**Контрольная работа**

**по дисциплине**

«Информационная безопасность в телекоммуникационных системах**»**

**на тему**

«Комплексные меры по защите информации (экономическая целесообразность, физическая, электромагнитная, криптографическая, активная защита)»

# Содержание:

# Введение 2

1. **Экономическая целесообразность 3**
2. **Физическая защита 7**
3. **Электромагнитная защита 9**
4. **Криптографическая защита 13**

# Активная защита 17

# Библиографический список 19

**Введение**

Анализ состояния дел в области защиты информации показывает, что в промышленно развитых странах мира уже сложилась вполне оформившаяся инфраструктура защиты информации в системах обработки данных. И, тем не менее, количество фактов злоумышленных действий над информацией не только не уменьшается, но и имеет достаточно устойчивую тенденцию к росту. Среди всех возможных каналов утечки информации наибольшую опасность в России в ближайшее время, очевидно, будут представлять технические каналы. Такое предположение основывается на следующих фактах:

* наличии в России большого числа технически грамотных специалистов, знания и навыки которых не востребованы вследствие тяжелого экономического положения;
* выхода на российский рынок западных фирм - производителей аппаратуры для технического шпионажа;
* недостаточного внимания, а чаще всего просто игнорирования проблем безопасности информации со стороны зарождающегося российского бизнеса.

Проблема обеспечения безопасности средств и систем, связанных с обработкой информации (информационная безопасность) обусловлена автоматизацией всей информационной инфраструктуры объектов и массового подключения систем обработки информации к локальным и глобальным сетям, что существенно расширило возможности несанкционированного доступа к информационным ресурсам предприятий. В настоящее время все ведущие западные страны и Россия, в том числе, поднимаются на новый этап развития - этап становления информационного общества, когда суммарная стоимость информации и информационных технологий, использующихся в обществе, в ближайшем будущем превзойдет затраты па другие виды деятельности. Информация и информационные технологии становятся основным рыночным товаром в обществе. Поэтому наиболее важными составляющими объекта защиты является информация и средства обработки и хранения информации.

Главным отличием информационной инфраструктуры, как объекта защиты, является то, что она имеет распределенный характер, охватывая практически все компоненты организации. Все это существенно усложняет обеспечение безопасности объекта обработки информации. Защита информации может осуществляться лишь в комплексе; отдельные меры не будут иметь смысла. При этом следует помнить, что:

* стойкость защиты во всех звеньях должна быть примерно одинакова; усиливать отдельные элементы комплекса при наличии более слабых элементов - бессмысленно.
* при преодолении защиты информации усилия прикладываются именно к слабейшему звену.

Для противостояния процессу нарушения безопасности необходимо выделить однородные элементы защиты. Поскольку они обеспечивают однотипность средств используемых для противодействия угрозам, то необходимо произвести системную классификацию процессов обеспечения защищенности, выделив в нем однородные подпроцессы. Современные системы безопасности основываются на реализации комплекса мероприятий по организации защиты информации.

**Экономическая целесообразность**

Многие решения в области защиты информации часто принимаются на интуитивно-понятийном уровне, без каких-либо экономических расчетов и обоснований. В результате только те начальники служб ИБ (CISO), которые за счет своей “инициативности” смогли заявить и отстоять потребность в защите информации могли как-то повлиять на планирование бюджета компании на ИБ.

Однако современные требования бизнеса, предъявляемые к организации режима ИБ, диктуют настоятельную необходимость использовать в своей работе более обоснованные технико-экономические методы и средства, позволяющие количественно измерять уровень защищенности компании, а также оценивать экономическую эффективность затрат на ИБ.

Для оценки эффективности корпоративной системы защиты информации рекомендуется использовать некоторые показатели эффективности, например показатели: совокупной стоимости владения (ТСО), экономической эффективности бизнеса и непрерывности бизнеса(BCP), коэффициенты возврата инвестиций на ИБ (ROI) и другие.

В частности, известная методика совокупной стоимости владения (TCO) была изначально предложена аналитической компанией Gartner Group в конце 80-х годов (1986-1987) для оценки затрат на информационные технологии. Методика Gartner Group позволяет рассчитать всю расходную часть информационных активов компании, включая прямые и косвенные затраты на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников компании, реорганизацию, реструктуризацию бизнеса и т. д.

Существенно, что сегодня методика ТСО может быть использована для доказательства экономической эффективности существующих корпоративных систем защиты информации. Она позволяет руководителям служб информационной безопасности обосновывать бюджет на ИБ, а также доказывать эффективность работы сотрудников службы. Кроме того, поскольку оценка экономической эффективности корпоративной системы защиты информации становится "измеримой", становится возможным оперативно решать задачи контроля и коррекции показателей экономической эффективности и в частности показателя ТСО. Таким образом, показатель ТСО можно использовать как инструмент для оптимизации расходов на обеспечение требуемого уровня защищенности корпоративной информационной системы (КИС) и обоснование бюджета на ИБ. При этом в компании эти работы могут выполняться самостоятельно, с привлечением системных интеграторов в области защиты информации, или совместно предприятием и интегратором.

