированной информации является, как правило, персонал, работающий с другими документами и базами данных. При этом следует иметь в виду, что утрата (утеря) ценной информации происходит в большинстве случаев не в результате преднамеренных действий, а из невнимательности и безответственности персонала.

Виды угроз защищаемым информационным ресурсам. Наиболее часто встречаются следующие угрозы защищаемым информационным ресурсам:

- кража (хищение), утеря документа или отдельных его частей (листов, приложений, схем, фотографий, дискет, аудио и видеокассет и др.), носителя информации.;

- копирование бумажных и электронных документов, баз данных, фото, видео, аудиодокументов, сообщение информации или прочтение документа по линиям связи;
- подмена документов, носителей и отдельных частей документа с целью их фальсификации или сокрытия факта утери, хищения;
- работа в чужих электронных баз данных, с чужими компьютерами, тайное ознакомление с документами и базами данных, перезапись или запоминание информации;
- дистанционный просмотр документов и изображений дисплея с помощью технических средств разведки;
- ошибочные (умышленные или случайные) действия персонала при работе с документами (разрушение разрешительной системы доступа, правил обращения с документами, технологии их обработки и хранения);
- случайное или умышленное уничтожение ценных документов и баз данных, их несанкционированная модификация, искажение и фальсификация;
- считывание данных в чужих массивах за счет использования остаточной информации на копировальной ленте, бумаге, дисках и дискетках;
- утечка информации по техническим каналам при обсуждении и диктовке текста документа, работе с компьютером и другой офисной техникой.

Угрозы информационным ресурсам в компьютерных системах. Особенно опасны угрозы для электронных документов, так как определить факт кражи информации часто невозможно.

В отношении информационных ресурсов, обрабатываемых и хранящихся в компьютерах и локальных сетях, угрозы классифицируются по степени риска следующим образом:

- непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы (самая частая и большая опасность);
- кражи и подлоги информации;
- угрозы, исходящие от стихийных ситуаций внешней среды;
- угрозы заражения вирусами.

Условия утраты информационных ресурсов. Утраты или разглашение (утечка) информационных ресурсов ограниченного доступа могут наступить:

- при наличии определенных интересов определенных учреждений или лиц к конкретной информации;
- при возникновении риска угрозы, организованной злоумышленником или случайной;
- при наличии условий, позволяющего злоумышленнику осуществить необходимые действия и овладеть информацией.

Эти условия могут включать:

- отсутствие системы аналитической работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов;

- неэффективную систему защиты информации или отсутствие этой системы;
- неупорядоченный подбор персонала и текучесть кадров;
- сложный психологический климат в коллективе;
- слабые знания сотрудниками организации порядка и правил защиты информации ограниченного доступа или непонимание необходимости их соблюдения;
- отсутствие маркировки (грифирования) информации и документов (в том числе на технических носителях) ограниченного доступа;
- отсутствие контроля со стороны администрации за соблюдение персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;
- бесконтрольное посещение учреждения посторонними лицами.

Следует учитывать, что риск угрозы информации появляется сразу же при возникновении необходимости (и даже мысли) ее документирования. В связи с этим система защиты должна начинать функционировать заблаговременно.

При зарождении потребности в создании документа первоначально следует решить: является ли данная информация ограниченного доступа и, если является, то какая степень ее закрытости.

4. Каналы утечки информации

Угрозы целостности и сохранности информационных ресурсов ограниченного доступа практически реализуются через риск образования несанкционированного получения кем-то (добывания) или утраты защищаемой информации и документов. Эти каналы обозначаются, как правило, термином «каналы утечки информации». Каждая конкретная организация обладает своим набором каналов утечки, зависящим от множества объективных и субъективных факторов (профиля деятельности, объемов защищаемой информации, профессионального уровня персонала, местоположения здания организации и т.д.).

Разглашение (огласка) информации. В том случае, когда речь идет об утрате информации по вине персонала, используется термин»разглашение (огласка) информации». Человек может разглашать информацию устно, письменно, с помощью жестов, мимики, условных сигналов, лично, через посредников, по каналам связи и т.д.

Утечка информации. Термин «утечка информации» относится к утрате информации за счет ее перехвата с помощью технических средств, по техническим каналам.

Разглашение, утечка информации характеризуется двумя моментами: а) информация переходит непосредственно к заинтересованному лицу – злоумышленнику и б) к третьему лицу. Под третьим лицом в данном случае понимается любые лица (коллеги по работе, посетители, технический персонал организации, работники служб экстремальной помощи и т.п.), получившие ин-

формацию во владение в силу обстоятельств, но не обладающие правом владения ею и, что очень важно – не заинтересованные в этой информации. Однако от третьего лица информация может перейти к злоумышленнику.

Переход информации к третьему лицу можно назвать непреднамеренным, стихийным, случайным, хотя при этом факт утечки, разглашения информации, нарушения безопасности имеет место. Непреднамеренный переход информации к третьему лицу возникает в результате:

- утери или неправильного уничтожения документов, пакета с документами;
- незнание, игнорирование или умышленного выполнения сотрудником требований по защите информации;
- излишней разговорчивости сотрудников при отсутствии злоумышленника (с коллегами по работе, друзьями, иными лицами в местах общего пользования, в транспорте и т.п.);
- работы с документами ограниченного доступа при посторонних лицах, несанкционированной передачи их другому сотруднику;
- использование сведений ограниченного доступа в открытой печати, личных записях, дневниках и т.п.;
- наличие в документах излишней информации ограниченного доступа;
- самовольного копирования сотрудником документов в служебных или коллекционных целях.

В отличие от третьего лица злоумышленник целенаправленно охотится за конкретной информацией и преднамеренно, тайно создает каналы утечки или разглашения информации. Такие каналы вырабатываются злоумышленниками в зависимости от конкретных обстоятельств и отличаются большим разнообразием видов и их сочетаний.

Каналы утраты любых информационных ресурсов, особенно информации ограниченного доступа, могут быть организационными или техническими.

Организационные каналы разглашения информации. Организационные каналы разглашения информации основаны на установлении разнообразных, в т.ч. законных взаимоотношений злоумышленника с организацией или сотрудником для последующего несанкционированного доступа к интересующей злоумышленника информацией. Основными видами организационных каналов могут быть:

- поступление злоумышленника на работу в организацию, как правило, на техническую или вспомогательную должность (оператором ЭВМ, дворником, шофером и т.п.);
- установление злоумышленником доверительных взаимоотношений с сотрудниками организации или посетителем, сотрудником другой организации, имеющего доступ в данную организацию;
- анализ опубликованных материалов об организации, интервью сотрудников, статей журналистов, участие в открытых конференциях, совещаниях и т.п.;
- работа в информационных сетях;

- систематизация и анализ открытых документов организации, выделенных для уничтожения и находящихся в доступных местах, например, в пунктах вторичного сырья, на свалках и т.п.;
- криминальный, силовой доступ к информации, т.е. кража документов, дискет, компьютеров, шантаж персонала, инсценирование экстремальных ситуаций и т.п.;
- получение нужной информации от третьего (случайного) лица.

Технические каналы утечки информации. Технические каналы утечки информации возникают при использовании злоумышленником специальных технических средств разведки, позволяющую получить защищаемую информацию без контакта с персоналом организации. Эти каналы возникают при исследовании злоумышленником физических полей и излучений, возникающих в процессе работы офисной техники и перехвата информации, имеющей акустическую, визуальную или иную форму.

Любая управленческая деятельность связана с обсуждением ценной информации в кабинетах или по линиям связи, проведением расчетов и анализа ситуации на ЭВМ, печатанием и размножением документов и т.п. Все это открывает обширные технические возможности для злоумышленника в получении определенных необходимых ему сведений.

Результаты использования каналов утечки информации. В результате использования разнообразных методов и творческого сочетания каналов добывания информации ограниченного доступа злоумышленник получает:

- подлинник или оригинальную копию документа (бумажного, машиночитаемого, электронного) содержащего информацию ограниченного доступа;
- несанкционированно сделанную копию этого документа (рукописную или изготовленную с помощью копировального аппарата, фототехники, компьютера и т.д.), диктофонную, магнитофонную, видеокассету с записями текста документа, переговоров, совещаний;
- письменное или устное изложение за пределами организации содержание документа, ознакомление с которым осуществлялось санкционировано или тайно;
- устное изложение текста документа по телефону, переговорному устройству, специальной радиосвязи и т.п.;
- аналог документа, преданного по факсимильной связи или электронной почте;
- речевую или визуальную запись текста документа, выполненную с помощью технических средств разведки (радиозакладок, встроенных микрофонов и видеокамер, микрофотоаппаратов, фотографирования с большого расстояния).

Поиск и обнаружение каналов утечки информации. В основе поиска и обнаружения каналов разглашения (утечки) защищаемой информации лежит классификация и постоянное изучение источников, владеющих информацией и естественных, объективных каналов распространения этой информации.

Одновременно ведется учет, анализ и контроль потенциальных угроз информации, возможных каналов ее утраты и степени риска возникающих опасностей для информационных ресурсов. Осуществляется поиск реальных каналов разглашения (утечки) информации, оценка степени их опасности и подавление действующих опасных угроз (атак). Угрозы, каналы и риски являются одним из важнейших предметов аналитической работы, которая носит превентивный характер. На этапе обнаружения, исследования, изучения и идентификации угрозы может быть определена опасность информационным ресурсам или конкретной информации и включены дополнительные защитные механизмы.

Следовательно, обнаружение канала разглашения (утечки) информации или предотвращение его появления возможно только при наличии постоянной контрольной и аналитической системы безопасности информационных ресурсов в источнике и канале распространения информации. Уязвимым является любой элемент информационных ресурсов и информационных систем. Другие пути носят случайный характер ожидания ошибки в действиях злоумышленника, так как реальные каналы разглашения (утечки) информации всегда являются тайной этого лица.

