**ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ «ОБРАЗОВАНИЕ»**
**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

---

**А.Б. ИСАЕВ**

# СОВРЕМЕННЫЕ ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**Учебное пособие**

**Москва**
**2008**

*Инновационная образовательная программа*
*Российского университета дружбы народов*

**«Создание комплекса инновационных образовательных программ и формирование инновационной образовательной среды, позволяющих эффективно реализовывать государственные интересы РФ через систему экспорта образовательных услуг»**

Экспертное заключение –

доктор технических наук, профессор *Е.А. Воронин*

**Исаев А.Б.**

Современные технические методы и средства защиты информации: Учеб. пособие. – М.: РУДН, 2008. – 253 с.: ил.

Пособие посвящено изложению основ ряда современных методов и средств защиты информации в различных информационно-измерительных системах от различных видов несанкционированного доступа, включая электромагнитные утечки, технические, радиоэлектронные каналы, описание программных реализаций на основе программных закладок, для реализации утечки информации с использованием компьютерных вирусов и ряда других технических методов. В пособии дано описание адекватных средств защиты от современных методов взлома на основе электрических, электронных и электромеханических устройств и специальных программных средств защиты. Кроме того, значительное место уделено ряду современных криптографических методов защиты (например, компьютерной стенографии). Отметим, что пособие написано в рамках системного подхода к проблеме, основы которого также представлены в пособии.

Для студентов, обучающихся по направлению «Автоматизация и управление», а также аспирантов и научных работников, разрабатывающих эффективные алгоритмы защиты от взлома систем в различных практических условиях эксплуатации информационно-измерительных систем.

***Учебное пособие выполнено в рамках инновационной образовательной программы Российского университета дружбы народов, направление «Комплекс экспортоориентированных инновационных образовательных программ по приоритетным направлениям науки и технологий», и входит в состав учебно-методического комплекса, включающего описание курса, программу и электронный учебник.***

## СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Согласно Федеральному закону от 10.02.95 №24-ФЗ «Об информации, информатизации и защите информации» защите принадлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу.

В наше время стремительного развития новых информационных технологий, всеобщей компьютеризации, постоянно обостряющейся конкуренции различных товаропроизводителей все более изощренными становятся методы взлома систем информационной безопасности. Технические и интеллектуальные методы и средства несанкционированного доступа к информации различной физической природы, различной степени конфиденциальности и секретности, циркулирующей в информационных системах от локального до стратегического уровня, постоянно совершенствуются и становятся изощреннее.

В связи с этим, основной целью пособия «Современные технические методы и средства защиты информации» является выработка навыков у учащихся по формированию у них системного подхода к проблеме анализа и синтеза технических средств защиты информации от несанкционированного доступа. В результате освоения данного курса учащийся должен уметь оперативно и быстро выявить и классифицировать всевозможные каналы утечки информации, циркулирующей в информационной системе (ИС), исполняющей чаще всего функцию управления (ИУС) каким-либо объектом, подверженным угрозе безопасности информации.

Напомним, что под информационной системой мы понимаем взаимосвязанную совокупность средств, методов, персонала,

используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Однако современная концепция безопасности, действующая в рамках эффективного управления любой современной организацией, оперирует в подавляющем большинстве случаев с автоматизированными информационными системами, т.е. с такими комплексами, каждый из которых включает в себя компьютерное и коммуникационное оборудование, программное обеспечение, диагностические средства, информационные ресурсы, а также системный персонал.

К числу побочных целей данного пособия (в рамках вышеупомянутого системного подхода к проблеме синтеза методов и средств защиты информации от несанкционированного доступа) могут быть отнесены следующие вопросы:

1. Умение квалифицированно и оперативно оценить надежность применяемой в данной ситуации системы информационной безопасности;
2. Умение квалифицированно и оперативно выбирать или синтезировать системы информационной информации (СИБ), адекватно регулирующие на возможные в данной ситуации виды умышленных угроз для безопасности информации;
3. Умение квалифицированно и оперативно выбирать или синтезировать нужные в данной конкретной ситуации по обеспечению информационной безопасности технические средства защиты;
4. Умение квалифицированно и оперативно оценить надежность применяемой в данной ситуации системы информационной безопасности.

Напомним, что под безопасностью информационной системы мы понимаем защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов, высокий уровень

противостояния данной информационной системы различным возмущающим воздействиям.

Приведем стандартный перечень видов умышленных угроз безопасности информации:

- пассивные и активные угрозы;
- внутренние и внешние угрозы;
- утечка конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование информационных ресурсов;
- несанкционированный обмен информацией между абонентами;
- отказ от информации;
- нарушение информационного обслуживания;
- незаконное использование привилегий.

Заметим, что кроме пассивных, активных, внешних и внутренних угроз, носящих достаточно общий характер, все остальные приведенные угрозы в основном характерны для безопасности нормального функционирования используемых конкретных информационных систем, например, информационно-вычислительных систем, различных автоматизированных систем управления, систем управления, использующих искусственный интеллект и т.д.

Отметим, что под вышеупомянутыми техническими средствами мы понимаем специальные приборы, сооружения, создающие препятствие несанкционированному доступу к информационным данным. Это могут быть различные средства физического препятствия, сигнальные системы, средства визуального наблюдения, магнитные карты, биологические идентификаторы и т.д. Но, например, криптографические средства защиты

информации можно рассматривать и как технические средства защиты, и как аппаратно-программные.

Изложенные главные и побочные цели курса, стоящие перед специалистами по защите информации, далеко не исчерпывают приведенный выше перечень.

Заметим, что понятие «информационная безопасность» является понятием чрезвычайно широким, всеобъемлющим, нет смысла пытаться выделить одну главную задачу, ибо она будет носить чересчур общий характер, поэтому приведем перечень задач курса, наиболее интересных с нашей точки зрения:

1. Освоение основных теоретических и практических навыков для организации процедуры моделирования макросистем и микросистем, используемых в информационных технологиях управления системами информационной безопасности.

2. Умение квалифицированно и оперативно осуществлять процесс синтеза модели применяемой информационной системы на основе классического и системного подходов, интерпретировать различия моделей путем применения принципиально различных подходов для синтеза этих моделей, находить преимущества системного подхода.

3. Умение квалифицированно и оперативно составлять структурные схемы технических устройств, используемых в данной ситуации и представляющих собой потенциальные объекты взлома.

4. На основании структурных схем применяемых технических устройств выполнять расчеты надежности каждого технического устройства и расчет вероятности взлома применяемой информационной системы. Находить пути уменьшения вероятности взлома системы, в частности, путем модификации структурных схем отдельных технических устройств и модификации структурной схемы всей информационной системы данной задачи.

Данное пособие полностью соответствует курсу «Современные технические методы и средства защиты информации».

Курс предназначен для реализации программ «Обеспечение информационной безопасности автоматизированных систем», «Интеллектуальные системы», «Разработка и применение нанотехнологий на базе проектирования и управления системами качества промышленных предприятий». В свою очередь вышеупомянутый курс может рассматриваться как обязательный для направления «Автоматизация и управление», для остальных он может рассматриваться факультативно.

# Тема 1. Основные понятия теории защиты информации в измерительных системах и информационных технологиях управления объектом

Непрерывно растущий уровень информатизации современного общества, процессы ускоренного развития компьютерных технологий, телекоммуникационных систем приводят к быстрому накоплению информации в системах, имеющих косвенное отношение или напрямую связанных с процедурами управления различными процессами (от социальных до производственно-технических), идущими непрерывно в разных слоях общества. Такие системы, как известно, называются информационно-управляющими системами (ИУС). Напомним, что система – это целенаправленная совокупность взаимосвязанных элементов любой природы, а информационная система управления (ИСУ) – совокупность информации, производственно-технических и математических методов и моделей, технических, программных, других технологических средств и специалистов, предназначенная для обработки информации и принятия управленческих решений. Используя всевозможную информацию, получаемую в ходе функционирования, например, автоматизированной информационной системы, руководствующий орган может спланировать, сбалансировать ресурсы фирмы (материальные, финансовые, кадровые), оценить результаты предыдущих управленческих решений и на этой основе принять новые, более оптимальные управленческие решения.[1, 2, 4, 5]

Напомним, что основной составляющей частью любой автоматизированной информационной системы (АИС) является информационная технология (ИТ), представляющая собой процесс, использующий совокупность методов и средств реализации операций сбора, регистрации, передачи, накопления, обработки информации на базе

программно-аппаратного обеспечения для решения различных управленческих задач какого-либо объекта.