Следует отметить, что показатель ТСО может применяться практически на всех основных этапах жизненного цикла корпоративной системы защиты информации и позволяет “навести порядок” в существующих и планируемых затратах на ИБ. С этой точки зрения показатель ТСО позволяет объективно и независимо обосновать экономическую целесообразность внедрения и использования конкретных организационных и технических мер и средств защиты информации. При этом для объективности решения необходимо дополнительно учитывать и состояния внешней и внутренней среды предприятия, например показатели технологического, кадрового и финансового развития предприятия. Так как не всегда наименьший показатель ТСО корпоративной системы защиты информации может быть оптимален для компании.

Понятно, что умелое управление ТСО позволяет рационально и экономно реализовывать средства бюджета на ИБ, достигая при этом приемлемого уровня защищенности компании, адекватного текущим целям и задачам бизнеса. Существенно, что сравнение определенного показателя ТСО с аналогичными показателями ТСО по отрасли (аналогичными компаниями) и с “лучшими в группе” позволяет объективно и независимо обосновать затраты компании на ИБ. Ведь часто оказывается довольно трудно или даже практически невозможно оценить прямой экономический эффект от затрат на ИБ. Сравнение же “родственных” показателей ТСО позволяет убедиться в том, что проект создания или реорганизации корпоративной системы защиты информации компании является оптимальным по сравнению с некоторым среднестатистическим проектом в области защиты информации по отрасли. Указанные сравнения можно проводить, используя усредненные показатели ТСО по отрасли, рассчитанные экспертами Gartner Group или собственные экспертами компании с помощью методов математической статистики и обработки наблюдений.

Методика ТСО Gartner Group позволяет ответить на следующие актуальные вопросы:

* Какие ресурсы и денежные средства тратятся на ИБ?
* Оптимальны ли затраты на ИБ для бизнеса компании?
* Насколько эффективна работа службы ИБ компании по сравнению с другими?
* Как эффективно управлять инвестированием в защиту информации?
* Какие выбрать направления развития корпоративной системы защиты информации?
* Как обосновать бюджет компании на ИБ?
* Как доказать эффективность существующей корпоративной системы защиты информации и службы ИБ компании в целом?
* Какова оптимальная структура службы ИБ компании?
* Как правильно оценить аутсортинговые услуги по сопровождению корпоративной системы защиты информации?
* Как оценить эффективность проекта в области защиты информации?

В целом, определение затрат компании на ИБ подразумевает решение следующих трех задач:

1. оценку текущего уровня ТСО корпоративной системы защиты информации и КИС в целом;
2. аудит ИБ предприятия на основе сравнения уровня защищенности предприятия и рекомендуемого уровня ТСО;
3. формирование целевой модели ТСО.

Рассмотрим каждую из перечисленных задач.

Оценка текущего уровня ТСО. В ходе работ по оценке ТСО проводится сбор информации и расчет показателей ТСО организации по следующим направлениям:

* существующие компоненты КИС (включая систему защиты информации) и информационные активы компании (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства);
* существующие расходы на аппаратные и программные средства защиты информации (расходные материалы, амортизация);
* существующие расходы на организацию ИБ в компании (обслуживание систем защиты информации (СЗИ) и систем корпоративной защиты информации (СКЗИ), а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработку концепции и политики безопасности и пр.);
* существующие расходы на организационные меры защиты информации;
* существующие косвенные расходы на организацию ИБ в компании и в частности обеспечение непрерывности или устойчивости деятельности компании.

По результатам собеседования с TOP-менеджерами компании и проведения инструментальных проверок уровня защищенности организации проводится анализ следующих основных аспектов: политики безопасности; организации защиты; классификации и управления информационными ресурсами; управления персоналом; физической безопасности; администрирования компьютерных систем и сетей; управления доступом к системам; разработки и сопровождения систем; планирования бесперебойной работы организации; проверки системы на соответствие требованиям ИБ.

На основе проведенного анализа выбирается модель ТСО, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа выбирается из банка данных по эффективности затрат на ИБ и эффективности соответствующих профилей защиты аналогичных компаний.

Сравнение текущего показателя ТСО проверяемой компании с модельным значением показателя ТСО позволяет провести анализ эффективности организации ИБ компании, результатом, которого является определение “узких” мест в организации, причин их появления и выработка дальнейших шагов по реорганизации корпоративной системы защиты информации и обеспечения требуемого уровня защищенности КИС.