Рекомендуемые действия по отношению к источникам информации. Рекомендуется в целях контроля следующие аналитические действия по отношению к источникам (персоналу, документам, компьютерным системам и др.), которые обладают или могут обладать защищаемой информацией:

- классификация информации ограниченного доступа и ее распределение среди персонала различных категорий;
- учет и постоянная актуализация знания состава имеющихся и возможных источников (в том числе случайных) ценной информации;
- учет и сопоставление состава ценной информации, которой обладает каждый источник, т.е. знание уровня реальной, персональной осведомленности источника;
- наблюдение за степенью эффективности применяемой системы разбиения между источниками на неконструктивные - части ими знания ценной информации;
- учет и соблюдение вариации внутренних и внешних, потенциальных и реальных (пассивных и активных) угроз источнику, выявление процесса формирования канала разглашения (утечки) ценной информации;
- наблюдение за действенностью защитных мер по отношению к каждому источнику, заблаговременное противодействие злоумышленнику.

Каналы разглашения (утечки) информации всегда индивидуальны и зависят от конкретных задач, стоящих перед злоумышленником. Обычным и профессионально грамотным является сочетание в действиях злоумышленника каналов различного типов: организационных каналов (например, шантаж сотрудника) и технических каналов (например, перехват информации по каналам связи организации с помощью этого сотрудника). Изобретательность профессио-

нального злоумышленника не имеет предела, поэтому риск утраты информации в этом случае достаточно велик.

Однако следует иметь в виду, что технические каналы (например, акустические, электронные, электромагнитные и др.), в том числе технические каналы получения информации из компьютера и по каналам связи носят стандартный характер и перекрываются стандартными средствами противодействия.

Наиболее сложными для обнаружения являются организационные каналы, связанные с так называемым человеческим фактором. Например, трудно обнаружить инициативное сотрудничество злоумышленника с сотрудником организации (секретарем, референтом, экспертом, оператором ЭВМ и т.д.). Важным средством обеспечения безопасности является механизм подотчетности (протоколирования) всех несанкционированных операций с документами и информацией. Ведение протоколов должно дополняться аудитом – анализом зарегистрированной информации.

5. Содержание служебной тайны и конфиденциальность информации

Информационные ресурсы (официально документированная информация, документы) ограниченного доступа (распространения) делятся на секретные (конфиденциальные) и несекретные. Обязательным признаком (критерием принадлежности) секретного документа является наличие в нем сведений, отнесенных к государственной тайне.

Тайна. Под тайной понимается нечто сокрытое, неизвестное, непознанное или известное только определенному кругу лиц. Синонимом такой тайны является секрет, хотя при тщательном анализе этих понятий можно говорить о том, что понятие тайны более широкое, несущее концептуальный смысл.

В научном обороте четко выделяется тайны природы (тайны объективного свойства) и тайны людей, характеризуемые субъективными критериями и часто необъяснимыми интеллектуальными потребностями. Например, личная тайна человека, тайна искусства, секреты молодости, тайны мастерства и т.д.

Тайны, секреты всегда были, есть и будут обязательным атрибутом государственного управления на любом его уровне. Одновременно постоянными являются желание одних людей или организации узнать секреты, а других сохранить их защитить от разглашения.

Тайна всегда должна находиться в безопасности, должна быть уверенность в ее безопасности. Держать что-либо в тайне, секрете – значит защитить сведения о чем, защищать информацию. Но противоположная сторона (противник, злоумышленник, конкурент, соперник, преступник) всегда будет стремиться нарушить безопасность тайны, разрушить систему защиты и добить защищаемую информацию. Эти проблемы и явления можно назвать вечными, не зависящего от технического и интеллектуального состояния общества и научно-технического прогресса человечества. Однако следует помнить, что если что-то называется тайной, то это должно быть в действительности.

Условия возникновения тайны. Тайнами могут быть: факты, события, определенные сведения, базы данных, физические поля, излучения и т.д. Все это может стать тайной при соблюдении следующих условий:

- информация не должна отражать негативные стороны деятельности организации или конкретного лица, нарушения законодательства и другие подобные факты, скрывать преступления;
- информация не должна быть общедоступной или общеизвестной;
- возникновение или получение информации должно быть законным и связано с расходованием интеллектуального потенциала организации;
- персонал организации должен знать о ценности такой информации, и обучен правилам работы с ней;
- организация должна выполнить все необходимые действия по защите этой информации.

Виды тайн. Тайна может быть: государственной, служебной, профессиональной, банковской, коммерческой (предпринимательской) и личной. В организациях, в зависимости от вида его деятельности, имеют место те или иные виды тайн.

Государственная тайна. Под государственной тайной понимаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательской и оперативно-розыскной деятельности, распространение которой может нанести ущерб государству.

Служебная тайна. Под служебной тайной понимается несекретные сведения ограниченного распространения, связанные с владением и распоряжением интеллектуальной собственности на информационные ресурсы в сфере управленческих (деловых отношений) в государственных учреждениях, утрата (разглашение, утечка, уничтожение) которых может нанести ущерб его интересам и профессиональному престижу. Служебная тайна – не коммерческая тайна ведомства, учреждения, аппарата управления организаций, которая должна быть известна строго определенному кругу должностных лиц.

Центральной проблемой при создании системы защиты информации, составляющий любой вид тайны, в том числе служебной, является формирование разрешительной системы доступа персонала к информационным ресурсам, конфиденциальным сведениям, документам, базам данных и информационным системам, которая лежит в основе обеспечения режима конфиденциальности проводимых работ. Важно четко и однозначно определить: кто, кого, к каким сведениям, когда и как допускает.

Доступ к информации в вычислительных системах. При работе сотрудников организации с информационными системами, электронными массивами конфиденциальной документов, компьютерными базами данных проблемы разграничения доступа к информации становится главным направлением в обеспечении информационной безопасности.

Доступ к электронным базам данных для сотрудников организации всегда является многоступенчатым. Выделяются следующие главные составные части доступа:

- доступ к персональному компьютеру, серверу или терминалу;
- доступ к машинным носителям информации, хранящихся вне ЭВМ;
- непосредственный доступ к базам данных и файлам.

Каждая составная часть имеют свои принципы организации, правила, методы доступа и системы контроля.

6. Методы и средства защиты информации в информационных системах

При разработке информационной системы возникают проблемы по решению вопросов безопасности информации, составляющих коммерческую тайну, а также безопасности самых информационных систем.

Признаки информационных систем. Современные информационные системы обладают следующими основными признаками:

- наличием информации различной степени конфиденциальности;
- необходимостью криптографической защиты информации различной степени конфиденциальности при передаче данных;
- иерархичностью полномочий субъектов доступа и программ к АРМ, файл-серверам, каналам связи и информации системы, необходимостью изменения этих полномочий;
- организацией обработки информации в пакетном режиме, в диалоговом режиме, в режиме разделения времени между пользователями и в режиме реального времени, в режиме телеобработки;
- обязательным управлением потоками информации как в локальных, региональных и глобальных сетях, так и при передаче данных по каналам связи на далекие расстояния;
- необходимость регистрации и учета попыток несанкционированного доступа, событий в системе и документов, выводимых на печать;
- обязательным обеспечением целостности программного обеспечения и информации в информационной системе;
- наличием средств восстановление системы защиты информации;
- обязательным учетом магнитных носителей;
- наличием физической охраны средств вычислительной и коммуникационной техники.

Организационные мероприятия и процедуры. Организационные мероприятия и процедуры, используемые для решения проблемы безопасности информации, решаются на всех этапах проектирования и в процессе эксплуатации информационной системы.

Существенное значение при проектировании придается предпроектному обследованию объекта. На этой стадии:

- устанавливается наличие секретной (конфиденциальной) информации в разрабатываемой ИС, оценивается уровень конфиденциальности и объемы;
- определяются режимы обработки информации, состав комплекса технических средств, общесистемные программные средства и т.д.;
- анализируется возможность использования имеющихся на рынке сертифицированных средств защиты информации;
- определяется степень участия персонала, функциональных служб, специалистов и вспомогательных работников объекта автоматизации в обработке информации, характер взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению режима секретности на стадиях разработки.

Среди организационных мероприятий по обеспечению безопасности информации важное место занимает охрана объекта, на которой расположена защищаемая информационная система (территория здания, помещения, хранилища информационных носителей). При этом устанавливаются соответствующие посты охраны, технические средства, предотвращающие или существенно затрудняющие хищение средств вычислительной техники, информационных носителей, а также исключающие несанкционированный доступ к ИС и линиям связи.

Функционирование системы защиты информации от несанкционированного доступа, как комплекса программно-технических средств и организационных (процедурных) решений предусматривает:

- учет, хранение и выдачу пользователям информационных носителей, паролей, ключей;
- ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа);
- оперативный контроль за функционированием систем защиты секретной информации;
- контроль соответствия общесистемной программной среды эталону;
- приемку включаемых в ИС новых программных средств;
- контроль за ходом технологического процесса обработки информации путем регистрации действий пользователей;
- сигнализацию опасных событий.

Следует отметить, что без надлежащей организационной подготовки программно-технических средств защиты информации от несанкционированного доступа и точного выполнения, предусмотренных проектно-технической документации процедур, в должной мере не решить проблему обеспечения безопасности информации, какими современными эти программно-технические средства не были.

Принципы создание базовой системы защиты информации. Создание базовой системы защиты информации в ИС основано на следующих принципах:

Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий, означающей оптимальное сочетание программно-технических средств и организационных мер защиты.

Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки, т.е. предоставление пользователям минимума строго определенных полномочий, достаточного для успешного выполнения ими своих служебных обязанностей с точки зрения автоматизированной обработки доступной им конфиденциальной информации.

Полнота контроля и регистрация попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИС без ее предварительной регистрации.

Обеспечение надежности системы защиты, т.е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.

Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

Прозрачность системы защиты информации для общего, прикладного программного обеспечения пользователей ИС.

Экономическая целесообразность использования системы защиты информации, выражающая в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации ИС без защиты системы информации.

Проблема создания системы защиты информации включает в себя две взаимно дополняющих задачи: разработка системы защиты информации (ее синтез); оценка разработанной системы защиты информации.

Вторая задача решается путем анализа технических характеристик разработанной системы защиты информации с целью установления, удовлетворяет ли она комплексу требований к таким системам. Такая задача в настоящее время решается исключительно экспертным путем с помощью сертификации средств защиты и аттестации системы защиты информации в процесс ее внедрения.

Методы и средства обеспечения безопасности информации. Методы и средства обеспечения безопасности информации представлено на рис 2.

К ***основным методам*** обеспечения безопасности информации, используемым для создания механизма защиты, относятся следующие:

Припятствия – метод физического принуждения пути злоумышленнику (к аппаратуре, носителям информации и т.д.).