Заметим, что автоматизированные информационные системы (АИС) для информационной технологии – это основная среда, составляющими элементами которой являются средства и способы преобразования данных. Всякая ИТ представляет собой процесс, состоящий из четко регламентированных правил выполнения операций над информацией, циркулирующей в ИС [2, 6].

Хорошо известно, что среди многих требований, предъявляемых к любой ИСУ, одним из важнейших, а в некоторых ситуациях самым главным требованием, является безопасность ИСУ, степень ее защищенности, устойчивости как к непреднамеренным, так и преднамеренным воздействиям на систему, снижающим безопасность ИСУ. Эти воздействия провоцируются появлением все новых и новых информационных технологий, в результате чего образуются и новые каналы утечки (электромагнитные, параметрические и др.) информации, циркулирующей в системе (т.е. кража информации), а также новые виды каналов несанкционированного доступа к информации.

Из сказанного уже ясно, что создание всякой ИСУ (а также ИТ) представляет собой сложный, многогранный процесс проектирования, на стадиях которого необходимо проведение тщательного мониторинга всей предшествующей деятельности старой ИСУ и анализа ошибок и некорректностей процесса ее функционирования в старой информационно-технической среде. В процессе проектирования должны быть выявлены (наряду со старыми) и новые существенные характеристики создаваемой ИСУ, возникшие во время ее эксплуатации.

Вкратце рассмотрим структуру ИС и ИСУ, а также автоматизированных информационных систем (АИС), их основные разновидности. Начнем с некоторых понятий из области классификации

информационных систем и информационных технологий, например с проблемы классификации автоматизированных информационных систем.

Напомним, что система – это набор взаимосвязанных компонентов, функционирующих совместно для достижения определенной цели. Информационная система (ИС) – взаимосвязанная совокупность средств, методов, персонала, используемая для хранения, обработки и выдачи информации в интересах достижения поставленной цели. Автоматизированная информационная система (АИС) – это комплекс, включающий компьютерное и коммуникационное оборудование, программное обеспечение, лингвистические средства, информационные ресурсы и системный персонал. Система обеспечивает удовлетворение информационных потребностей пользователей с целью принятия управленческих решений. Структура АИС представлена в таблице 1.1.

Таблица 1.1.Структурные элементы АИС

Информационные технологии (ИТ) – инфраструктура, обеспечивающая реализацию информационных процессов, то есть процессов сбора, обработки, накопления, хранения, поиска и распространения информации. ИТ предназначены для снижения трудоемкости процессов использования информационных ресурсов, повышения их надежности и оперативности.

Функциональные подсистемы и приложения – специализированные программы, предназначенные обеспечить обработку и анализ информации для целей подготовки документов, принятия решений в конкретной функциональной области на базе ИТ.

Управление ИС – компонент, который обеспечивает оптимальное взаимодействие ИТ, функциональных подсистем и связанных с ними специалистов и развитие ИТ их в течение жизненного цикла ИС.

Каждая автоматизированная информационная система ориентирована на ту или иную предметную область. Под предметной областью понимают область проблем, знаний, человеческой деятельности, имеющую определенную специфику и круг фигурирующих в ней предметов.

При этом каждая автоматизированная система ориентирована на выполнение определенных функций в соответствующей ей области применения.

Существует большое разнообразие автоматизированных ИС, отличающихся своей ориентацией на уровень управления, сферу функционирования экономического объекта, на тот или иной характер процесса управления, вид поддерживаемых информационных ресурсов, архитектуру, способы доступа к системе и др.

По целевой функции ИС можно условно разделить на следующие основные категории.

Особую важность в общественной жизни имеют экономические информационные системы (ЭИС), связанные с предоставлением и обработкой информации для разных уровней управления экономическими объектами. Эта информация позволяет наиболее полно осуществлять функции учета, контроля, анализа, планирования и регулирования с целью принятия эффективных управленческих решений.

По уровню в системе государственного управления экономические информационные системы делятся на ИС федерального, регионального и муниципального значения.

В зависимости от области функционирования экономических объектов можно выделить ЭИС промышленно−производственной сферы и непромышленной сферы.

Системы поддержки принятия решений (СППР) − аналитические ИС, ИС руководителя − системы, обеспечивающие возможности изучения состояния, прогнозирования, развития и оценки возможных вариантов поведения на основе анализа данных, которые отражают результаты деятельности компании на протяжении определенного времени. В таких системах применяются современные технологии баз данных, OLAP (Online Analytical Processing − оперативная аналитическая обработка данных), ХД (хранилище данных), глубинный анализ и визуализация данных.

Информационно-вычислительные системы используются в научных исследованиях и разработках для проведения сложных и объемных расчетов, в качестве подсистем автоматизированных систем управления и СППР в том случае, если выработка управленческих решений должна опираться на сложные вычисления. К ним относятся информационно-расчетные системы, САПР (системы автоматизированного проектирования), имитационные стенды контроля.

Таблица 1.2. Виды автоматизированных ИС


Информационно-справочные системы предназначены для сбора, хранения, поиска и выдачи потребителям информации справочного характера; используются во всех сферах профессиональной деятельности (Гарант, Кодекс, Референт, системы семейства КонсультантПлюс: КонсультантБухгалтера, КорреспонденцияСчетов, НалогиБухучет,

КонсультантПлюс: Версия Проф, Деловые Бумаги, КонсультантПлюс: Эксперт и др.).

Основными видами ИС образования являются автоматизированные системы дистанционного обучения, системы обеспечения деловых игр, тренажеры и тренажерные комплексы. Они предназначены для автоматизации подготовки специалистов и обеспечивают обучение, управление процессом обучения и оценку его результатов.

Эффективность применения ИС для управления экономическими объектами (предприятиями, банками, торговыми организациями, государственными учреждениями и т.д.) зависит от широты охвата и интегрированности на их основе функций управления, от способности оперативно подготавливать управленческие решения, адаптироваться к изменениям внешней среды и информационных потребностей пользователей.

***Информационные технологии, их развитие и классификация***

Создание и функционирование ИС в управлении экономикой неразрывно связаны с развитием информационных технологий − главной составляющей информационных систем.

Информационные технологии (ИТ) − это комплекс методов переработки разрозненных исходных данных в надежную и оперативную информацию для принятия решений с помощью аппаратных и программных средств с целью достижения оптимальных параметров объекта управления.

Появление в конце 1950-х годов ЭВМ и стремительное совершенствование их эксплуатационных возможностей создало реальные предпосылки для автоматизации управленческого труда, формирования рынка информационных продуктов и услуг. Развитие ИТ шло параллельно

с появлением новых видов технических средств обработки и передачи информации, совершенствованием организационных форм использования компьютеров, насыщением инфраструктуры новыми средствами связи.

В условиях рыночных отношений все возрастающий спрос на информацию и информационные услуги привел к тому, что технология обработки информации стала ориентироваться на применение самого широкого спектра технических средств и прежде всего компьютеров и средств коммуникации. На их основе создавались компьютерные системы и сети различных конфигураций с целью не только накопления, хранения, переработки информации, но и максимального приближения терминальных устройств к рабочему месту специалиста или принимающего решения руководителя. Это явилось достижением многолетнего развития ИТ.

ИТ в настоящее время можно классифицировать по ряду признаков, в частности по способам построения компьютерной сети, виду технологии обработки информации, типу пользовательского интерфейса, области управления социально-экономическим процессом.