Формирование целевой модели ТСО. По результатам проведенного аудита моделируется целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы лучшей практики, типы СЗИ и СКЗИ, квалификация сотрудников компании и т. п.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку. Сюда же входят возможные временные увеличения затрат на управление и поддержку.

Для обоснования эффекта от внедрения новой корпоративной системы защиты информации (ROI) могут быть использованы модельные характеристики снижения совокупных затрат (ТСО), отражающие возможные изменения в корпоративной системе защиты информации.

Расходы на операции конечных пользователей. Это затраты на самоподдержку конечных пользователей, а также на поддержку пользователей друг друга в противовес официальной ИС поддержке. Затраты включают: самостоятельную поддержку, официальное обучение конечных пользователей, нерегулярное (неофициальное) обучение, самостоятельные прикладные разработки, поддержку локальной файловой системы.

Расходы на простои. Данная категория учитывает ежегодные потери производительности конечных пользователей от запланированных и незапланированных отключений сетевых ресурсов, включая клиентские компьютеры, совместно используемые серверы, принтеры, прикладные программы, коммуникационные ресурсы и программное обеспечение для связи.

Для анализа фактической стоимости простоев, которые связаны с перебоями в работе сети и которые оказывают влияние на производительность, исходные данные получают из обзора по конечным пользователям. Рассматриваются только те простои, которые ведут к потере производительности.

Вместе с методикой ТСО можно использовать разнообразные методы для расчета возврата инвестиций (ROI). Как правило, для оценки доходной части сначала анализируют те цели, задачи и направления бизнеса, которые нужно достигнуть с помощью внедрения или реорганизации существующих проектов в области системной интеграции, автоматизации и информационной безопасности. Далее используют некоторые измеримые показатели эффективности бизнеса для оценки эффекта отдельно по каждому решению. Допустим, с целью сокращения операционных расходов, обеспечения приемлемой конкурентной способности, улучшения внутреннего контроля и т. д. Указанные показатели не надо выдумывать, они существуют в избыточном виде. Далее можно использовать методики расчета коэффициентов возврата инвестиций в инфраструктуру предприятия (ROI), например, также Gartner Group.

Достаточно результативно использовать следующую комбинацию: ТСО как расходную часть и ROI как расчетную. Кроме того, сегодня существуют и другие разнообразные методы и технологии расчета и измерения различных показателей экономической эффективности

Для исключения лишних расходов по защите вся информация делится на категории в соответствии с требуемой степенью защиты. Эта степень определяется, исходя из:

* возможного ущерба для владельца при несанкционированном доступе к защищаемой информации;
* экономической целесообразности преодоления защиты для противника.

Естественно, производить такую оценку для каждого документа было бы слишком трудоёмко. Поэтому сложилась практика определения категорий секретности документов, по которым документы распределяются по формальным признакам. Например, в наших государственных органах принято 4 категории секретности:

* «для служебного пользования»,
* «секретно» (кат.3),
* «совершенно секретно», (кат.2)
* «совершенно секретно особой важности» (кат.1).

Для упрощения решения вопросов защиты следует применять аналогичную схему. Издаётся инструкция, которая определяет, по каким признакам документ (информация) относится к той или иной категории, и какие сотрудники к какой категории имеют доступ.

**Физическая защита**

Решение задачи разработки автоматизированной системы анализа физической защищенности объекта обработки и хранения информации предполагает решение следующих задач:

* рассмотрение типов объектов защиты,
* анализ угроз на объектах защиты
* классификация возможных элементов защиты.

Под объектом защиты понимают любую структуру частных, общественных, государственных, и коммерческих организаций, содержащих информацию которая имеет определенную ценность для владельцев.

В общем случае, составляющими любого объекта обработки и хранения информации являются:

1. территория организации, здания и помещения, в которых хранится и обрабатывается информация и ценности;
2. средства обработки информации (ЭВМ, локальные и глобальные сети) и оргтехнику, используемую для передачи и тиражирования информации (телефоны, факсы, копировальные аппараты, модемы);
3. электронные и бумажные носители информации (жесткие и гибкие магнитные диски, оптические накопители, CD/DVD-ROM и др.);
4. сотрудники и посетители предприятия, владеющие информацией.

Физическая защита обеспечивается службой охраны, основной задачей которой является предупреждение несанкционированного физического проникновения на территорию, в здания и помещения объекта злоумышленников и их сдерживание в течение расчетного времени (до прибытия милиции или сил поддержки).