Управление доступом – метод защиты информации регулированием использования всех ресурсов информационной системы (элементов баз данных, программных и технических средств). Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Маскировка – метод защиты информации путем ее криптографического закрытия. Этот метод закрытия широко применяется за рубежом, как при обработке, так и при хранении информации. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

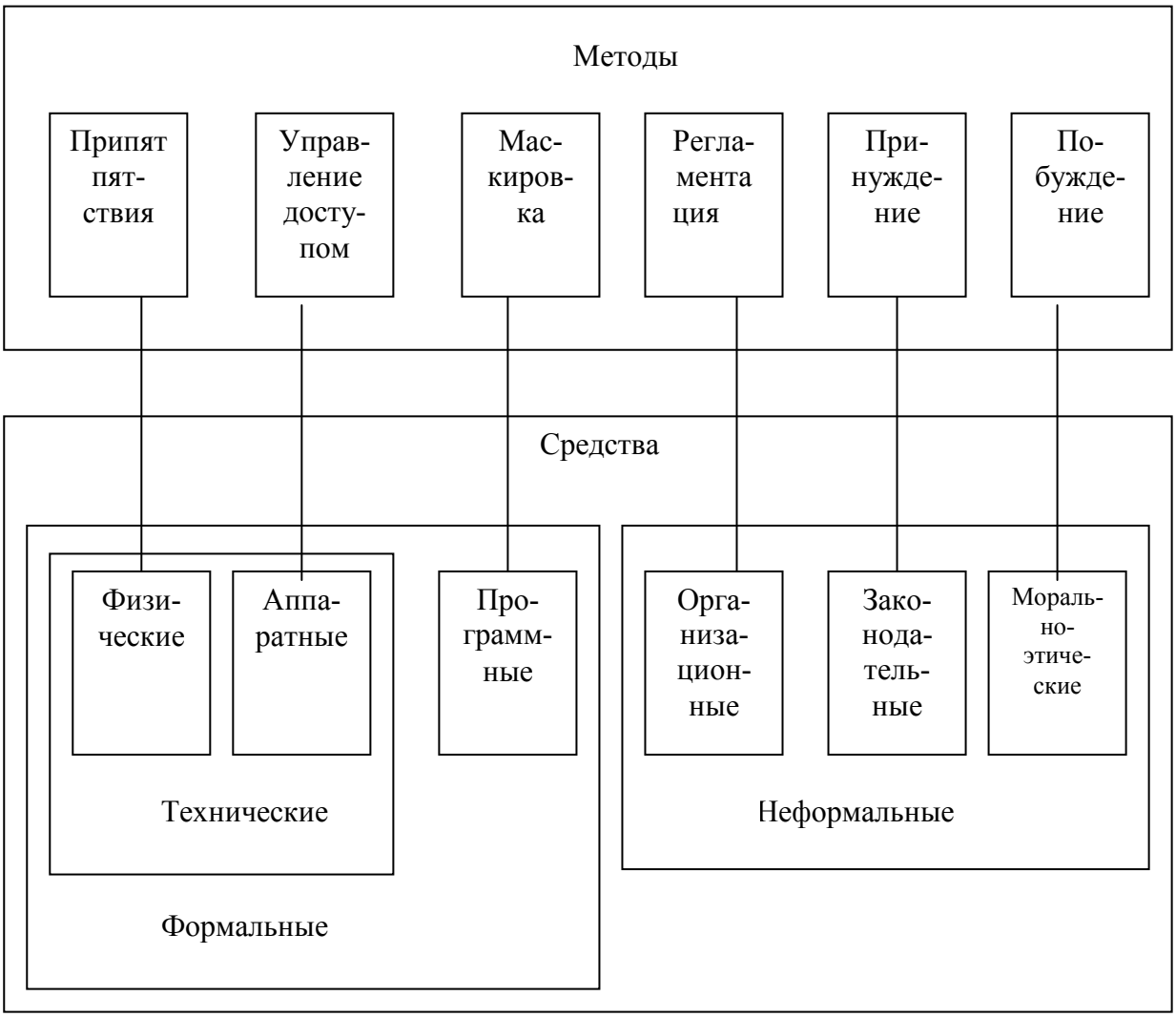

Рис 2. Методы и средства обеспечения безопасности информации.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при котором возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение – такой метод защиты информации, при котором пользователь и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – такой метод защиты информации, который побуждает пользователя и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписанных).

Рассмотренные методы обеспечения безопасности реализуется на практике за счет применения различных средств защиты, такие как технические, программные, организационные, законодательные и морально-этические.

К ***основным средствам*** защиты, используемым для создания механизма защиты, относятся следующие:

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств подразделяются на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.

Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программное обеспечение представляют собой программное обеспечение, специально предназначенное для выполнения функции защиты информации.

Организационные средства защиты информации представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной и коммуникационной техники для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы оборудования на всех этапах жизненного цикла (строительство помещений, проектирование информационной системы, монтаж, наладка оборудования, испытания, эксплуатации).

Морально-этические средства защиты реализуются в виде всевозможных форм, которые сложились традиционно или складывается по мере распространения вычислительной и коммуникационной техники в обществе. Эти нормы в большой части не являются обязательными как законодательные меры, однако несоблюдение их обычно ведет к потере авторитета и престижа человека.

Законодательные средства защиты определяются законодательными актами, которыми регламентируются правила пользования, обработки и передачи

информации ограниченного доступа и устанавливаются меры ответственности за нарушения этих правил.

Все рассмотренные средства защиты подразделяются на *формальные* (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и *неформальные* (определяется целенаправленной деятельностью человека, либо регламентирует эту деятельность).

Механизмы шифрования. Для реализации мер безопасности используются различные механизмы шифрования (криптографии).

Криптография – это наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений.

Сущность криптографических методов заключается в следующем. Готовые к передаче сообщения, будь то данные, речь или графическое изображение того или иного документа, обычно называется открытым, или незащищенным, текстом или сообщением. В процессе передачи такого сообщения по незащищенным каналам связи, оно может быть легко перехвачено или отслежено подслушивающем лицом посредством его умышленных или неумышленных действий. Для предотвращения несанкционированного доступа к этому сообщению оно зашифровывается и тем самым преобразуется в шифрограмму или закрытый текст. Когда же санкционированный пользователь получает сообщение, он дешифрирует или раскрывает его посредством обратного преобразования криптограммы, вследствие чего получается исходный открытый текст.

Методу преобразования в криптографической системе соответствует использование *специального алгоритма*. Действие такого алгоритма запускается уникальным числом или битовой последовательностью, обычно называемым *шифрующим ключом*.

Каждый используемый ключ может производить различные шифрованные сообщения, определяемые только этим ключом. Для большинства систем закрытия схема генератора ключа может представлять собой либо набор инструкции команд, либо часть, узел аппаратуры (hardware) либо компьютерную программу (software), либо все это вместе, но в любом случае процесс шифрования / дешифрования единственным образом определяется выбранным специальным ключом.

Наряду с шифрованием, также используются другие механизмы безопасности информации: цифровая (электронная) подпись, контроль доступа, обеспечение целостности данных, обеспечение аутентификации, а также постановка графика, управление маршрутизацией, арбитраж или освидетельствование.

7. Криптографические методы обработки информации

Обеспечение защиты информации от несанкционированного доступа – дело сложное, требующее широкого проведения теоретических и экспериментальных исследований по вопросам системного проектирования. Наряду с применением разных приоритетных режимов и систем разграничения доступа раз-

работчики информационных систем уделяют внимание различным криптографическим методам обработки информации.

Криптографические методы можно разбить на два класса:

1) обработка информации путем замены и перемещения букв, при котором объем данных не меняется (шифрование);
2) сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз (кодирование).

По способу реализации криптографические методы возможны в аппаратном и программном исполнении.

Для защиты текстовой информации при передачах на удаленные станции телекоммуникационной сети используются аппаратные способы шифрования и кодирования. Для обмена информацией между ЭВМ по телекоммуникационной сети, а также для работы с локальными абонентами возможны как аппаратные, так и программные способы. Для хранения информации на магнитных носителях применяются программные способы шифрования и кодирования.

Ассиметричные алгоритмы шифрования. Развитие основных типов криптографических протоколов (ключевой обмен, электронно-цифровая подпись (ЭЦП), аутентификация и др.) было бы невозможно без создания открытых ключей и построенных на их основе ассиметричных протоколов шифрования.

Основная идея асимметричных криптоалгоритмов состоит в том, что для шифрования сообщения используется один ключ, а при дешифровании – другой. Кроме того, процедура шифрования выбрана так, что она необратима даже по известному ключу шифрования – это второе необходимое условие асимметричной криптографии. То есть, зная ключ шифрования и зашифрованный текст, невозможно восстановить исходное сообщение – прочесть его можно только с помощью второго ключа – ключа дешифрования. А раз так, то ключ шифрования для отправки писем какому-либо лицу можно вообще не скрывать – зная его все равно невозможно прочесть зашифрованное сообщение. Поэтому, ключ шифрования называют в асимметричных системах "открытым ключом", а вот ключ дешифрования получателю сообщений необходимо держать в секрете – он называется "закрытым ключом".

Таким образом, избавляются от необходимости решать сложную задачу обмена секретными ключами.

Напрашивается вопрос: "Почему, зная открытый ключ, нельзя вычислить закрытый ключ?" – это третье необходимое условие асимметричной криптографии – алгоритмы шифрования и дешифрования создаются так, чтобы, зная открытый ключ, невозможно вычислить закрытый ключ.

В целом система переписки при использовании асимметричного шифрования выглядит следующим образом. Для каждого из N абонентов, ведущих переписку, выбрана своя пара ключей: "открытый" E_j и "закрытый" D_j, где j – номер абонента. Все открытые ключи известны всем пользователям сети, каждый закрытый ключ, наоборот, хранится только у того абонента, которому он принадлежит. Если абонент, скажем под номером 7, собирается передать информацию абоненту под номером 9, он шифрует данные ключом шифрования E_9 и

отправляет ее абоненту 9. Несмотря на то, что все пользователи сети знают ключ E_9 и, возможно, имеют доступ к каналу, по которому идет зашифрованное послание, они не могут прочесть исходный текст, так как процедура шифрования необратима по открытому ключу. И только абонент №9, получив послание, производит над ним преобразование с помощью известного только ему ключа D_9 и восстанавливает текст послания. Заметьте, что если сообщение нужно отправить в противоположном направлении (от абонента 9 к абоненту 7), то нужно будет использовать уже другую пару ключей (для шифрования ключ E_7, а для дешифрования – ключ D_7).