Повышение требований к оперативности информационного обмена и управления, а следовательно, к срочности обработки информации, привело к созданию не только локальных, но и многоуровневых и распределенных систем организационного управления объектами, какими являются, например, банковские, налоговые, снабженческие, статистические и другие службы. За счет усложнения программных средств управления базами данных повышается скорость, обеспечиваются защита и достоверность информации при выполнении экономических расчетов и выработке управленческих решений.

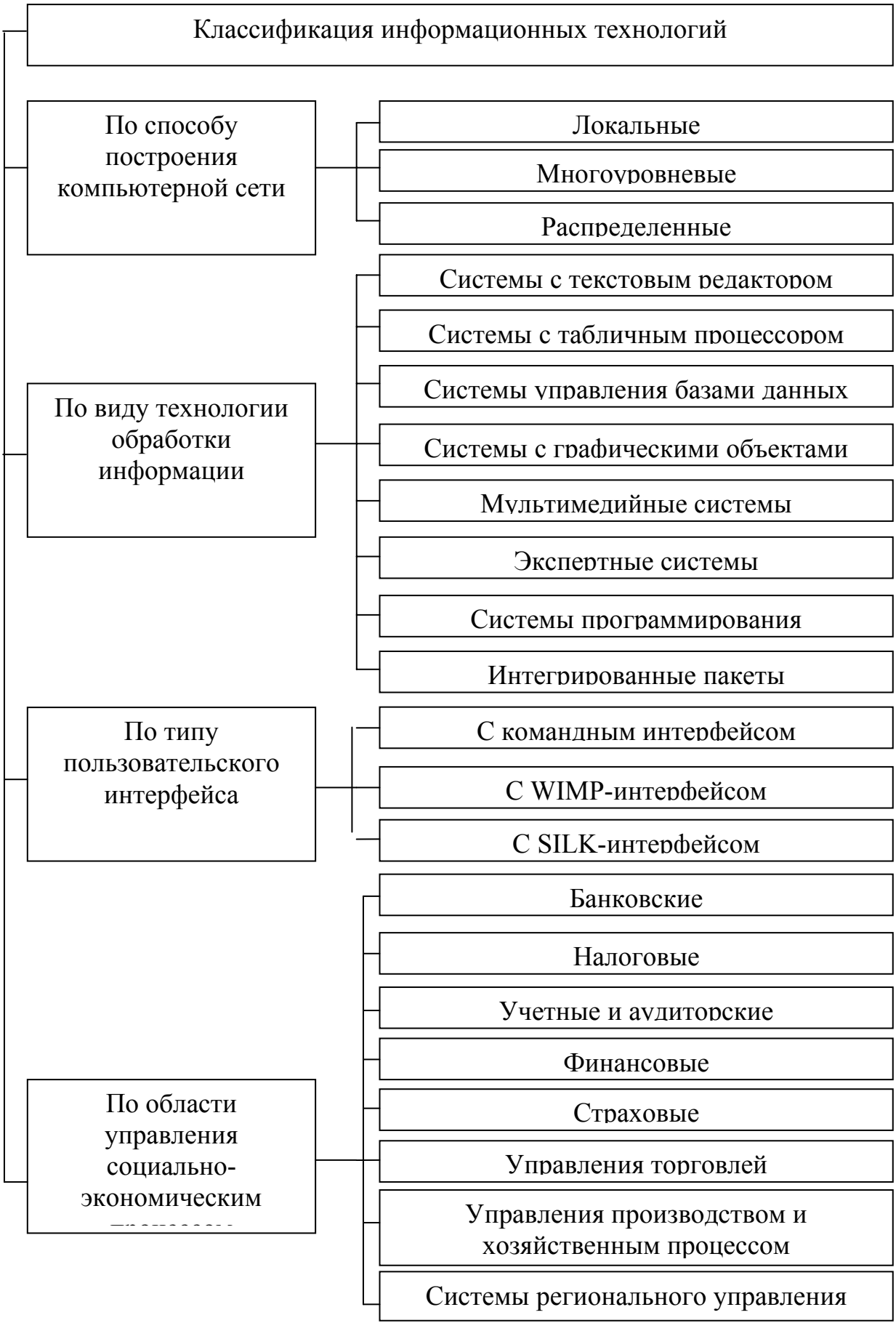
В многоуровневых и распределенных компьютерных информационных системах организационного управления одинаково успешно могут быть решены как проблемы оперативной работы с информацией, так

и проблемы анализа экономических ситуаций при выработке и принятии управленческих решений. В частности, создаваемые автоматизированные рабочие места специалистов предоставляют возможность пользователям работать в диалоговом режиме, оперативно решать текущие задачи, удобно вводить данные с терминала, вести их визуальный контроль, вызывать нужную информацию для обработки, определять достоверность результатной информации и выводить ее на экран, печатающее устройство или передавать по каналам связи.

По виду технологии обработки информации ИТ рассматриваются в программном аспекте и включают: текстовую обработку, электронные таблицы, автоматизированные банки данных, обработку графической информации, мультимедийные и другие системы.

Перспективным направлением развития компьютерной технологии является создание программных средств для вывода высококачественного звука и видеоизображения. Технология формирования видеоизображения получила название компьютерной графики. Компьютерная графика – это создание, хранение и обработка моделей объектов и их изображений с помощью компьютера. Данная технология проникла в область экономического анализа, моделирования различного рода конструкций, она незаменима в производстве, проникает в рекламную деятельность, делает занимательным досуг. Формируемые и обрабатываемые с помощью цифрового процессора изображения могут быть демонстрационными и анимационными.

Таблица 1.3. Классификация автоматизированных ИТ



К первой группе, как правило, относят коммерческую (деловую) и иллюстративную графику, ко второй – инженерную и научную, а также связанную с рекламой, искусством, играми, когда выводятся не только одиночные изображения, но и последовательность кадров в виде фильма (интерактивный вариант). Интерактивная машинная графика является одним из наиболее прогрессивных направлений среди новых информационных технологий. Это направление переживает бурное развитие в области появления новых графических станций и в области специализированных программных средств, позволяющих создавать реалистические объемные движущиеся изображения, сравнимые по качеству с кадрами видеофильма.

По типу пользовательского интерфейса можно рассматривать ИТ с точки зрения возможностей доступа пользователя к информационным и вычислительным ресурсам (под интерфейсом понимают определенные стандартом правила взаимодействия пользователей, устройств, программ).

С помощью командного интерфейса пользователь подает команды компьютеру, а компьютер их выполняет и выдает результат пользователю. Командный интерфейс реализован в виде пакетной технологии и технологии командной строки.

Пакетная ИТ исключает возможность пользователя влиять на обработку информации пока она производится в автоматическом режиме. Это объясняется организацией обработки, которая основана на выполнении программно-заданной последовательности операций над заранее накопленными в системе и объединенными в пакет данными.

Интерфейс сетевой ИТ предоставляет пользователю средства те-ледоступа к территориально распределенным информационным и вычислительным ресурсам благодаря развитым средствам связи, что делает такие ИТ широко используемыми и многофункциональными.

Характерная особенность WIMP-интерфейса (Window – окно, Image – образ, Menu – меню, Pointer – указатель) – ведение диалога с пользователем с помощью графических образов – меню, окон, других элементов. Примером программ с графическим интерфейсом является операционная система MS Windows.

Существует, но пока не широко используется SILK-интерфейс (Speech – речь, Image – образ, Language – язык, Knowledge – знание). Он наиболее приближен к обычной, человеческой форме общения. В рамках этого интерфейса идет «разговор» человека и компьютера. Компьютер, анализируя человеческую речь, находит для себя команды, выбирая в ней ключевые фразы. Результат выполнения команд он также преобразует в понятную человеку форму. Разновидностями интерфейсов являются интерфейсы на основе речевой (команды подаются голосом путем произнесения специальных зарезервированных слов – команд) и биометрической технологий (для управления компьютером используется выражение лица человека, направление его взгляда, размер зрачка, рисунок радужной оболочки глаз, отпечатки пальцев и другая уникальная информация). Изображения считываются с цифровой видеокамеры, а затем с помощью специальных программ распознавания образов из этого изображения выделяются команды.