Непременным условием поддержания ИБ является своевременное пресечение возможных акций нарушителей. Основными этапами действий потенциального злоумышленника при проникновении на объект обработки и хранения информации является: выявление объекта; наблюдение за объектом и разработка вариантов проникновения; реализация основного или альтернативного варианта проникновения на объект; уход из объекта защиты с возможной полной или частичной ликвидацией следов проникновения. Метод проникновения через несетевые периферийные устройства от остальных методов заключается в том, что для его выполнения необходимо физическое присутствие злоумышленника на объекте вычислительной техники. Поэтому главная цель охраны естественным образом может быть декомпозирована на такие частные подцели как:

* предотвращение несанкционированного доступа на территорию объекта и в его жизненно важные зоны;
* обнаружение проникшего на объект нарушителя до момента, когда он может совершить акцию, и доведение информации о вторжении до сил охраны;
* своевременное пресечение акции (захват или нейтрализация нарушителя, угрожающего функционированию объекта обработки и хранения информации), которую может совершить нарушитель, проникший на объект;
* минимизация ущерба.

Все существующие механизмы защиты работают только на этапе реализации угрозы. Т.е. по существу они являются средствами блокирующими, а не упреждающими атаки. В абсолютном большинстве случаев они защищают от атак, которые уже находятся в процессе осуществления. И даже если они смогли предотвратить ту или иную атаку, то намного более эффективным было бы упреждение атак, т.е. устранение самих предпосылок реализации вторжений.

Наиболее важной и трудной проблемой является проблема своевременного пересечения акций злоумышленника на этапе проектирования объекта обработки и хранения информации и в процессе его функционирования. На данных этапах основными задачами является следующее: какие и где ввести новые подсистемы защиты на объекте защиты или как задействовать старые подсистемы для повышения уровня защищенности объекта в текущий интервал времени.

Во время внедрения средств безопасности на объекте, человек может сделать ошибки, которые с легкостью обнаружит в дальнейшем злоумышленник. Поэтому появляется общая задача оценки некоторых показателей защищенности: время в течение, которого на объект обработки и хранения информации не будет предпринято несанкционированного действия, среднее время и вероятность проникновения на объект, степень наблюдаемости объекта защиты и другие.

**Электромагнитная защита**

Проблема утечки информации из вычислительной техники (ВТ) через побочные электромагнитные излучения и наводки (ПЭМИН) известна специалистам уже на протяжении более чем 20 лет.

Возможные каналы утечки информации образуются:

* НЧ электромагнитными полями, возникающими при работе технических средств передачи, обработки, хранения, отображения информации и вспомогательных технических средств и систем ;
* при воздействии на технические средства передачи, обработки, хранения, отображения информации и вспомогательные технические средства и систем, магнитных и акустических полей;
* при возникновении паразитной ВЧ генерации;
* при прохождении информативных (опасных) сигналов в цепи электропитания;
* при взаимном влиянии цепей;
* при прохождении информативных (опасных) сигналов в цепи заземления;
* при паразитной модуляции ВЧ сигнала;
* вследствие ложных коммутаций и несанкционированных действий.

При передаче информации с ограниченным доступом в элементах схем, конструкций, подводящих и соединяющих проводах технических средств протекают токи информативных (опасных) сигналов. Возникающие при этом электромагнитные поля могут воздействовать на случайные антенны. Сигналы, принятые случайными антеннами, могут привести к образованию каналов утечки информации.

Работа персонального компьютера, как и любого другого электронного устройства, сопровождается электромагнитными излучениями радиодиапазона. Для ПК эти излучения регистрируются в диапазоне до 1 ГГц с максимумом в полосе 50 МГц – 300 МГц. Такой широкий спектр излучения объясняется тем, что в устройствах ВТ информацию переносят последовательности прямоугольных импульсов малой длительности. Поэтому непреднамеренное излучение будет содержать составляющие с частотами, как первых гармоник, так и гармоник более высоких порядков.

К появлению дополнительных составляющих в побочном электромагнитном излучении приводит и применение в ВТ высокочастотной коммутации. Говорить о какой-либо диаграмме направленности электромагнитных излучений ПК не приходится, так как на практике расположение его составных частей (системный блок, монитор, соединительные кабели и провода питания) относительно друг друга имеет неограниченное число комбинаций. Поляризация излучений ПК – линейная. В конечном счете, она определяется расположением соединительных кабелей, так как именно они являются основными источниками излучений в ПК, у которых системный блок имеет металлический кожух.

Кроме излученного электромагнитного поля вблизи работающего ПК существуют квазистатические магнитные и электрические поля, быстро убывающие с расстоянием, но вызывающие наводки на любые проводящие цепи (металлические трубы, телефонные провода, провода системы пожарной безопасности и т.д.). Эти поля существенны на частотах от десятков килогерц до десятков мегагерц. Что касается уровней побочных электромагнитных излучений ВТ, то они регламентированы с точки зрения электромагнитной совместимости целым рядом зарубежных и отечественных стандартов, Так, например, согласно публикации N22 CISPR (Специальный Международный Комитет по Радиопомехам) для диапазона 230-1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием ВТ, на расстоянии 10 метров не должен превышать 37 dB. Очевидно, что этот уровень излучения достаточен для перехвата на значительных расстояниях.