Как мы видим, во-первых, в асимметричных системах количество существующих ключей связано с количеством абонентов линейно (в системе из N пользователей используются 2*N ключей), а не квадратично, как в симметричных системах. Во-вторых, при нарушении конфиденциальности k-ой рабочей станции злоумышленник узнает только ключ D_k : это позволяет ему читать все сообщения, приходящие абоненту k, но не позволяет выдавать себя за него при отправке писем.

Стандарт ассимметричного шифрования RSA. Самым распространенным алгоритмом ассиметричного шифрования является алгоритм RSA. Он был предложен тремя исседователями-математиками Рональдом Ривестом (R.Rivest) , Ади Шамиром (A.Shamir) и Леонардом Адльманом (L.Adleman) в 1977-78 годах. Разработчикам данного алгоритма удалось эффективно воплотить идею односторонних функций с секретом. Стойкость RSA базируется на сложности факторизации больших целых чисел. В 1993 году метод RSA был обнародован и принят в качестве стандарта (PKCS #1: RSA Encryption standart). RSA можно применять как для шифрования/расшифрования, так и для генерации/проверки электронно-цифровой подписи.

Генерация ключей. Первым этапом любого асимметричного алгоритма является создание пары ключей : открытого и закрытого и распространение открытого ключа "по всему миру". Для алгоритма RSA этап создания ключей состоит из следующих операций:

-выбираются два простых (!) числа p и q

вычисляется их произведение n = (p*q)

-выбирается произвольное число e (e<n), такое, что НОД(e,(p-1)(q-1))=1, то есть e должно быть взаимно простым с числом (p-1)(q-1).

методом Евклида решается в целых числах (!) уравнение e*d+(p-1)(q-1)*y=1. Здесь неизвестными являются переменные d и y – метод Евклида как раз и находит множество пар (d,y), каждая из которых является решением уравнения в целых числах.

Два числа (e,n) – публикуются как открытый ключ.

Число d хранится в строжайшем секрете – это и есть закрытый ключ, который позволит читать все послания, зашифрованные с помощью пары чисел (e,n).

Шифрование/расшифрование. Как же производится собственно шифрование с помощью этих чисел:

Отправитель разбивает свое сообщение на блоки, равные $k=[\log_2(n)]$ бит, где квадратные скобки обозначают взятие целой части от дробного числа.

Подобный блок может быть интерпретирован как число из диапазона $(0;2^k-1)$. Для каждого такого числа (назовем его m_i) вычисляется выражение $c_i=((m_i)^e) \bmod n$. Блоки c_i и есть зашифрованное сообщение, и их можно спокойно передавать по открытому каналу, поскольку операция возведения в степень по модулю простого числа, является необратимой математической задачей. Обратная ей задача носит название "логарифмирование в конечном поле" и является на несколько порядков более сложной задачей. То есть даже если злоумышленник знает числа e и n, то по c_i прочесть исходные сообщения m_i он не может никак, кроме как полным перебором m_i.

А вот на приемной стороне процесс дешифрования все же возможен, и поможет нам в этом хранимое в секрете число d. Достаточно давно была доказана теорема Эйлера, частный случай которой утверждает, что если число n представимо в виде двух простых чисел p и q, то для любого x имеет место равенство $(x^{(p-1)(q-1)}) \bmod n = 1$. Для дешифрования RSA-сообщений воспользуемся этой формулой.

Возведем обе ее части в степень (-y) : $(x^{(-y)(p-1)(q-1)}) \bmod n = 1^{(-y)} = 1$.

Теперь умножим обе ее части на x : $(x^{(-y)(p-1)(q-1)+1}) \bmod n = 1*x = x$.

А теперь вспомним как мы создавали открытый и закрытый ключи. Мы подбирали с помощью алгоритма Евклида d такое, что $e*d+(p-1)(q-1)*y=1$, то есть $e*d=(-y)(p-1)(q-1)+1$. А следовательно в последнем выражении предыдущего абзаца мы можем заменить показатель степени на число (e*d). Получаем $(x^{e*d}) \bmod n = x$. То есть для того чтобы прочесть сообщение $c_i=((m_i)^e) \bmod n$ достаточно возвести его в степень d по модулю m:

$((c_i)^d) \bmod n = ((m_i)^{e*d}) \bmod n = m_i$.

На самом деле операции возведения в степень больших чисел достаточно трудоемки для современных процессоров, даже если они производятся по оптимизированным по времени алгоритмам. Поэтому обычно весь текст сообщения кодируется обычным блочным шифром (намного более быстрым), но с использованием ключа сеанса, а вот сам ключ сеанса шифруется как раз асимметричным алгоритмом с помощью открытого ключа получателя и помещается в начало файла.

Алгоритм ЭльГамаля. Криптографы со своей стороны вели поиски более эффективных систем открытого шифрования и в 1985 году Т.Эль-Гамаль (США) предложил следующую схему на основе возведения в степень по модулю большого простого числа P.
Задается большое простое число P и целое число A, $1 < A < P$. Сообщения представляются целыми числами M из интервала $1 < M < P$.

Шифрование сообщений. Протокол передачи сообщения M выглядит следующим образом.

абоненты знают числа **A** и **P**;

абоненты генерируют независимо друг от друга случайные числа **Ka, Kb,** удовлетворяющих условию **$1 < K < P$**

получатель вычисляет и передаёт отправителю число B, определяемое последовательностью **$B = A^{Kb} \bmod(P)$**

отправитель шифрует сообщение M и отправляет полученную последовательность получателю **$C = M * B^{Ka} \bmod(P)$**

получатель расшифровывает полученное сообщение **$D = (A^{Ka})^{-Kb} \bmod(P)$, $M = C * D \bmod(P)$**

В этой системе открытого шифрования та же степень защиты, что для алгоритма RSA с модулем **N** из **200** знаков, достигается уже при модуле **P** из **150** знаков. Это позволяет в **5-7** раз увеличить скорость обработки информации. Однако, в таком варианте открытого шифрования нет подтверждения подлинности сообщений.

Подтверждение подлинности отправителя. Для того, чтобы обеспечить при открытом шифровании по модулю простого числа P также и процедуру подтверждения подлинности отправителя Т.ЭльГамаль предложил следующий протокол передачи подписанного сообщения M:

абоненты знают числа **A** и **P**;

отправитель генерирует случайное число **Ka** удовлетворяющее условию **$1 < Ka < P$** и хранит его в секрете:

вычисляет и передаёт получателю число B, определяемое последовательностью **$B = A^{Ka} \bmod(P)$**

Для сообщения **M (1 < M < P)** выбирает случайное число **L (1 < L < P)**, удовлетворяющее условию **$(L, P - 1) = 1$**

вычисляет число **$R = A^{L} \bmod(P)$**

решает относительно S **$M = Ka * R + L * S \bmod(P)$**

передаёт подписанное сообщение **[M, R, S]**

получатель проверяет правильность подписи **$A^M = (B^R) * (R^S) \bmod(P)$**

В этой системе секретным ключом для подписывания сообщений является число X, а открытым ключом для проверки достоверности подписи число B. Процедура проверки подписи служит также и для проверки правильности расшифрования, если сообщения шифруются.

Алгоритм Шамира. Еще один интересный пример использования возведения в степень по модулю большого простого числа P для открытого шифрования предложил A.Shamir (один из авторов RSA). Как и в системе ЭльГамаля сообщения M представляются целыми числами из интервала $1 < M < P$.

Передача сообщений. Передача сообщения происходит следующим образом:

абоненты знают числа P;

абоненты генерируют независимо друг от друга случайные числа **Ka, Kb,** удовлетворяющих условию **$1 < K < P$**

отправитель вычисляет значение и передаёт получателю **$C = M^{Ka} \bmod(P)$**

получатель вычисляет и передаёт отправителю число B, определяемое последовательностью **$D = C^{Kb} \bmod(P)$**

отправитель аннулирует свой шифр и отправляет полученную последовательность получателю **$E=D^{(X-1)} \bmod(P)$ $E = D^{Fa} \bmod(P)$,** где **$Fa = Ka - 1$**

получатель расшифровывает полученное сообщение **M = E ^{Fb} mod(P),** где **Fb = Kb –1**

Пример использования. Эта процедура ОШ может быть использована, например, для таких "экзотических" целей как игра в карты по телефону. Действительно, если игрок А желает "сдать" игроку В, скажем, 5 карт из 52 как при игре в покер, он зашифровывает обозначения всех карт и передает их игроку В:

Ca = Ma ^{Ka} mod(P), где **I=1,2,..,52**

Игрок В выбирает из них 5, зашифровывает своим ключом 22 и возвращает игроку А **Da = Ca ^{Kb} mod(P),** где **I=1,2...,5**

Игрок А снимает с этих 5 карт свой шифр и выдает их игроку В. Игрок В расшифровывает полученные карты **Ma = Ea ^{Fb} mod (P)**

При этом оставшаяся часть колоды C(6)...C(52) теперь находится у игрока В, но он не может раскрыть эти карты, т.к. они зашифрованы на ключе его партнера А. Остальные процедуры игры проделываются аналогично.

Криптосистемы на основе эллиптических уравнений. Эллиптические кривые - математический объект, который может определен над любым полем (конечным, действительным, рациональным или комплексным). В криптографии обычно используются конечные поля. Эллиптическая кривая есть множество точек *(x,y),* удовлетворяющее следующему уравнению:

$y^2 = x^3 + ax + b$,

а также бесконечно удаленная точка. Для точек на кривой довольно легко вводится операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах RSA и Эль-Гамаля.

В реальных криптосистемах на базе эллиптических уравнений используется уравнение

$y^2 = x^3 + ax + b \bmod p$,

где p - простое.

Проблема дискретного логарифма на эллиптической кривой состоит в следующем: дана точка G на эллиптической кривой порядка r (количество точек на кривой) и другая точка Y на этой же кривой. Нужно найти единственную точку *x* такую, что Y = *x*G, то есть Y есть *x*-я степень G.