Конвергенция компьютерной и телекоммуникационной технологий создает возможности для повышения производительности. Примерами могут служить создание сетей банковских автоматов, новый виток интереса к видеоконференциям, дизайн и производство с помощью компьютера, работа из дома, автоматическое формирование заказов на товары и услуги, электронные публикации и финансовые операции.

Информационно-телекоммуникационные технологии (ИТТ) в современных организациях играют чрезвычайно важную роль. Они обеспечивают выполнение самых разных задач:

• доступ к внешним и внутренним базам данных в режиме прямого доступа для получения исследовательской, научной, рабочей и другой информации;

• использование экспертных систем для диагностики, управления и принятия решений;

• передачу данных по электронной почте;

• формирование электронных бюллетеней для деловой и технической информации общего пользования;

• проведение видеоконференций;

• создание систем хранения и поиска информации;

• компьютерный дизайн;

• компьютерное обучение;

• индексацию и хранение документов.

Очень интенсивно на корпоративном уровне используются ингранет-технологии, существенно упрощающие работу с большими массивами информации, их структуризацию, поиск и деловое применение. Кредитные организации используют ИТТ для определения финансового риска при инвестициях и операциях с ценными бумагами.

Роль ИТТ в традиционных отраслях промышленности и сфере услуг (транспортные перевозки, туризм, медицинское обслуживание, издательство, страхование, розничная торговля и т.п.) столь велика, что без их использования выдержать острую конкуренцию практически невозможно.

Зарубежные специалисты выделяют пять основных тенденций развития информационных технологий. Кратко охарактеризуем их.

1. Первая тенденция связана с изменением характеристик информационного продукта, который все больше превращается в гибрид между результатом расчетно-аналитической работы и специфической услугой, предоставляемой индивидуальному пользователю ПК.

2. Отмечаются способность к параллельному взаимодействию логических элементов ИТ, совмещение всех типов информации (текста, образов, цифр, звуков) с ориентацией на одновременное восприятие человеком посредством органов чувств.

3. Прогнозируется ликвидация всех промежуточных звеньев на пути от источника информации к ее потребителю, например, становится возможным непосредственное общение автора и читателя, продавца и покупателя, певца и слушателя, ученых между собой, преподавателя и обучающегося, специалистов на предприятии через систему видеоконференций, электронный киоск, электронную почту.

4. В качестве ведущей называется тенденция к глобализации информационных технологий в результате использования спутниковой связи и всемирной сети Интернет, благодаря чему люди могут общаться между собой и с общей базой данных, находясь в любой точке планеты.

5. Конвергенция рассматривается как последняя черта современного процесса развития ИТ, которая заключается в стирании различий между сферами материального производства и информационного бизнеса, в максимальной диверсификации видов деятельности фирм и корпораций, взаимопроникновении различных отраслей промышленности, финансового сектора и сферы услуг.

Перейдем к изложению некоторых основных понятий систем информационной безопасности (СИБ). Итак, развитие новых информационных технологий и всеобщая компьютеризация приводят к тому, что информационная безопасность (как свойство ИСУ) не только становится из желательной обязательной, она стала еще и одной из важнейших характеристик ИС. Существует довольно обширный класс систем обработки информации, при разработке которых фактор безопасности играет первостепенную роль (например, банковские информационные системы). Приведем важнейшие характеристики ИС,

связанные с ее безопасностью, или безопасностью функционирования системы.

Под безопасностью ИС понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Если исходить из классического рассмотрения кибернетической модели любой управляемой системы, возмущающие воздействия на нее могут носить случайный характер. Поэтому среди угроз безопасности информации следует выделять как один из видов угрозы случайные, или непреднамеренные. Их источниками могут быть выход из строя аппаратных средств, неправильные действия работников ИС или ее пользователей, непреднамеренные ошибки в программном обеспечении и т.д. Такие угрозы тоже следует держать во внимании, так как ущерб от них может быть значительным. Однако в данной главе наибольшее внимание уделяется угрозам умышленным, которые, в отличие от случайных, преследуют цель нанесения ущерба управляемой системе или пользователям. Это делается нередко ради получения личной выгоды.

Многочисленные публикации последних лет показывают, что злоупотребления информацией, циркулирующей в ИС или передаваемой по каналам связи, совершенствовались не менее интенсивно, чем меры защиты от них.

Сегодня можно утверждать, что рождается новая современная технология – технология защиты информации в компьютерных

информационных системах и в сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз ИС и ИТ.

Большинство задач инженерно-технической защиты – это противоборство органов и специалистов по безопасности информации, с одной стороны, и злоумышленников, с другой стороны. Под злоумышленниками, «взломщиками» понимаются, говоря юридическим языком, физические лица, пытающиеся незаконным путем, подчас нестандартным образом, добыть, изменить или уничтожить информацию законных владельцев, пользователей.

Отсюда следует ожидать, что задачи защиты (от взлома) инженерно-технической информации как задачи, возникающие вследствие деятельности людей, должны носить характер неопределенности, в них, как правило, на начальной стадии отсутствует точная математическая постановка, а само решение может быть мало достоверным, т.к. зависит от большого количества факторов разнообразной природы. Такие задачи с неопределенной информацией относятся к классу слабоформализуемых задач, для их решения используется системный поход.

К числу причин применения системного подхода отнесем такие, как:

а) наличие большого числа факторов, влияющих на точность решения задачи;

б) отсутствие достоверных количественных данных об этих факторах;

в) отсутствие формальных математических алгоритмов получения оптимальных решений слабо формализованных задач по совокупности неточных исходных данных.

Слабоформализуемые задачи часто встречаются на практике. Например, назначение первоначальной продажной цены на товары и

покупка товара за цену, «устраивающую» нас, поэтому они, как правило, решаются эвристически. Однако при значительном числе факторов (больше десяти), точность эвристических крайне низка. К числу таких слабо формализуемых задач относятся задачи инженерно-технической защиты.

Вообще говоря, успешное решение любых инженерно-технических задач проводится на основе моделей исследуемых объектов или процессов. Вспомним, что модель (в частности, математическая) это объект-заместитель объекта-оригинала, причем в модели стремятся добиться сходства, в лучшем случае, нескольких характерных признаков оригинала с признаками модели.

Однако наиболее универсальной моделью объекта является представление этого объекта некоторой системой (см. определение выше) Отсюда возникает системный подход – наиболее высокий уровень описания объекта. Этот подход означает, что каждая система является интегрированным целым даже тогда, когда она состоит из отдельных разобщенных подсистем. В основе системного подхода лежит рассмотрение системы, как интегрированного целого, причем это рассмотрение при разработке начинается с главного – формулировки цели функционирования системы, формализуемой в виде целевой функции системы (математической модели).

Отметим несколько характерных признаков системного подхода:

а) совокупность сил и средств, обеспечивающих решение задачи, представляется в виде модели, называемой системой;
б) система описывает совокупность параметров;
в) любая система рассматривается как подсистема более сложной системы, влияющей на структуру исследуемой системы;
г) любая система имеет иерархическую структуру, элементами и связями которой нельзя пренебрегать без достаточных технологий;

д) при анализе системы необходим абсолютно полный учет;

е) свойства системы превышают сумму свойств ее элементов, за счет качественно новых свойств, так называемых системных свойств, возникающих в силу того, что элементы системы вступают в сложное взаимодействие друг с другом, и целевая функция системы определяет характер этого взаимодействия.

Итак, важнейшей чертой системного подхода является декларирование факта, что у совокупности элементов, объединенных в систему с целевой функцией возникают новые системные свойства (признаки), ранее отсутствующие у отдельных элементов системы.

Эффективность системного подхода на практике зависит от умения специалиста выявлять и объективно анализировать все многообразие факторов и связей любого сложного объекта исследования, каковым является конкретный объект защиты.

## Тема 2. Виды умышленных угроз безопасности информации.

Развитие новых информационных технологий, глобальная компьютеризация, приводят к тому, что информационная безопасность предприятия, высокий уровень защищенности информации находятся в прямой зависимости от уровня затрат на нее, что, в свою очередь, ведет к неизбежному повышению затрат на незаконное добывание информации злоумышленниками. В данном разделе речь пойдет о классификации видов умышленных угроз безопасности информации, но естественно допустить, что всякие угрозы имеют свои источники, выявлением которых должна заниматься служба безопасности предприятия.