Таким образом, соответствие электромагнитных излучений средств ВТ нормам на электромагнитную совместимость не является гарантией сохранения конфиденциальности обрабатываемой в них информации. Кроме того, надо заметить, что значительная часть парка ПК в России не отвечает даже этим нормам, так как в погоне за дешевизной в страну ввозилась техника в основном «желтой» сборки, не имеющая сертификатов качества.

Самым мощным источником излучения в ПК является система синхронизации. Однако перехват немодулированных гармоник тактовой частоты вряд ли сможет кого-нибудь заинтересовать.

При использовании для перехвата ПЭМИН обычного бытового радиоприемника возможно распознавание на слух моментов смены режимов работы ПК, обращения к накопителям информации на жестком и гибком магнитных дисках, нажатия клавиш и т.д. Но подобная информация может быть использована только как вспомогательная и не более.

Таким образом, не все составляющие побочного излучения персональных компьютеров являются опасными с точки зрения реального перехвата обрабатываемой в них информации. Для восстановления информации анализ лишь уровня электромагнитных излучений недостаточен, нужно еще знать их структуру. Поэтому в техническом плане проще всего решается задача перехвата информации, отображаемой на экране дисплея ПК.

Информация, отображенная на экране дисплея, может быть восстановлена в монохромном виде с помощью обыкновенного телевизионного приемника. При этом на экране телевизионного приемника изображение будет состоять из черных букв на белом фоне, а на экране дисплея ПК - из белых букв на черном фоне. Это объясняется тем, что в отличие от дисплея максимум видеосигнала в телевизионном приемнике определяет уровень черного, а минимум - уровень белого.

Выделение из ПЭМИН ПК информации о сигнале синхронизации изображения представляет собой довольно сложную техническую задачу. Гораздо проще эта проблема решается использованием внешних перестраиваемых генераторов синхросигналов. Даже при использовании обычных комнатных телевизионных антенн (например, типа «Маяк») перехват информации может быть осуществлен на расстояниях порядка 10-15 метров. При использовании направленных антенн с большим коэффициентом усиления дальность перехвата возрастает до 50-80 метров. При этом лучшее качество восстановления информации соответствует текстовым изображениям.

Современный уровень развития электроники позволяет изготовить подобные устройства перехвата информации небольших размеров, что обеспечит необходимую скрытность их работы.

В качестве технических способов исключения возможностей перехвата информации за счет ПЭМИН ПК можно перечислить следующие:

* доработка устройств ВТ с целью минимизации уровня излучений;
* электромагнитная экранировка помещений, в которых расположена вычислительная техника;

Экраны помещений выполняются в виде цельносварной металлической конструкции. В экране помещений предусматриваются так называемые технологические отверстия, которые в той или иной степени снижают эффективность экранирования. К таким отверстиям относятся: дверные и оконные проемы, смотровые и вентиляционные отверстия, отверстия для подвода электропитания, связи сигнализации и контроля, а также отверстия для ввода труб водоснабжения, отопления и др.

Для уменьшения просачивания излучений РЭС все технологические отверстия оборудуются специальными фильтрами и экранами.

Дверные проемы оборудуются уплотняющими устройствами, обеспечивающими хороший контакт обшитой металлом двери с экраном стен. В некоторых случаях для повышения эффективности экранирования оборудуются входные тамбуры с двойными или тройными дверями.

Для ослабления излучений по вводам проводов цепей электропитания, связи управления, сигнализации и т.д. применяются специальные фильтры (заградительные или поглощающие). Заградительные фильтры представляют собой индуктивно-емкостные цепи с сосредоточенными параметрами. Поглощающие фильтры основаны на применении твердых и сыпучих поглотителей: смеси песка и чугунной дроби, ферритовых порошков и т.д.

Экранирование вентиляционных отверстий производится с помощью диафрагм и ловушек различного сечения, представляющих запредельные волноводы. Диафрагмы используются в основном в диапазоне менее 10000 МГц.

На частотах свыше 10000 МГц для экранирования вентиляционных каналов целесообразно применять ловушки. Ловушка представляет собой зигзагообразно изогнутый по длине металлический короб с поперечным сечением, равным сечению вентиляционного отверстия. На внутреннюю поверхность короба наносится радиопоглощающий материал с рифленой поверхностью. Эффективность ловушки определяется качеством радиопоглощающего материала и числом зигзагов.

Помимо сеток для экранирования дверей и окон возможно применение металлизированных штор из токопроводящей ткани. Для изготовления штор могут применяться ткани трех типов. Первый тип представляет хлопчатобумажную ткань плотного плетения, на которую методом распыления нанесен тонкий слой алюминия или цинка.