8. Электронно-цифровая подпись

Общие положения. При ведении деловой переписки, при заключении контрактов подпись ответственного лица является непременным атрибутом документа, преследующим несколько целей:

- гарантирование истинности письма путем сличения подписи с имеющимся образцом;
- гарантирование авторства документа (с юридической точки зрения)

Выполнение данных требований основывается на следующих свойствах подписи:

- подпись аутентична, то есть с ее помощью получателю документа можно доказать, что она принадлежит подписывающему;

- подпись неподделываема; то есть служит доказательством, что только тот человек, чей автограф стоит на документе, мог подписать данный документ, и никто иной.
- подпись непереносима, то есть является частью документа и поэтому перенести ее на другой документ невозможно.
- документ с подписью является неизменяемым.
- подпись неоспорима.
- любое лицо, владеющее образцом подписи может удостоверится, что документ подписан владельцем подписи.

Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является электронно-цифровая подпись (ЭЦП), которая сохранила основные свойства обычной подписи.

Существует несколько методов построения ЭЦП, а именно:

- шифрование электронного документа (ЭД) на основе симметричных алгоритмов. Данная схема предусматривает наличие в системе третьего лица – арбитра, пользующегося доверием обеих сторон. Авторизацией документа в даной схеме является сам факт зашифрования ЭД секретным ключем и передача его арбитру.
- использование ассиметричных алгоритмов шифрования. Фактом подписания документа является зашифрование его на секретном ключе отправителя.
- развитием предыдущей идеи стала наиболее распространенная схема ЭЦП – зашифрование окончательного результата обработки ЭД хеш-функцией при помощи ассиметричного алгоритма.

Кроме перечисленных, существуют и другие методы построения схем ЭЦП: групповая подпись, неоспариваемая подпись, доверенная подпись и др. Появление этих разновидностей обусловлено разнообразием задач, решаемых с помощью электронных технологий передачи и обработки электронных документов.

Алгоритм DSA. В 1991 г. в США был опубликован проект федерального стандарта цифровой подписи - DSS (Digital Signature Standard, [DSS91], описывающий систему цифровой подписи DSA (Digital Signature Algorithm). Одним из основных критериев при создании проекта была его патентная чистота.

Предлагаемый алгоритм DSA, имеет, как и RSA, теоретико-числовой характер, и основан на криптографической системе Эль-Гамаля в варианте Шнорра. Его надежность основана на практической неразрешимости определенного частного случая задачи вычисления дискретного логарифма. Современные методы решения этой задачи имеют приблизительно ту же эффективность, что и методы решения задачи факторизации; в связи с этим предлагается использовать ключи длиной от 512 до 1024 бит с теми же характеристиками надежности, что и в системе RSA. Длина подписи в системе DSA меньше, чем в RSA, и составляет 320 бит.

С момента опубликования проект получил много критических отзывов, многие из которых были учтены при его доработке. Одним из главных аргументов против DSA является то, что, в отличие от общей задачи вычисления дискретного логарифма, ее частный случай, использованный в данной схеме, мало изучен и, возможно, имеет существенно меньшую сложность вскрытия. Кроме того, стандарт не специфицирует способ получения псевдослучайных чисел, используемых при формировании цифровой подписи, и не указывает на то, что этот элемент алгоритма является одним из самых критичных по криптографической стойкости.

Функции DSA ограничены только цифровой подписью, система принципиально не предназначена для шифрования данных. По быстродействию система DSA сравнима с RSA при формировании подписи, но существенно (в 10-40 раз) уступает ей при проверке подписи.

Вместе с проектом DSS опубликован проект стандарта SHS (Secure Hash Standard), описывающий однонаправленную хэш-функцию SHA (Secure Hash Algorithm), рекомендованную для использования вместе с DSA. Хэш-функция SHA является модификацией алгоритма MD4, хорошо известного в криптографической литературе.

Генерация ЭЦП. При генерации ЭЦП используются параметры трех групп:

- общие параметры;
- секретный ключ;
- открытый ключ.

Общие параметры необходимы для функционирования системы в целом. Секретный ключ используется для формирования ЭЦП, а открытый – для проверки ЭЦП. Общими параметрами системы являются простые целые числа **p,q,g**, удовлетворяющие следующим условиям:

p: 2^511<p<2^512

q: простой делитель числа (p-1), который удовлетворяет условию

2^159<q<2^160

g: так называемый генератор,удовлетворяющий равенству

g=h^((p-1)/q)mod p >1.

Пararараметры **p,q,g** публикуются для всех участников обмена ЭД с ЭЦП.

Секретный ключ x случайно выбирается из диапазона [1,q] и держится в секрете.

Открытый ключ вычисляется: **y=g^x mod p**.

Также при описании данной схемы будут использоваться следующие обозначения и дополнительные параметры: m – входное сообщение пользователя для схемы с ЭЦП; k - случайное число, удовлетворяющее условию 0<k<q, хранящееся в секрете и меняющееся от одной подписи к другой; H – хэш-функция, h – хэш-код сообщения.

Процесс генерации ЭЦП состоит из нескольких этапов:

1.Вычисляется хэш-код сообщения m **h=H(m)**

2.Из диапазона [1,q] случайным образом выбирается значение k и вычисляется r= **(g^k mod p) mod q**

3. Вычисляется **S= (k^-1(h+xr)) mod q**, где **k^-1** удовлетворяет условию **(k^-1*k) mod q =1**

Значения r,s являются ЭЦП сообщения m и передаются вместе с ним по каналам связи.

Проверка ЭЦП. Пусть принято сообщение m1 и его подпись s1,r1. Проверка ЭЦП происходит следующим образом:

проверяется выполнений условий **0<r1<q, 0<s1<q,** и если хотя бы одно из них нарушено, подпись отвергается.

вычисляются значения:

w= s1^-1 mod q

u1 = (H(m1)w) mod q

u2 = ((r1/w) mod q

v = ((g^u1y^u2) mod p) mod q

проверяется равенство v = r1

Если последнее равенство выполняется, то подпись принимается. В данном стандарте специфицируется также процедура генерации основных параметров системы и проводится доказательство того, что если v=r1, то m1=m, r1=r, s1=s.

Стандарт на процедуры ЭЦП ГОСТ Р 34.10-94. Российским стандартом на процедуры выработки и проверки ЭЦП является ГОСТ Р 34.10-94. Схема ЭЦП, предложенная в данном стандарте, во многом напоминает подпись в DSA.

Цифровая подпись представляет собой два больших целых простых числа. Общедоступные параметры схемы ЭЦП (p,q,a) должны удовлетворять следующим условиям:

p: 2^501<p<2^512 или **2^1020<p<2^1020**

q: простой делитель числа (p-1), который удовлетворяет условию: **2^254<q<2^256**

a: 1<a<p-1, a^q(mod p) =1

Секретный ключ x случайно выбирается из диапазона [1,q] и держится в секрете.

Открытый ключ вычисляется: **y=a^x mod p.**

Генерация ЭЦП. Процесс генерации ЭЦП состоит из нескольких этапов:

1.Вычисляется хэш-код сообщения m h=H(m)

(хэш-функция, используемая в данном стандарте в соответствии с ГОСТ Р 34.10-94), если h(m)(mod p) = 0, то h(m) присваевается значение 0…02551

2.Из диапазона [1,q] случайным образом выбирается значение k

3. Вычисляется r= (**a^k mod p) , r1=r(mod p**); если r1=0, следует вернуться к предыдущему этапу и выработать другое значение k.

4. Вычисляется **s= (xr1+kh(m))(mod p)**; если s=0, то необходимо выработать другое значение k.

Значения r1,s1 являются ЭЦП сообщения m и передаются вместе с ним по каналам связи.

Проверка ЭЦП. Проверка ЭЦП происходит следующим образом**:**

- проверяется выполнений условий **0<r<q, 0<s<q,** и если хотя бы одно из них нарушено, подпись отвергается.
- вычисляется хэш-код данного сообщения h=H(m); Если h(m)(mod p) = 0, то битовое представление h(m): 0…02551
- Вычисляется значение **v=(h(m))^q-2(mod p).**
- Вычисляется значения **z1=sv(mod p); z2=(q-r1)v(mod p).**
- Вычисляется значение **u=(a^z1y^z2(mod p))(mod q)**
- Проверяется равенство **u = r1**

Если последнее равенство выполняется, то подпись принимается.

Цифровые подписи, основанные на симметричных криптосистемах. На первый взгляд, сама эта идея может показаться абсурдом. Действительно, общеизвестно, что так называемая «современная», она же двухключевая криптография возникла и стала быстро развиваться в последние десятилетия именно потому, что ряд новых криптографических протоколов типа протокола цифровой подписи не удалось эффективно реализовать на базе традиционных криптографических алгоритмов, широко известных и хорошо изученных к тому времени. Тем не менее, это возможно. И первыми, кто обратил на это внимание, были родоначальники криптографии с открытым ключом У. Диффи и М. Хеллман, опубликовавшие описание подхода, позволяющего выполнять процедуру цифровой подписи одного бита с помощью блочного шифра. Прежде чем изложить эту идею, сделаем несколько замечаний о сути и реализациях цифровой подписи.

Стойкость какой-либо схемы подписи доказывается обычно установлением равносильности соответствующей задачи вскрытия схемы какой-либо другой, о которой известно, что она вычислительно неразрешима. Практически все современные алгоритмы ЭЦП основаны на так называемых «сложных математических задачах» типа факторизации больших чисел или логарифмирования в дискретных полях.

Однако доказательство невозможности эффективного вычислительного решения этих задач отсутствует, и нет никаких гарантий, что они не будут решены в ближайшем будущем, а соответствующие схемы взломаны – как это произошло с «ранцевой» схемой цифровой подписи. Более того, с бурным прогрессом средств вычислительных техники «границы надежности» методов отодвигаются в область все больших размеров блока.

Всего пару десятилетий назад, на заре криптографии с открытым ключом считалось, что для реализации схемы подписи *RSA* достаточно даже 128-битовых чисел. Сейчас эта граница отодвинута до 1024-битовых чисел – практически на порядок, – и это далеко еще не предел. Это приводит к необходимости переписывать реализующие схему программы, и зачастую перепроектировать аппаратуру.