На данную проблему можно смотреть с государственных позиций или с позиций общенациональной безопасности, но можно с более частных, более индивидуальных, например, с позиции владельца крупного предприятия.

С позиции государственности источниками угроз информации могут быть:

- органы зарубежной разведки;
- органы разведки коммерческих структур другого государства;
- криминальные структуры другого государства, заинтересованные, например, в организации новых наркотрафиков и масштабном изготовлении наркотических веществ (интерес таких структур лежит на стыке фармакологической и химической промышленности).

С другой стороны, такие способы взлома, как «троянский конь», «логические бомбы», «червь» и др., скорее будут применяться не органами разведки другого государства, а при «промышленном шпионаже», осуществляемом предприятиями, с которыми на внутренних рамках конкурирует данное предприятие.

Ниже нами будут рассмотрены виды угроз, типичные в основном для внутригосударственного промышленного шпионажа со стороны конкурентов, органов разведки других государств. Будет полезным привести самые банальные способы взлома, такие как:

а) устройство пожара;

б) порча системы водоснабжения;

в) сознательная порча или вывод из строя ценного инженерно-технологического оборудования и другие грубые способы проникновения и взлома систем.

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов ИС, не отказываясь при этом от влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д. [4, 6].

Активные угрозы имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, разрушение ПО компьютеров, нарушение работы линий связи и т.д. Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.

Умышленные угрозы подразделяются также на внутренние (возникающие внутри управляемой организации) и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, широкое распространение получил промышленный шпионаж – это наносящие ущерб владельцу коммерческой тайны незаконные сбор,

присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

- утечка конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование информационных ресурсов;
- несанкционированный обмен информацией между абонентами;
- отказ от информации;
- нарушение информационного обслуживания;
- незаконное использование привилегий.

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- маскировка под запросы системы;
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- злоумышленный вывод из строя механизмов защиты;
- расшифровок специальными программами зашифрованной информации;
- информационные инфекции.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Существует и постоянно разрабатывается огромное множество вредоносных программ, цель которых – порча информации в БД и ПО

компьютеров. Большое число разновидностей этих программ не позволяет разработать постоянные и надежные средства защиты против них.

Мы будем рассматривать в основном вредоносные вирусные программы – логические бомбы, «троянский конь», «червь» и т.д. Их подробное рассмотрение будет произведено в разделе 16.

В заключение обратим внимание на важнейшую роль алгоритмов ввода имени и пароля пользователя, а также на еще один, редко упоминаемый вид угроз взлома – «люки».

Итак, при умышленном проникновении в систему взломщик не имеет санкционированных параметров для входа в систему, применяя самые различные способы взлома, описанные выше. Если объектом взлома является пароль другого пользователя, то способ взлома может заключаться в переборе возможных паролей или же путем использования ошибок программы входа.

Таким образом, основную нагрузку на защиту системы от взлома несет программа входа, поэтому алгоритмы ввода имени и пароля, алгоритмы шифрования, не должны содержать ошибок. Противостоять взлому системы может введение ограничений на число попыток неправильного ввода пароля. Кроме того, администратор безопасности должен постоянно контролировать активных пользователей системы: их имена, характер работы, время ввода и вывода и многие другие характерные признаки пользователей.

Кроме того, наличие так называемых «люков» – это условие, реализующее многие виды угроз для ИС. Люк – скрытая, недокументированная точка входа в программный модуль, находящийся в составе ПО информационной системы (ИС) и информационной технологии (ИТ). Люк вставляется в программном этапе отладки для облегчения работы: данный модуль можно будет вызывать в разных местах, что позволит отлаживать отдельные части программы независимо.

Наличие люка позволяет вызывать программу нестандартным образом, что может серьезно сказаться на состоянии системы защиты, образуя в ней бреши для несанкционированного доступа. Люки оказываются в программе по разным причинам – их забыли убрать, оставив для дальнейшей отладки, или же, например, для реализации тайного доступа к программе после ее установки.

Однако большая опасность люков компенсируется высокой сложностью их обнаружения. Защита от люков одна – не допускать их появления в программе, а при приемке программных продуктов от производителя необходим внимательный анализ исходных текстов программ с целью обнаружения люков.

К сожалению, опыт показывает, что во всех странах убытки от злонамеренных действий непрерывно возрастают, причем это напрямую связано не только с недоступностью средств безопасности как таковых, но с отсутствием взаимосвязи между ними. Другими словами, системный подход полностью не реализуется (о системном подходе смотри выше, тема № 1).

В заключении отметим, что подробное рассмотрение технических каналов утечки – акустических, электрических, лазерных, электромагнитных, радиопрокладки и ряда других, осуществлено в разделе 5 (см. ниже).

## Тема 3. Методы и технические средства построения технических систем информационной безопасности, их структура

***Оценка безопасности ИС***

В условиях использования АИТ под безопасностью понимается состояние защищенности ИС от внутренних и внешних угроз.

Показатель защищенности ИС – характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности.

Для оценки реального состояния безопасности ИС могут применяться различные критерии. Анализ отечественного и зарубежного опыта показал определенную общность подхода к определению состояния безопасности ИС в разных странах. Для предоставления пользователю возможности оценки вводится некоторая система показателей и задается иерархия классов безопасности. Каждому классу соответствует определенная совокупность обязательных функций. Степень реализации выбранных критериев показывает текущее состояние безопасности. Последующие действия сводятся к сравнению реальных угроз с реальным состоянием безопасности [3, 6].

Если реальное состояние перекрывает угрозы в полной мере, система безопасности считается надежной и не требует дополнительных мер. Такую систему можно отнести к классу систем с полным перекрытием угроз и каналов утечки информации. В противном случае система безопасности нуждается в дополнительных мерах защиты.

Политика безопасности – это набор законов, правил в сочетании с практическим опытом, на основе которого строится управление, защита и распределение конфиденциальной информации.

Анализ классов безопасности показывает, что чем он выше, тем более жесткие требования предъявляются к системе.

Руководящие документы в области защиты информации разработаны Государственной технической комиссией при Президенте Российской Федерации. Требования этих документов обязательны для исполнения только организациями государственного сектора либо коммерческими организациями, которые обрабатывают информацию, содержащую государственную тайну. Для остальных коммерческих структур документы носят рекомендательный характер.

### *Методы и средства построения систем информационной безопасности (СИБ). Структура СИБ*

Создание систем информационной безопасности в ИС и ИТ основывается на следующих принципах (см. гл. 2): системный подход, принцип непрерывного развития системы, разделение и минимизация полномочий, полнота контроля и регистрация попыток, обеспечение надежности системы защиты, обеспечение контроля за функционированием системы защиты, обеспечение всевозможных средств борьбы с вредоносными программами, обеспечение экономической целесообразности.

При рассмотрении структуры СИБ возможен традиционный подход – выделение обеспечивающих подсистем. Система информационной безопасности, как и любая ИС, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет способна выполнить свою целевую функцию. С учетом этого СИБ должна иметь следующие виды обеспечения: правовое, организационное, информационное, техническое (аппаратное), программное, математическое, лингвистическое, нормативно-методическое.

Нормативно-методическое обеспечение может быть слито с правовым, куда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации; различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований соблюдения конфиденциальности.

Следует отметить, что из всех мер защиты в настоящее время ведущую роль играют организационные мероприятия. Поэтому следует выделить вопрос организации службы безопасности. Реализация политики безопасности требует настройки средств защиты, управления системой защиты и осуществления контроля функционирования ИС. Как правило, задачи управления и контроля решаются административной группой, состав и размер которой зависят от конкретных условий. Очень часто в эту группу входят администратор безопасности, менеджер безопасности и операторы.