Ткани второго типа содержит в своей основе металлические нити, которые при скручивании образуют соленоиды. Вихревые токи, возникающие в соленоидах, препятствуют прохождению радиоволн через ткань.

Третий тип тканей представляет собой волокнистые материалы с содержанием углерода до 98%.

Повышение эффективности экранирования стен, потолка и пола помещения может быть достигнуто путем нанесения на них токопроводящих покрытий, проведения металлизации их поверхностей или оклеивания металлической фольгой.

Проведение частичного экранирования может обеспечить (с учетом ослабляющего действия стен и перекрытий зданий) в диапазоне 0.3-10 ГГЦ снижение уровня излучения от 30 до 80дб.

Используя различные радиопоглощающие материалы и схемотехнические решения удается существенно снизить уровень излучений ВТ. Стоимость подобной доработки зависит от размера требуемой зоны безопасности и колеблется в пределах 20-70% от стоимости ПК.

Электромагнитная экранировка помещений в широком диапазоне частот является сложной технической задачей, требует значительных капитальных затрат и не всегда возможна по эстетическим и эргономическим соображениям.

**Криптографическая защита**

Криптография– область знаний, изучающая тайнопись (криптография) и методы ее раскрытия (криптоанализ). Криптография считается разделом математики.

До недавнего времени все исследования в этой области были только закрытыми, но в посление несколько лет у нас и за рубежом стало появляться всё больше публикаций в открытой печати. Отчасти смягчение секретности объясняется тем, что стало уже невозможным скрывать накопленное количество информации. С другой стороны, криптография всё больше используется в гражданских отраслях, что требует раскрытия сведений.

Криптография, в отличие от мер физической защиты, обладает тем уникальным свойством, что при правильном выборе метода затраты на обеспечение защиты информации много меньше затрат на преодоление этой защиты.

Цель криптографической системы заключается в том, чтобы зашифровать осмысленный исходный текст (также называемый открытым текстом), получив в результате совершенно бессмысленный на взгляд шифрованный текст (шифртекст, криптограмма). Получатель, которому он предназначен, должен быть способен расшифровать (говорят также "дешифровать") этот шифртекст, восстановив, таким образом, соответствующий ему открытый текст. При этом противник (называемый также криптоаналитиком) должен быть неспособен раскрыть исходный текст. Существует важное отличие между расшифрованием (дешифрованием) и раскрытием шифртекста.

Раскрытием криптосистемы называется результат работы криптоаналитика, приводящий к возможности эффективного раскрытия любого, зашифрованного с помощью данной криптосистемы, открытого текста. Степень неспособности криптосистемы к раскрытию называется ее стойкостью.

Вопрос надёжности систем ЗИ - очень сложный. Дело в том, что не существует надёжных тестов, позволяющих убедиться в том, что информация защищена достаточно надёжно. Во-первых, криптография обладает той особенностью, что на "вскрытие" шифра зачастую нужно затратить на несколько порядков больше средств, чем на его создание. Следовательно, тестовые испытания системы криптозащиты не всегда возможны. Во-вторых, многократные неудачные попытки преодоления защиты вовсе не означают, что следующая попытка не окажется успешной. Не исключён случай, когда профессионалы долго, но безуспешно бились над шифром, а некий новичок применил нестандартный подход - и шифр дался ему легко. В результате такой плохой доказуемости надёжности средств ЗИ на рынке очень много продуктов, о надёжности которых невозможно достоверно судить. Естественно, их разработчики расхваливают на все лады своё произведение, но доказать его качество не могут, а часто это и невозможно в принципе. Как правило, недоказуемость надёжности сопровождается ещё и тем, что алгоритм шифрования держится в секрете.

На первый взгляд, секретность алгоритма служит дополнительному обеспечению надёжности шифра. Это аргумент, рассчитанный на дилетантов. На самом деле, если алгоритм известен разработчикам, он уже не может считаться секретным, если только пользователь и разработчик - не одно лицо. К тому же, если вследствие некомпетентности или ошибок разработчика алгоритм оказался нестойким, его секретность не позволит проверить его независимым экспертам. Нестойкость алгоритма обнаружится только тогда, когда он будет уже взломан, а то и вообще не обнаружится, ибо противник не спешит хвастаться своими успехами.

Поэтому криптограф должен руководствоваться правилом, впервые сформулированным голландцем Керкхоффом: стойкость шифра должна определяться только секретностью ключа. Иными словами, правило Керкхоффа состоит в том, что весь механизм шифрования, кроме значения секретного ключа априори считается известным противнику.

Все методы шифровки можно разделить на две группы: шифры с секретным ключом и шифры с открытым ключом.

Первые характеризуются наличием некоторой информации (секретного ключа), обладание которой даёт возможность как шифровать, так и расшифровывать сообщения. Поэтому они именуются также одноключевыми. Шифры с открытым ключом подразумевают наличие двух ключей - открытого и закрытого; один используется для шифровки, другой для расшифровки сообщений. Эти шифры называют также двухключевыми.