Ничего подобного не наблюдается в области классических блочных шифров, если не считать изначально ущербного и непонятного решения комитета по стандартам США ограничить размер ключа алгоритма *DES* 56-ю битами, тогда как еще во время обсуждения алгоритма предлагалось использовать ключ

большего размера. Схемы подписи, основанные на классических блочных шифрах, свободны от указанных недостатков:

- во-первых, их стойкость к попыткам взлома вытекает из стойкости использованного блочного шифра, поскольку классические методы шифрования изучены гораздо больше, а их надежность обоснована намного лучше, чем надежность асимметричных криптографических систем;
- во-вторых, даже если стойкость использованного в схеме подписи шифра окажется недостаточной в свете прогресса вычислительной техники, его легко можно будет заменить на другой, более устойчивый, с тем же размером блока данных и ключа, без необходимости менять основные характеристики всей схемы – это потребует только минимальной модификации программного обеспечения;

Итак, вернемся к схеме Диффи и Хеллмана подписи одного бита сообщения с помощью алгоритма, базирующегося на любом классическом блочном шифре. Предположим, в нашем распоряжении есть алгоритм зашифрования E_K, оперирующий блоками данных X размера n и использующий ключ размером n_K: $|X| = n$, $|K| = n_K$. Структура ключевой информации в схеме следующая: секретный ключ подписи k_S *выбирается* как произвольная (случайная) пара ключей k_0, k_1 используемого блочного шифра:

$k_S = (k_0, k_1)$;

Таким образом, размер ключа подписи равен удвоенному размеру ключа использованного блочного шифра:

$|K_S| = 2|K| = 2n_K$.

Ключ проверки представляет собой результат шифрования двух блоков текста X_0 и X_1 с ключами k_0 и k_1 соответственно:

$k_V = (C_0, C_1) = (E_{k_0}(X_0), E_{k_1}(X_1))$

где являющиеся параметром схемы блоки данных несекретны и известны проверяющей подпись стороне. Таким образом, размер ключа проверки подписи равен удвоенному размеру блока использованного блочного шифра:

$|k_V| = 2|X| = 2n$.

Алгоритм *Sig* выработки цифровой подписи для бита t ($t \in \{0,1\}$) заключается просто в выборе соответствующей половины из пары, составляющей секретный ключ подписи:

$s = S(t) = k_t$.

Алгоритм *Ver* проверки подписи состоит в проверке уравнения $E_{k_t}(X_t) = C_t$, которое, очевидно, должно выполняться для нашего t. Получателю известны все используемые при этом величины.

Таким образом, функция проверки подписи будет следующей:

$$V(t, s, K_C) = \begin{cases} 1, E_S(X_t) = C_t \\ 0, E_S(X_t) \neq C_t \end{cases}.$$

Покажем, что данная схема работоспособна, для чего проверим выполнение необходимых свойств схемы цифровой подписи:

1. Невозможность подписать бит t, если неизвестен ключ подписи. Действительно, для выполнения этого злоумышленнику потребовалось бы решить

уравнение $E_s(X_t) = C_t$ относительно s, что эквивалентно определению ключа для известных блоков шифрованного и соответствующего ему открытого текста, что вычислительно невозможно в силу использования стойкого шифра.

2. Невозможность подобрать другое значение бита t, которое подходило бы под заданную подпись, очевидна: число возможных значений бита всего два и вероятность выполнения двух следующих условий одновременно пренебрежимо мала в просто в силу использования криптостойкого алгоритма:

$\boldsymbol{E}_s(\boldsymbol{X}_0) = \boldsymbol{C}_0$, $\boldsymbol{E}_s(\boldsymbol{X}_1) = \boldsymbol{C}_1$.

Таким образом, предложенная Диффи и Хеллманом схема цифровой подписи на основе классического блочного шифра обладает такой же стойкостью, что и лежащий в ее основе блочный шифр, и при этом весьма проста. Однако, у нее есть два существенных недостатка.

Первый недостаток заключается в том, что данная схема позволяет подписать лишь один бит информации. В блоке большего размера придется отдельно подписывать каждый бит, поэтому даже с учетом хэширования сообщения все компоненты подписи – секретный ключ, проверочная комбинация и собственно подпись получаются довольно большими по размеру и более чем на два порядка превосходят размер подписываемого блока. Предположим, что в схеме используется криптографический алгоритм E_K с размером блока и ключа, соответственно n и n_K. Предположим также, что используется функция хэширования с размером выходного блока n_H. Тогда размеры основных рабочих блоков будут следующими:

размер ключа подписи: $n_{kS} = 2n_H n_K$.

размер ключа проверки подписи: $n_C = 2n_H n$.

размер подписи: $n_S = n_H \cdot n_K$.

Если, например, в качестве основы в данной схеме будет использован шифр ГОСТ 28147–89 с размером блока $n = 64$ бита и размером ключа $n_K = 256$ бит, и для выработки хэш–блоков будет использован тот же самый шифр в режиме выработки имитовставки, что даст размер хэш–блока $n_H = 64$ то размеры рабочих блоков будут следующими:

размер ключа подписи: $n_{kS} = 2n_H n_K = 2 \cdot 64 \cdot 256$ бит= 4096 байт;

размер ключа проверки подписи: $n_C = 2n_H n = 2 \cdot 64 \cdot 64$ бит = 1024 байта.

размер подписи: $n_S = n_H \cdot n_K = 64 \cdot 256$ бит = 2048 байт.

Второй недостаток данной схемы, быть может, менее заметен, но столь же серьезен. Дело в том, что пара ключей выработки подписи и проверки подписи могут быть использованы только один раз. Действительно, выполнение процедуры подписи бита сообщения приводит к раскрытию половины секретного ключа, после чего он уже не является полностью секретным и не может быть использован повторно. Поэтому для каждого подписываемого сообщения необходим свой комплект ключей подписи и проверки. Это практически исключает возможность использования рассмотренной схемы Диффи–Хеллмана в первоначально предложенном варианте в реальных системах ЭЦП.

Однако, несколько лет назад Березин и Дорошкевич предложили модификацию схемы Диффи–Хеллмана, фактически устраняющую ее недостатки.

Центральным в этом подходе является алгоритм «односторонней криптографической прокрутки», который в некотором роде может служить аналогом операции возведения в степень. Как обычно, предположим, что в нашем распоряжении имеется криптографический алгоритм E_K с размером блока данных и ключа соответственно n и n_K бит, причем $n \le n_K$.

Пусть в нашем распоряжении также имеется некоторая функция отображения $\boldsymbol{n}$–битовых блоков данных в $\boldsymbol{n_K}$–битовые $Y = P_{n \to n_K}(X)$, $|X| = n$, $|Y| = n_K$. Определим рекурсивную функцию $\boldsymbol{R_k}$ «односторонней прокрутки» блока данных T размером n бит k раз ($k \ge 0$) при помощи следующей формулы:

$$\boldsymbol{R}_{\boldsymbol{k}}(\boldsymbol{T}) = \begin{cases} \boldsymbol{T}, \boldsymbol{k} = 0, \\ \boldsymbol{E}_{\boldsymbol{P}_{\boldsymbol{n} \to \boldsymbol{n}_K}(\boldsymbol{R}_{\boldsymbol{k}-1}(\boldsymbol{T}))}(\boldsymbol{X}), \boldsymbol{k} > 0, \end{cases}$$

где X – произвольный несекретный n-битовый блок данных, являющийся параметром процедуры прокрутки.

По своей идее функция односторонней прокрутки чрезвычайно проста, надо всего лишь нужное количество раз (k) выполнить следующие действия: расширить n-битовый блок данных T до размера ключа использованного алгоритма шифрования (n_K), на полученном расширенном блоке как на ключе зашифровать блок данных X, результат зашифрования занести на место исходного блока данных (T). По определению операция $R_k(T)$ обладает двумя важными для нас свойствами:

1. Аддитивность и коммутативность по числу прокручиваний:

$$R_{k+k'}(T) = R_{k'}(R_k(T)) = R_k(R_{k'}(T)).$$

2. Односторонность или необратимость прокрутки: если известно только некоторое значение функции $R_k(T)$, то вычислительно невозможно найти значение $R_{k'}(T)$ для любого $k' < k$ – если бы это было возможно, в нашем распоряжении был бы способ определить ключ шифрования по известному входному и выходному блоку алгоритма E_K. что противоречит предположению о стойкости шифра.

Теперь покажем, как указанную операцию можно использовать для подписи блока T, состоящего из n_T битов.

Секретный ключ подписи k_S выбирается как произвольная пара блоков k_0, k_1, имеющих размер блока данных используемого блочного шифра, т.е. размер ключа выработки подписи равен удвоенному размеру блока данных использованного блочного шифра: $|k_S| = 2n$;

Ключ проверки подписи вычисляется как пара блоков, имеющих размер блоков данных использованного алгоритма по следующим формулам:

$$k_C = (C_0, C_1) = (R_{2^{n_T}-1}(K_0), R_{2^{n_T}-1}(K_1)).$$

В этих вычислениях также используются несекретные блоки данных X_0 и X_1, являющиеся параметрами функции «односторонней прокрутки», они обязательно должны быть различными. Таким образом, размер ключа проверки подписи также равен удвоенному размеру блока данных использованного блочного шифра: $|k_C| = 2n$.

Вычисление и проверка ЭЦП будут выглядеть следующим образом:

Алгоритм Sig_{n_T} выработки цифровой подписи для n_T-битового блока T заключается в выполнении «односторонней прокрутки» обеих половин ключа подписи T и $2^{n_T}–1–T$ раз соответственно:

$s = Sig_{n_T}(T) = (s_0,s_1) = R_T(k_0), R_{2^{n_T}-1-T}(k_1))$.

Алгоритм Ver_{n_T} проверки подписи состоит в проверке истинности соотношений $R_{2^{n_T}-1-T}(s_0) = C_0, R_T(s_1) = C_1$, которые, очевидно, должны выполняться для подлинного блока данных $\boldsymbol{T}$:

$R_{2^{n_T}-1-T}(s_0) = R_{2^{n_T}-1-T}(R_T(k_0)) = R_{2^{n_T}-1-T+T}(k_0) = R_{2^{n_T}-1}(k_0) = C_0$,

$R_T(s_1) = R_T(R_{2^{n_T}-1-T}(k_1)) = R_{T+2^{n_T}-1-T}(k_1) = R_{2^{n_T}-1}(k_1) = C_1$.