Обеспечение и контроль безопасности представляют собой комбинацию технических и административных мер. По данным зарубежных источников, у сотрудников административной группы обычно 1/3 времени занимает техническая работа и около 2/3 - административная (разработка документов, связанных с защитой ИС, процедуры проверки системы защиты и т.д.). Разумное сочетание этих мер способствует уменьшению вероятности нарушений политики безопасности.

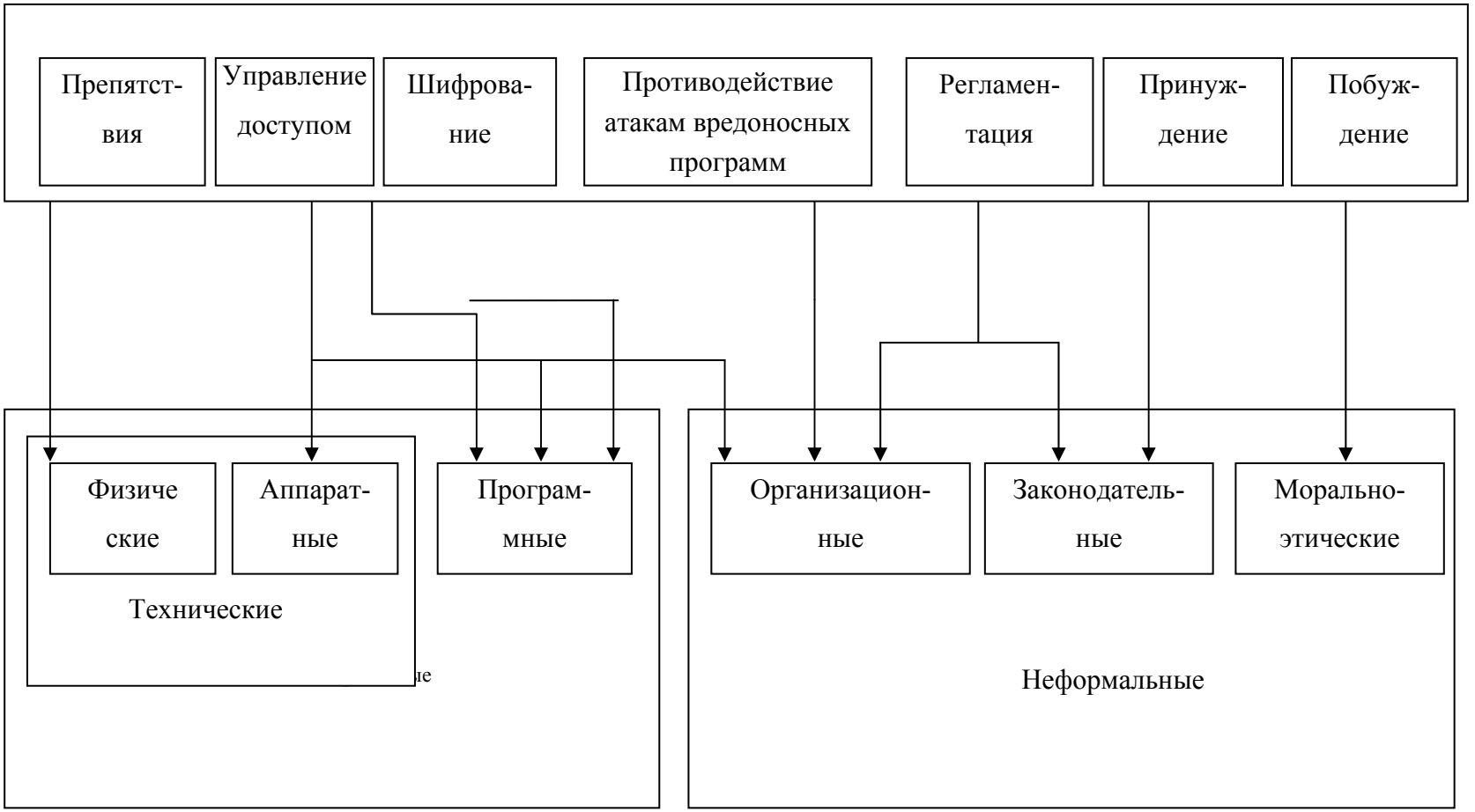
Административную группу иногда называют группой информационной безопасности. Эта группа может быть организационно слита с подразделением, обеспечивающим внутримашинное информационное обеспечение, т.е. с администратором БнД. Но чаще она обособлена от всех отделов или групп, занимающихся управлением самой ИС, программированием и другими относящимися к системе задачами, во избежание возможного столкновения интересов.

Нормативы и стандарты по защите информации накладывают требования на построение ряда компонентов, которые традиционно входят в обеспечивающие подсистемы самих информанионных систем, т.е. можно говорить о наличии тенденции к слиянию обеспечивающих подсистем ИС и СИБ.

Примером может служить использование операционных систем – основы системного ПО ИС. В разных странах выполнено множество исследований, в которых анализируются и классифицируются изъяны защиты ИС. Выявлено, что основные недостатки защиты ИС сосредоточены в операционных системах (ОС). Использование защищенных ОС является одним из важнейших условий построения современных ИС. Особенно важны требования к ОС, ориентированным на работу с локальными и глобальными сетями. Развитие Интернета оказало особенно сильное влияние на разработку защищенных ОС. Развитие сетевых технологий привело к появлению большого числа сетевых компонентов (СК). Системы, прошедшие сертификацию без учета требований к сетевому программному обеспечению, в настоящее время часто используются в сетевом окружении и даже подключаются к Интернету. Это приводит к появлению изъянов, не обнаруженных при сертификации защищенных вычислительных систем, что требует непрерывной доработки ОС.

Методы и средства обеспечения безопасности информации в АИС в обобщенном и упрощенном виде отражает схема, представленная в таблице 3.1.

Таблица 3.1. Методы и средства обеспечения безопасности информации






38

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Шифрование – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ – комплекс разнообразных мер организационного характера и по использованию антивирусных программ [3; 8].

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

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

Побуждение – такой метод защиты, который побуждает пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Программные средства – специализированные программы и программные комплексы, предназначенные для защиты информации в ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем руководителя организации.

Законодательные средства защиты определяются законодательными актами страны, которые регламентируются правилами пользования, обработки и передачи информации ограниченного доступа и устанавливают меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, формируются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются.

## Тема 4. Криптографические методы защиты информации

### *Криптографческие методы защиты информации*

Сущность криптографических методов заключается в следующем. Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым преобразуется в шифрограмму, т.е. в закрытый текст или графическое изображение документа. В таком виде сообщение и передается по каналу связи, пусть даже и незащищенному. Санкционированный пользователь после получения сообщения дешифрует его (т.е. раскроет) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям. Таким образом, даже в случае перехвата сообщения взломщиком текст сообщения становится недоступным для него.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (последовательностью бит), обычно называемым шифрующим ключом [1, 2, 5].

Каждый используемый ключ может производить различные шифрованные сообщения, определяемые только этим ключом. Для большинства систем закрытия схема генератора ключа может представлять собой набор инструкций и команд либо узел аппаратуры, либо компьютерную программу, либо все вместе взятое, но в любом случае процесс шифрования (дешифрования) определяется только этим специальным ключом. Чтобы обмен зашифрованными данными проходил успешно как отправителю, так и получателю необходимо знать правильную ключевую установку и хранить ее в тайне.

Стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации принятой информации.

Перейдем к изложению основных понятий, терминов современной криптографии.

***Шифрование***

Шифрование – это способ изменения сообщения или другого документа, обеспечивающий искажение (сокрытие) его содержания. Кодирование – это преобразование обычного, понятного, текста в код. При этом подразумевается, что существует взаимно однозначное соответствие между символами текста (данных, чисел, слов) и символьного кода – в этом принципиальное отличие кодирования от шифрования. Часто кодирование и шифрование считают одним и тем же, забывая о том, что для восстановления закодированного сообщения, достаточно знать правило подстановки (замены). Для восстановления же зашифрованного сообщения, помимо знания правил шифрования, требуется и ключ к шифру. Ключ понимается нами как конкретное секретное состояние параметров алгоритмов шифрования и дешифрования. Знание ключа дает возможность прочтения секретного сообщения. Впрочем, как вы увидите ниже, далеко не всегда незнание ключа гарантирует то, что сообщение не сможет прочесть посторонний человек. Шифровать можно не только текст, но и различные компьютерные файлы – от файлов баз данных и текстовых процессоров до файлов изображений.