Этот тип шифров подразумевает наличие некой информации (ключа), обладание которой позволяет как зашифровать, так и расшифровать сообщение. С одной стороны, такая схема имеет те недостатки, что необходимо кроме открытого канала для передачи шифрограммы наличие также секретного канала для передачи ключа, а кроме того, при утечке информации о ключе, невозможно доказать, от кого из двух корреспондентов произошла утечка.

С другой стороны, среди шифров именно этой группы есть единственная в мире схема шифровки, обладающая абсолютной теоретической стойкостью. Все прочие можно расшифровать хотя бы в принципе. Такой схемой является обычная шифровка (например, операцией XOR) с ключом, длина которого равна длине сообщения. При этом ключ должен использоваться только раз. Любые попытки расшифровать такое сообщение бесполезны, даже если имеется априорная информация о тексте сообщения. Осуществляя подбор ключа, можно получить в результате любое сообщение.

Шифры с открытым ключом подразумевают наличие двух ключей - открытого и закрытого; один используется для шифровки, другой для расшифровки сообщений. Открытый ключ публикуется - доводится до сведения всех желающих, секретный же ключ хранится у его владельца и является залогом секретности сообщений. Суть метода в том, что зашифрованное при помощи секретного ключа может быть расшифровано лишь при помощи открытого и наоборот. Ключи эти генерируются парами и имеют однозначное соответствие друг другу. Причём из одного ключа невозможно вычислить другой.

Характерной особенностью шифров этого типа, выгодно отличающих их от шифров с секретным ключом, является то, что секретный ключ здесь известен лишь одному человеку, в то время как в первой схеме он должен быть известен по крайней мере двоим. Это даёт такие преимущества:

* не требуется защищённый канал для пересылки секретного ключа, вся связь осуществляется по открытому каналу;
* «что знают двое, знает свинья» - наличие единственной копии ключа уменьшает возможности его утраты и позволяет установить чёткую персональную ответственность за сохранение тайны;
* наличие двух ключей позволяет использовать данную шифровальную систему в двух режимах - секретная связь и цифровая подпись.

Все государства уделяют пристальное внимание вопросам криптографии. Наблюдаются постоянные попытки наложить некие рамки, запреты и прочие ограничения на производство, использование и экспорт криптографических средств. Например, в России лицензируется ввоз и вывоз средств защиты информации, в частности, криптографических средств, согласно Указу Президента Российской Федерации от 3 апреля 1995 г. N 334 и постановлению Правительства Российской Федерации от 15 апреля 1994 г. N 331.

Криптографическая защита относительно дёшева, а средства её преодоления либо очень дороги, либо вообще не существуют.

Криптосистема не может считаться надёжной, если не известен полностью алгоритм её работы. Только зная алгоритм, можно проверить, устойчива ли защита. Однако проверить это может лишь специалист, да и то зачастую такая проверка настолько сложна, что бывает экономически нецелесообразна.

Чтобы продавать средства информационной защиты, сертификация необходима. Такие положения действуют в России и в большинстве стран.

У нас единственным органом, уполномоченным проводить сертификацию, является Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ). Орган этот подходит к вопросам сертификации очень тщательно. Совсем мало разработок сторонних фирм смогли получить сертификат ФАПСИ. Иногда можно наблюдать такую картину. Фирма торгует неким программным, программно аппаратным комплексом или техническим решением, при этом гордо заявляет: «Продукция имеет сертификат ФСБ, Минсвязи, Госсвязьнадзора и т.п.» Надо сознавать, что документы эти юридически ничтожны.

ФСБ уполномочена лишь создавать и эксплуатировать без лицензирования средства криптозащиты (ст.20 ФЗ "Об органах федеральной службы безопасности в Российской Федерации"; п.8 Положения о Федеральной службе безопасности Российской Федерации, утв. Указом Президента РФ от 6 июля 1998 г. N 806). Также право на создание и эксплуатацию криптографических средств предоставлено Федеральной службе охраны (ст.30 ФЗ "О государственной охране"). А вот Службе внешней разведки в праве разрабатывать криптосредства отказано (ст.6 ФЗ "О внешней разведке"). Порядок сертификации установлен Положением о сертификации средств защиты информации (утв. постановлением Правительства РФ от 26 июня 1995 г. N 608).

Кроме того, ФАПСИ лицензирует деятельность предприятий, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации (Указ Президента РФ от 03.04.95 N 334 "О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации"; а также Закон РФ "О федеральных органах правительственной связи и информации").

Для сертификации необходимым условием является соблюдение стандартов при разработке систем защиты информации. Стандарты выполняют сходную функцию. Они позволяют, не проводя сложных, дорогостоящих и даже не всегда возможных исследований, получить уверенность, что данный алгоритм обеспечивает защиту достаточной степени надёжности.