Таким образом, функция проверки подписи будет следующей:

$$\boldsymbol{V}(\boldsymbol{T},\boldsymbol{s},\boldsymbol{K_C}) = \begin{cases} 1, \boldsymbol{R}_{2^{n_T}-1-\boldsymbol{T}}(\boldsymbol{s}_0) = \boldsymbol{C}_0 \ \ \& \ \ \boldsymbol{R}_{\boldsymbol{T}}(\boldsymbol{s}_1) = \boldsymbol{C}_1, \\ 0, \boldsymbol{R}_{2^{n_T}-1-\boldsymbol{T}}(\boldsymbol{s}_0) \neq \boldsymbol{C}_0 \ \ | \ \ \boldsymbol{R}_{\boldsymbol{T}}(\boldsymbol{s}_1) \neq \boldsymbol{C}_1. \end{cases}$$

Покажем, что для данной схемы выполняются необходимые условия работоспособности схемы подписи:

Предположим, что в распоряжении злоумышленника есть n_T-битовый блок T, его подпись $s = (s_0,s_1)$, и ключ проверки $k_C = (C_0,C_1)$. Пользуясь этой информацией, злоумышленник пытается найти правильную подпись $s' = (s'_0,s'_1)$ для другого n_T-битового блока T'. Для этого ему надо решить следующие уравнения относительно s'_0 и s'_1:

$R_{2^{n_T}-1-T'}(s'_0) = C_0$,

$R_{T'}(s'_1) = C_1$.

В распоряжении злоумышленника есть блок данных T с подписью $s = (s_0,s_1)$, что позволяет ему вычислить одно из значений s'_0,s'_1, даже не владея ключом подписи:

(a) если $T < T'$, то $s'_0 = R_{T'}(k_0) = R_{T'-T}(R_T(k_0)) = R_{T'-T}(s_0)$,

(b) если $T > T'$, то $s'_1 = R_{2^{n_T}-1-T'}(k_1) = R_{T-T'}(R_{2^{n_T}-1-T}(k_1)) = R_{T-T'}(s_1)$.

Однако для нахождения второй половины подписи ($\boldsymbol{s}'_1$ и $\boldsymbol{s}'_0$ в случаях (a) и (b) соответственно) ему необходимо выполнить прокрутку в обратную сторону, т.е. найти $R_k(X)$, располагая только значением для большего k, что является вычислительно невозможным. Таким образом, злоумышленник не может подделать подпись под сообщением, если не располагает секретным ключом подписи.

Второе требование также выполняется: вероятность подобрать блок данных T', отличный от блока T, но обладающий такой же цифровой подписью, чрезвычайно мала и может не приниматься во внимание. Действительно, пусть цифровая подпись блоков T и T' совпадает. Тогда подписи обоих блоков будут равны соответственно:

$s = S_{n_T}(T) = (s_0,s_1) = (R_T(k_0),$

$R_{2^{n_T}-1-T}(k_1))$,

$s' = S_{n_T}(T') = (s'_0,s'_1) = (R_{T'}(k_0),\ R_{2^{n_T}-1-T'}(k_1))$,

но $s=s'$, следовательно:

$R_T(k_0) = R_{T'}(k_0)$ и $R_{2^{n_T}-1-T}(k_1) = R_{2^{n_T}-1-T'}(k_1)$.

Положим для определенности $T \le T'$, тогда справедливо следующее:

$R_{T'-T}(k_0^*) = k_0^*$, $R_{T'-T}(k_1^*) = k_1^*$, где $k_0^* = R_T(k_0)$, $k_1^* = R_{2^{n_T}-1-T'}(k_1)$

Последнее условие означает, что прокручивание двух различных блоков данных одно и то же число раз оставляет их значения неизменными. Вероятность такого события чрезвычайно мала и может не приниматься во внимание.

Таким образом рассмотренная модификация схемы Диффи–Хеллмана делает возможным подпись не одного бита, а целой битовой группы. Это позволяет в несколько раз уменьшить размер подписи и ключей подписи/проверки данной схемы. Однако надо понимать, что увеличение размера подписываемых битовых групп приводит к экспоненциальному росту объема необходимых вычислений и начиная с некоторого значения делает работу схемы также неэффективной. Граница «разумного размера» подписываемой группы находится где-то около десяти бит, и блоки большего размера все равно необходимо подписывать «по частям».

Теперь найдем размеры ключей и подписи, а также объем необходимых для реализации схемы вычислений. Пусть размер хэш–блока и блока используемого шифра одинаковы и равны n, а размер подписываемых битовых групп равен n_T. Предположим также, что если последняя группа содержит меньшее число битов, обрабатывается она все равно как полная n_T-битовая группа. Тогда размеры ключей подписи/проверки и самой подписи совпадают и равны следующей величине:

$$|\boldsymbol{K_S}| = |\boldsymbol{K_C}| = |\boldsymbol{s}| = 2\boldsymbol{n}\lceil \frac{\boldsymbol{n}}{\boldsymbol{n_T}} \rceil \approx 2\frac{\boldsymbol{n}^2}{\boldsymbol{n_T}} \text{ бит},$$

где $\lceil x \rceil$ обозначает округление числа x до ближайшего целого в сторону возрастания. Число операций шифрования $E_K(X)$, требуемое для реализации процедур схемы, определяются нижеследующими соотношениями:

при выработке ключевой информации оно равно:

$$\boldsymbol{W_K} = 2 \cdot (2^{n_T} - 1)\lceil \frac{\boldsymbol{n}}{\boldsymbol{n_T}} \rceil \approx \frac{2^{n_T+1}\boldsymbol{n}}{\boldsymbol{n_T}},$$

при выработке и проверке подписи оно вдвое меньше:

$$\boldsymbol{W_S} = \boldsymbol{W_C} = (2^{n_T} - 1)\lceil \frac{\boldsymbol{n}}{\boldsymbol{n_T}} \rceil \approx \frac{2^{n_T}\boldsymbol{n}}{\boldsymbol{n_T}}.$$

Размер ключа подписи и проверки подписи можно дополнительно уменьшить следующими приемами:

1. Нет необходимости хранить ключи подписи отдельных битовых групп, их можно динамически вырабатывать в нужный момент времени с помощью генератора криптостойкой гаммы. Ключом подписи в этом случае будет являться обычный ключ использованного в схеме подписи блочного

шифра. Например, если схема подписи будет построена на алгоритме ГОСТ 28147-89, то размер ключа подписи будет равен 256 битам.

2. Аналогично, нет необходимости хранить массив ключей проверки подписи отдельных битовых групп блока, достаточно хранить его значение хэш-функции этого массива. При этом алгоритм выработки ключа подписи и алгоритм проверки подписи будут дополнены еще одним шагом – вычислением хэш-функции массива проверочных комбинаций отдельных битовых групп.

Таким образом, проблема размера ключей и подписи решена, однако, второй недостаток схемы – одноразовость ключей – не преодолен, поскольку это невозможно в рамках подхода Диффи–Хеллмана.

Для практического использования такой схемы, рассчитанной на подпись N сообщений, отправителю необходимо хранить N ключей подписи, а получателю – N ключей проверки, что достаточно неудобно. Эта проблема может быть решена в точности так же, как была решена проблема ключей для множественных битовых групп – генерацией ключей подписи для всех N сообщений из одного мастер-ключа и свертывание всех проверочных комбинаций в одну контрольную комбинацию с помощью алгоритма вычисления хэш-функции.

Такой подход решил бы проблему размера хранимых ключей, но привел бы к необходимости вместе подписью каждого сообщения высылать недостающие N–1 проверочных комбинаций, необходимых для вычисления хэш-функции массива всех контрольных комбинаций отдельных сообщений. Ясно, что такой вариант не обладает преимуществами по сравнению с исходным.

Упомянутыми выше авторами был предложен механизм, позволяющий значительно снизить остроту проблемы. Его основная идея – вычислять контрольную комбинацию (ключ проверки подписи) не как хэш-функцию от линейного массива проверочных комбинаций всех сообщений, а попарно – с помощью бинарного дерева. На каждом уровне проверочная комбинация вычисляется как хэш-функция от конкатенации двух проверочных комбинаций младшего уровня. Чем выше уровень комбинации, тем больше отдельных ключей проверки "учитывается" в ней.

Предположим, что наша схема рассчитана на 2^L сообщений. Обозначим через $C_i^{(l)}$ i-тую комбинацию l-того уровня. Если нумерацию комбинаций и уровней начинать с нуля, то справедливо следующее условие: $0 \le i < 2^{L-l}$, а i-ая проверочная комбинация l-того уровня рассчитана на 2^l сообщений с номерами от $i \cdot 2^l$ до $(i+1) \cdot 2^l - 1$ включительно. Число комбинаций нижнего, нулевого уровня равно 2^L, а самого верхнего, L-того уровня – одна, она и является контрольной комбинацией всех 2^L сообщений, на которые рассчитана схема.

На каждом уровне, начиная с первого, проверочные комбинации рассчитываются по следующей формуле:

$$C_i^{(l+1)} = H(C_{2i}^{(l)} \| C_{2i+1}^{(l)}),$$

где через $A \| B$ обозначен результат конкатенации двух блоков данных A и B, а через $H(X)$ – процедура вычисления хэш-функции блока данных X.

При использовании указанного подхода вместе с подписью сообщения необходимо передать не N–1, как в исходном варианте, а только $\log_2 N$ контрольных комбинаций. Передаваться должны комбинации, соответствующие смежным ветвям дерева на пути от конечной вершины, соответствующей номеру использованной подписи, к корню.

Пример организации проверочных комбинаций в виде двоичного дерева в схеме на восемь сообщений приведена на рисунке 4.1. Так, при передаче сообщения № 5 (контрольная комбинация выделена рамкой) вместе с его подписью должны быть переданы контрольная комбинация сообщения № 4 ($C_4^{(0)}$), общая для сообщений №№ 6–7 ($C_3^{(1)}$) и общая для сообщений №№ 0–3 ($C_0^{(2)}$), все они выделены на рисунке другим фоном.