Идея шифрования состоит в предотвращении просмотра истинного содержания сообщения (текста, файла и т.п.) теми, у кого нет средств его

дешифрования. А прочесть файл сможет лишь тот, кто сумеет его дешифровать [6].

Со средних веков и до наших дней необходимость шифрования военных, дипломатических и государственных документов стимулировало развитие криптографии. Сегодня потребность в средствах, обеспечивающих безопасность обмена информацией, многократно возросла.

### *Основные понятия и определения криптографии*

Перечислим основные понятия и определения криптографии.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст-упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных ИС, можно привести следующие:

- алфавит $Z_{33}$ – 32 буквы русского алфавита и пробел;
- алфавит $Z_{256}$ – символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит – $Z_2 = \{0,1\}$;
- восьмиричный алфавит или шестнадцатиричный алфавит;

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T-преобразований открытого текста, члены этого семейства индексируются, или обозначаются символом k; параметр k является ключом.

Пространство ключей К – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на симметричные и с открытым ключом (или асимметричные).

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины «распределение ключей» и «управление ключами» относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Преобразование $T_k$ определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте и длина шифрованного текста должна быть равной длине исходного текста;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

### *Симметричные и асимметричные криптосистемы*

Рассмотрим вкратце концепцию симметричных и асимметричных криптосистем. Оставаясь в рамках симметричной системы, необходимо иметь надежный канал связи для передачи секретного ключа. Но такой канал не всегда бывает доступен, и потому американские математики Диффи, Хеллман и Меркле разработали в 1976 г. концепцию открытого ключа и асимметричного шифрования.

В таких криптосистемах общедоступным является только ключ для процесса шифрования, а процедура дешифрования известна лишь обладателю секретного ключа. В асимметричных системах должно удовлетворяться следующее требование: нет такого алгоритма (или он пока неизвестен), который бы из криптотекста и открытого ключа выводил исходный текст.

### *Основные современные методы шифрования*

Алгоритмы замены или подстановки – символы исходного текста заменяются на символы другого (или того же) алфавита в соответствии с заранее определенной схемой, которая и будет ключом данного шифра. Отдельно этот метод в современных криптосистемах практически не используется из-за чрезвычайно низкой криптостойкости.

Алгоритмы перестановки – символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом. Алгоритм перестановки сам по себе обладает низкой криптостойкостью, но входит в качестве элемента в очень многие современные криптосистемы.

Алгоритмы гаммирования – символы исходного текста складываются с символами некой случайной последовательности. Самым распространенным примером считается шифрование файлов «имя пользователя.pwl», в которых операционная система Microsoft Windows

95 хранит пароли к сетевым ресурсам данного пользователя (пароли на вход в NT-серверы, пароли для DialUp-доступа в Интернет и т.д.). Когда пользователь вводит свой пароль при входе в Windows 95, из него по алгоритму шифрования RC4 генерируется гамма (всегда одна и та же), применяемая для шифрования сетевых паролей. Простота подбора пароля обусловливается в данном случае тем, что Windows всегда предпочитает одну и ту же гамму.

Алгоритмы, основанные на сложных математических преобразованиях исходного текста по некоторой формуле. Многие из них используют нерешенные математические задачи. Например, широко используемый в Интернете алгоритм шифрования RSA основан на свойствах простых чисел.

Комбинированные методы. Последовательное шифрование исходного текста с помощью двух и более методов.

### *Алгоритмы шифрования*

### *Алгоритмы замены (подстановки)*

В этом наиболее простом методе символы шифруемого текста заменяются другими символами, взятыми из одного (одно- или моноалфавитная подстановка) или нескольких (много- или полиалфавитная подстановка) алфавита.

Самой простой разновидностью является прямая (простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого или некоторого другого алфавита. Таблица замены может иметь следующий вид:

Таблица 4.1. Таблица простой замены

| Исходные символы шифруемого текста | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Заменяющие символы | s | p | x | l | r | z | i | m | a | y | e | d | w | t | b | g | v | n | j | o | c | f | h | q | u | k |

Используя эту таблицу, зашифруем текст: In this book the reader will find a comprehensive survey... Получим следующее зашифрованное сообщение: At omiy pbbe omr nrsirn fadd zail s xbwgnrmrtjafr jcnfru... Однако такой шифр имеет низкую стойкость, так как зашифрованный текст имеет те же статистические характеристики, что и исходный. Например, текст на английском языке содержит символы со следующими частотами появления (в порядке убывания): E – 0,13, T –0,105, A – 0,081, O 0,079 и т.д. В зашифрованном тексте наибольшие частоты появления в порядке убывания имеют буквы R – 0,12, O - 0,09, A и N по 0,07.

Естественно предположить, что символом R зашифрована буква E, символом O – буква T и т.д. Это действительно соответствует таблице замены. Дальнейшая расшифровка не составляет труда.

Если бы объем зашифрованного текста был намного больше, чем в рассмотренном примере, то частоты появления букв в зашифрованном тексте были бы еще ближе к частотам появления букв в английском алфавите, и расшифровка была бы еще проще. Поэтому простую замену используют редко и лишь в тех случаях, когда шифруемый текст короток.

Для повышения стойкости шрифта используют полиалфавитные подстановки, в которых для замены символов исходного текста используются символы нескольких алфавитов. Известно несколько разновидностей полиалфавитной подстановки, наиболее известными из которых являются одно- (обыкновенная и монофоническая) и многоконтурная.

При полиалфавитной одноконтурной обыкновенной подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй – символом второго алфавита и т.д., пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.

Схема шифрования Вижинера. Таблица Вижинера представляет собой квадратную матрицу с $n^2$ элементами, где n – число символов используемого алфавита. На таблице 4.2 показана верхняя часть таблицы Вижинера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Сначала размещается первая строка, а под нею – строки, соответствующие буквам ключа в порядке следования этих букв в ключе шифрования. Пример такой рабочей матрицы для ключа «книга» приведен на таблице 4.3. Процесс шифрования осуществляется следующим образом:

1. Под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз.

2. Каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящимися под ними букв ключа.

3. Полученный текст может разбиваться на группы по несколько знаков.

Таблица 4.2. Таблица Вижинера

| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а |
| в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б |
| г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в |
| д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г |
| е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д |
| И т.д. до 33-ей строки… | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



Таблица 4.3. Рабочая матрица для ключа «книга»

| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **к** | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й |
| **н** | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м |
| **и** | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з |
| **г** | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в |
| **а** | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |

Пусть, например, требуется зашифровать сообщение: *максимально допустимой ценой является пятьсот руб. за штуку.* В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа. Получаем:

*максимально допустимой ценой является пятьсот руб. за*
*штуку книгакнигак нигакнигак нигак нигакниг акнигак ниг ак нигак*

Дальше осуществляется непосредственное шифрование в соответствии со вторым правилом, а именно: берем первую букву шифруемого текста (М) и соответствующую ей букву ключа (К); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (К) – в нашем примере такой буквой является Ч; выбранную таким образом букву помещаем в зашифрованный текст. Эта процедура циклически повторяется до зашифрования всего текста.

Эксперименты показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Нетрудно видеть, что замена по таблице Вижинера эквивалентна простой замене с циклическим изменением алфавита, т.е. здесь мы имеем полиалфавитную подстановку, причем число используемых алфавитов определяется числом букв в слове ключа. Поэтому стойкость такой замены определяется произведением стойкости прямой замены на число используемых алфавитов, т.е. число букв в ключе.

Расшифровка текста производится в следующей последовательности:

1. Над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз.

2. В строке подматрицы Вижинера, соответствующей букве ключа отыскивается буква, соответствующая знаку зашифрованного текста.

Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста.

3. Полученный текст группируется в слова по смыслу.