**Активная защита**

Этот вид защиты - самый эффективный в тех случаях, когда точно известен источник угрозы для вашей информации. Если это так, то предпринимаются активные мероприятия против попыток получить доступ к вашей информации. Например, следующие:

* поиск и выведение из строя устройств для скрытого съёма вашей информации;
* выявление и задержание лиц, устанавливающих такие устройства или совершающих иные незаконные действия по доступу к вашей информации;
* выявление возможных каналов утечки или несанкционированного доступа к вашей информации и направление по таким каналам дезинформации;
* создание ложных потоков информации с целью маскировки истинных потоков и отвлечения сил противника на их дешифровку;
* демонстрации противнику возможностей вашей защиты (не обязательно истинных) для создания у него впечатления бесперспективности преодолеть вашу защиту;
* контрразведывательные мероприятия с целью получить сведения о том, как именно противник получает доступ к вашей информации и соответствующего противодействия.

Активная радиотехническая маскировка предполагает формирование и излучение в непосредственной близости от ВТ маскирующего сигнала. Различают энергетический и неэнергетический методы активной маскировки. При энергетической маскировке излучается широкополосный шумовой сигнал с уровнем, существенно превышающим во всем частотном диапазоне уровень излучений ПК. Одновременно происходит наводка шумовых колебаний в отходящие цепи. Возможности энергетической активной маскировки могут быть реализованы только в случае, если уровень излучений ПК существенно меньше норм на допускаемые радиопомехи от средств ВТ. В противном случае устройство активной энергетической маскировки будет создавать помехи различным радиоустройствам, расположенным поблизости от защищаемого средства ВТ, и потребуется согласование его установки со службой радиоконтроля. Из устройств активной энергетической маскировки наиболее известны: «Гном», «Шатер», «ИнейT», «Гамма». Их стоимость достигает 25- 30% от стоимости ПК. При установке такого устройства необходимо убедиться в достаточности мер защиты, так как в его частотной характеристике возможны провалы. Для этого потребуется привлечение специалистов с соответствующей измерительной аппаратурой.

Предлагается неэнергетический (статистический), метод активной маскировки, являющийся для большинства малых и средних фирм оптимальным способом ЗИ с точки зрения цены/эффективности защиты и простоты реализации.

Метод активной маскировки заключается в изменении вероятностной структуры сигнала, принимаемого приемником злоумышленников, путем излучения специального маскирующего сигнала. Исходной предпосылкой в данном методе является случайный характер электромагнитных излучений ПК.

Для описания этих излучений используется теория марковских случайных процессов. В качестве вероятностных характеристик применяются матрицы вероятностей переходов и вектор абсолютных вероятностей состояний. Сформированный с помощью оригинального алгоритма сигнал излучается в пространство компактным устройством, которое может устанавливаться как на корпусе самого ПК, так и в непосредственной близости от него. Уровень излучаемого этим устройством маскирующего сигнала не превосходит уровня информативных электромагнитных излучений ПК, поэтому согласования установки маскирующего устройства со службой радиоконтроля не требуется. Более того, подобные устройства в отличие от устройств активной энергетической маскировки не создают ощутимых помех для других электронных приборов, находящихся рядом с ними, что также является их неоспоримым преимуществом. Установка и включение устройств активной маскировки, реализующих статистический метод, могут быть произведены без каких-либо трудоемких монтажных работ.

Устройство не требует квалифицированного обслуживания, его надежная работа гарантируется встроенной схемой контроля работоспособности. Следует отметить, что в случаях: доработки устройств ВТ, электромагнитной экранировки помещений и активной энергетической маскировки - показателем защищенности является отношение сигнал/шум, обеспечиваемое на границе минимально допустимой зоны безопасности. Максимально допустимое отношение сигнал/шум рассчитывается в каждом конкретном случае по специальным методикам. При активной радиотехнической маскировке с использованием статистическом метода в качестве показателя, характеризующем защищенность, применяется матрица вероятностей переходов. В случае идеальной защищенности эта матрица будет соответствовать матрице вероятностей переходов шумового сигнала, все элементы которой равны между собой.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Торокин А.А. Инженерно-техническая защита информации – Изд. Гелиос АРВ, 2005
2. Галкин А. П. Оценка необходимости защиты информации предприятия - Вестник ассоциации Русская оценка. 1999. № 1. С. 55-58.
3. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. - М.: Гелиос АРВ, 2004
4. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры. Пер.с англ. – М.: Изд. БИНОМ, 2006.
5. Петраков А.В. Основы практической защиты информации. – М.: СОЛОН-Пресс, 2006
6. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки: Учеб. пособие. М.: Российский гос. гуманит. ун-т, 2002. 309 с