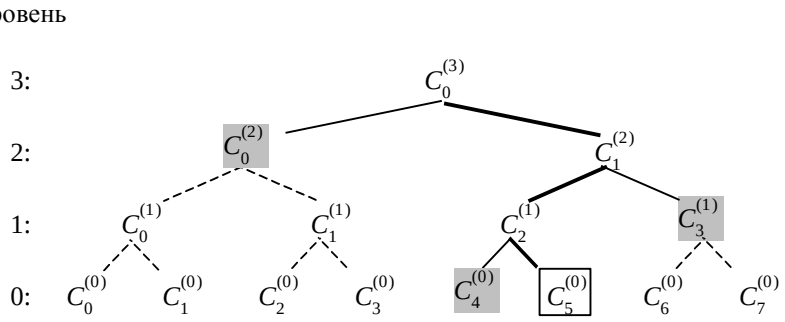

Рис. 4.1. Двоичное дерево для схемы ЭЦП на 8 сообщений

При проверке подписи значение $C_5^{(0)}$ будет вычислено из сообщения и его подписи, а итоговая контрольная комбинация, подлежащая сравнению с эталонной, по следующей формуле:

$$C = C_0^{(3)} = H(C_0^{(2)} \| H(H(C_4^{(0)} \| C_5^{(0)}) \| C_3^{(1)})).$$

Необходимость отправлять вместе с подписью сообщения дополнительную информацию, нужную для проверки подписи, на самом деле не очень обременительна. Действительно, в системе на $1024=2^{10}$ подписей вместе с сообщением и его подписью необходимо дополнительно передавать 10 контрольных комбинаций, а в системе на $1048576 = 2^{20}$ подписей – всего 20 комбинаций. Однако, при большом числе подписей, на которые рассчитана система, возникает другая проблема – хранение дополнительных комбинаций, если они рассчитаны предварительно, или их выработка в момент формирования подписи.

Дополнительные контрольные комбинации, которые передаются вместе с подписью и используются при ее проверке, вырабатываются при формировании ключа проверки по ключу подписи и могут храниться в системе и использоваться в момент формирования подписи, либо вычисляться заново в этот момент.

Первый подход предполагает затраты дисковой памяти, так как необходимо хранить 2^{L+1}–2 значений хэш-функции всех уровней, а второй требует большого объема вычислений в момент формирования подписи. Можно использовать и компромиссный подход – хранить все хэш-комбинации начиная с

некоторого уровня l^*, а комбинации меньшего уровня вычислять при формировании подписи.

В рассмотренной выше схеме подписи на 8 сообщений можно хранить все 14 контрольных комбинаций, используемых при проверки (всего их 15, но самая верхняя не используется), тогда при проверке подписи их не надо будет вычислять заново. Можно хранить 6 комбинаций начиная с уровня 1 ($C_0^{(1)}$, $C_1^{(1)}$, $C_2^{(1)}$, $C_3^{(1)}$, $C_0^{(2)}$, $C_1^{(2)}$), тогда при проверке подписи сообщения № 5 необходимо будет заново вычислить комбинацию $C_4^{(0)}$, а остальные ($C_0^{(2)}$,$C_3^{(1)}$) взять из таблицы, и т.д.. Указанный подход позволяет достичь компромисса между быстродействием и требованиям к занимаемому количеству дискового пространства.

Отметим, что отказ от хранения комбинаций одного уровня приводит к экономии памяти и росту вычислительных затрат примерно вдвое, то есть зависимость носит экспоненциальный характер.

Атаки на ЭЦП. Стойкость большинства схем ЭЦП зависит от стойкости ассиметричных алгоритмов шифрования и хэш-функций.

Существует следующая классификация атак на схемы ЭЦП:

- атака с известным открытым ключем.
- атака и известными подписанными сообщениями – противник, кроме открытого ключа имеет и набор подписанных сообщений.
- простая атака с выбором подписанных сообщений – противник имеет возможность выбирать сообщения, при этом открытый ключ он получает после выбора сообщения.
- направленная атака с выбором сообщения
- адаптивная атака с выбором сообщения.

Каждая атака преследует определенную цель, которые можно разделить на несколько классов:

- полное раскрытие. Противник находит секретный ключ пользователя
- универсальная подделка. Противник находит алгоритм, функционально аналогичный алгоритму генерации ЭЦП
- селективная подделка. Подделка подписи под выбранным сообщением.
- экзистенциальная подделка. Подделка подписи хотя бы для одного случайно выбранного сообщения.

На практике применение ЭЦП позволяет выявить или предотвратить следующие действия нарушителя:

- отказ одного из участников авторства документа.
- модификация принятого электронного документа.
- подделка документа.
- навязывание сообщений в процессе передачи – противник перехватывает обмен сообщениями и модифицирует их.
- имитация передачи сообщения.

Так же существуют нарушения, от которых невозможно оградить систему обмена сообщениями – это повтор передачи сообщения и фальсификация вре-

мени отправления сообщения. Противодействие данным нарушениям может основываться на использовании временных вставок и строгом учете входящих сообщений.

Некоторые средства работы с ЭЦП. В настоящее время существует большое количество комплексов для работы с электронной подписью, или использующие ее. Приведем некоторые из них:

PGP. Наиболее известный - это пакет PGP (Pretty Good Privacy) – (www.pgpi.org), без сомнений являющийся на сегодня самым распространенным программным продуктом, позволяющим использовать современные надежные криптографические алгоритмы для защиты информации в персональных компьютерах.

К основным преимуществам данного пакета, выделяющим его среди других аналогичных продуктов следует отнести следующие:

1. ***Открытость.*** Исходный код всех версий программ PGP доступен в открытом виде. Любой эксперт может убедиться в том, что в программе эффективно реализованы криптоалгоритмы. Так как сам способ реализации известных алгоритмов был доступен специалистам, то открытость повлекла за собой и другое преимущество - эффективность программного кода.

2. ***Стойкость.*** Для реализации основных функций использованы лучшие (по крайней мере на начало 90-х) из известных алгоритмов, при этом допуская использование достаточно большой длины ключа для надежной защиты данных

3. ***Бесплатность.*** Готовые базовые продукты PGP (равно как и исходные тексты программ) доступны в Интернете в частности на официальном сайте PGP Inc.

(www.pgpi.org).

4. ***Поддержка как централизованной*** (через серверы ключей) **так и *децентрализованной*** (через «сеть доверия») ***модели*** распределения открытых ключей.

5. ***Удобство программного интерфейса.*** PGP изначально создавалась как продукт для широкого круга пользователей, поэтому освоение основных приемов работы отнимает всего несколько часов

GNU Privacy Guard (GnuPG). GnuPG (www.gnupg.org) - полная и свободно распространяемая замена для пакета PGP. Этот пакет не использует патентованый алгоритм IDEA, и поэтому может быть использован без каких-нибудь ограничений. GnuPG соответсвует стандарту RFC2440 (OpenPGP).

Текущая версия – 1.0.4, платформы – Unices, Windows 9x/NT

Криптон. Пакет программ КРИПТОН®Подпись

(http://www.ancud.ru/crypto/crpodpis.htm) предназначен для использования электронной цифровой подписи (ЭЦП) электронных документов.

Программы пакета КРИПТОН®Подпись функционируют на компьютере, удовлетворяющем следующим требованиям:

- наличие операционной системы Windows-95/98 или Windows NT 4.0;
- наличие УКЗД серии КРИПТОН с соответствующим драйвером для Windows-95/98/NT или его программного драйвера-эмулятора для Windows - Crypton Emulator версии 1.3 или выше.

- наличие Crypton API для Windows версии 2.2 или выше (входит в поставку УКЗД серии КРИПТОН и содержит также драйвер поставляемого УКЗД);
- наличие манипулятора "мышь".

В стандартной поставке для хранения файлов открытых ключей используются дискеты. Помимо дискет, пакет КРИПТОН®Подпись дает возможность использования всех типов ключевых носителей (смарт-карт, электронных таблеток Touch Memory и др.), поддерживаемых текущей версией интерфейса SCApi, входящего в поставку Crypton API v2.2 и выше.

ВербаО - система криптографической защиты информации. СКЗИ "Верба-О" представляет собой программный комплекс, предназначенный для защиты информации при ее хранении на дисках и (или) передаче по каналам связи. СКЗИ "Верба - О" решает следующие задачи:

- шифрование/расшифрование информации на уровне файлов;
- генерацию электронной цифровой подписи (ЭЦП);
- проверку ЭЦП;
- обнаружение искажений, вносимых злоумышленниками или вирусами в защищаемую информацию.

СКЗИ "Верба - О" в различных модификациях функционирует под управлением операционных систем MS DOS v5.0 и выше, Windows 95, Windows NT, UNIX (HP UX) на персональных ЭВМ, совместимых с IBM PC/ AT. Требуемый объем оперативной памяти не более 155 Кбайт. Кроме того, необходим накопитель на гибком магнитном диске (НГМД).

Литература

1. Б.Ю. Ходиев, А.А. Мусалиев, Б.А. Бегалов. Менеджмент информационных систем. Монография. Ташкент. Изд. «Фан». 2007.
2. Миллий иктисодда ахборот тизимлари ва технологиялари: Олий укув юртлари талабалари учун укув кулланма // Муаллифлар: Р.Х.Алимов, Б.Ю.Ходиев, К.А.Алимов ва бошкалар.; С.С.Гуломовнинг умумий тахрири остида. – Т.: «Шарк», 2004.
3. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. ДМК. Москва, 2000 г.
4. "Методы и средства защиты информации" (курс лекций). Авторские права: Беляев А.В. (http://www.citforum.ru/internet/infsecure/index.shtml)
5. Криптография.
(http://www.citforum.ru/internet/securities/crypto.shtml).
6. http://www.e-sign.ru).
7. Александр Володин «Кто заверит ЭЦП». Журнал «Банковские системы» - ноябрь 2000. (http://www.bizcom.ru/system/2000-11/04.html)
8. Теоретические основы - Безопасность информационных систем – Криптографические системы.
(http://argosoft.webservis.ru/Base/Crypt.html#Механизмы шифрования)
9. Криптографические алгоритмы с открытым ключом
(http://argosoft.webservis.ru/Base/RSAintro.html#Криптографические алгоритмы с открытым ключом)
10. Современные криптографические методы защиты информации – Системы с открытым ключом.
(http://ppt.newmail.ru/crypto04.htm#Heading20)
11. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии – Москва, Горячая линия – Телеком, 2001