Нетрудно видеть, что процедуры как прямого, так и обратного преобразования являются строго формальными, что позволяет реализовать их алгоритмически. Более того, обе процедуры легко реализуются по одному и тому же алгоритму.

Одним из недостатков шифрования по таблице Вижинера является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключи с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющих смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Вижинера. Приведу только некоторые из них:

- во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке;
- в качестве ключа используется случайность последовательных чисел. Из таблицы Вижинера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10. Эти строки используются в соответствии с чередованием цифр в выбранном ключе.

  Известны также и многие другие модификации метода.

***Алгоритм перестановки***

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка – написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительные изменения, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке проявляются серьезные неудобства.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).

П У С Т Ь Б У Д Е Т Т А К К А

К М Ы Х О Т Е Л И К Л М Н О П

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Если строки укоротить, а количество строк увеличить, то получится прямоугольник-решетка, в который можно записывать исходный текст. Но тут уже потребуется предварительная договоренность между адресатом и отправителем посланий, поскольку сама решетка может быть различной длины-высоты, записывать ее можно по строкам, по столбцам, по спирали туда или по спирали обратно, можно писать и по диагоналям, а для шифрования тоже можно брать различные направления. В общем, здесь масса вариантов.

***Алгоритм гамирования***

Суть этого метода состоит в том, что символы шифруемого текста поочередно складываются с символами некоторой специальной последовательности, которая называется гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название «гаммирование». Процедуру наложения гаммы на исходный текст можно осуществить двумя способами. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю k, где k – число символов в алфавите, т.е.

$$R_i = ( S_i + G ) \bmod (k-1),$$

где $R_i$, $S_i$, G – символы соответственно зашифрованного, исходного текста и гаммы.

Таблица 4.4. Пример шифрования гаммированием

| Шифруемый текст | Б | У | Д | Ь … |
|---|---|---|---|---|
| | 010010 | 100000 | 110010 | 100000 |
| Знаки гаммы | 7 | 1 | 8 | 2 … |
| | 000111 | 000001 | 001000 | 000010 |
| Шифрованный текст | 010101 | 1000001 | 111010 | 100010 |

При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2. Вместо сложения по модулю 2 при гаммировании можно использовать и другие логические операции, например преобразование по правилам логической эквивалентности и неэквивалентности.

Такая замена равносильна введению еще одного ключа, которым является выбор правила формирования символов зашифрованного сообщения из символов исходного текста и гаммы (таблица 4.4).

Стойкость шифрования методом гаммирования определяется главным образом свойством гаммы – длительностью периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода.

Обычно разделяют две разновидности гаммирования – с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При этом если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким, т.е. его нельзя вскрыть при помощи статистической обработки зашифрованного текста. Это, однако, не означает, что дешифрование такого текста вообще невозможно: при наличии некоторой дополнительной информации исходный текст может быть частично или полностью восстановлен даже при использовании бесконечной гаммы.

В качестве гаммы может быть использована любая последовательность случайных символов, например, последовательность цифр числа π и т.п. При шифровании с помощью, например, аппаратного шифратора последовательность гаммы может формироваться с помощью датчика псевдослучайных чисел (ПСЧ). В настоящее время разработано

несколько алгоритмов работы таких датчиков, которые обеспечивают удовлетворительные характеристики гаммы.

### *Алгоритмы, основанные на сложных математических преобразованиях. Алгоритм RSA*

Алгоритм RSA (по первым буквам фамилий его создателей Rivest-Shamir-Adleman) основан на свойствах простых чисел (причем очень больших). Простыми называются такие числа, которые не имеют делителей, кроме самих себя и единицы. А взаимно простыми называются числа, не имеющие общих делителей, кроме 1.

Для начала выберем два очень больших простых числа (большие исходные числа нужны для построения больших криптостойких ключей. Например, Unix-программа ssh-keygen по умолчанию генерирует ключи длиной 1024 бита). Определим параметр n как результат перемножения p и q. Выберем большое случайное число и назовем его d, причем оно должно быть взаимно простым с результатом умножения (p–l)*(q–1). Отыщем такое число e, для которого верно соотношение

$$(e*d) \bmod ((p–1) *(q–1)) = 1$$

(mod – остаток от деления, т. е. если e, умноженное на d, поделить на ((p–1) *(q–1)), то в остатке получим 1).

Открытым ключом является пара чисел e и n, а закрытым – d и n. При шифровании исходный текст рассматривается как числовой ряд, и над каждым его числом мы совершаем операцию

$$C(i)= ( M(i)^e ) \bmod n.$$

В результате получается последовательность C(i), которая и составит криптотекст. Декодирование информации происходит по формуле

$$M(i) = (C(i)^d) \bmod n$$

Как видите, расшифровка предполагает знание секретного ключа. Давайте попробуем на маленьких числах. Установим p=3, q=7. Тогда

n=p*q=21. Выбираем d как 5. Из формулы (e*5) mod 12=1 вычисляем e=17. Открытый ключ 17, 21, секретный - 5, 21.

Зашифруем последовательность «2345»:

$C(2)= 2^{17} \bmod 21 =11$

$C(3)= 3^{17} \bmod 21= 12$

$C (4)= 4^{17} \bmod 21= 16$

$C(5)= 5^{17} \bmod 21= 17$

Криптотекст - 11 12 16 17.

Проверим расшифровкой:

$M(2)= 11^5 \bmod 21= 2$

$M(3)= 12^5 \bmod 21= 3$

$M(4)= 16^5 \bmod 21= 4$

$M(5)= 17^5 \bmod 21= 5$

Как видим, результат совпал.

Криптосистема RSA широко применяется в Интернете. Когда вы подсоединяетесь к защищенному серверу по протоколу SSL, устанавливаете на свой ПК сертификат WebMoney либо подключаетесь к удаленному серверу с помощью Open SSH или SecureShell, то все эти программы применяют шифрование открытым ключом с использованием идей алгоритма RSA. Действительно ли эта система так надежна?

С момента своего создания RSA постоянно подвергалась атакам типа Brute-force attack (атака методом грубой силы, т.е. перебором). В 1978 г. авторы алгоритма опубликовали статью, где привели строку, зашифрованную только что изобретенным ими методом. Первому, кто расшифрует сообщение, было назначено вознаграждение в размере 100 долл., но для этого требовалось разложить на два сомножителя 129-значное число. Это был первый конкурс на взлом RSA. Задачу решили только через 17 лет после публикации статьи.

Криптостойкость RSA основывается на том предположении, что исключительно трудно, если вообще реально, определить закрытый ключ из открытого. Для этого требовалось решить задачу о существовании делителей огромного целого числа. До сих пор ее аналитическими методами никто не решил, и алгоритм RSA можно взломать лишь путем полного перебора. Строго говоря, утверждение, что задача разложения на множители сложна и что взлом системы RSA труден, также не доказано.

Компания RSA (http://www.rsa.ru) регулярно проводит конкурсы на взлом собственных (и не только собственных) шифров. Предыдущие конкурсы выиграла организация Distributed.net (http://www.distributed. net/), являющаяся Интернет-сообществом добровольцев.

Участники Distributed.net загружают к себе на ПК небольшую программу-клиент, которая подсоединяется к центральному серверу и получает кусочек данных для вычислений. Затем все данные загружаются на центральный сервер, и клиент получает следующий блок исходной информации. И так происходит до тех пор, пока все комбинации не будут перебраны. Пользователи, участники системы, объединяются в команды, а на сайте ведется рейтинг как команд, так и стран. Например, участвующей в конкурсе по взлому RC5-64 (блочный шифр компании RSA, использующий ключ длиной 64 бита) организации Distributed.net удалось осуществить взлом через пять лет (1757 дней) работы. За это время в проекте участвовали 327 856 пользователей и было перебрано 15 268 315 356 922 380 288 вариантов ключа. Выяснилось, что была (не без юмора) зашифрована фраза «some things are better left unread» («некоторые вещи лучше оставлять непрочтенными»). Общие рекомендации-по шифру RC5-64 таковы: алгоритм достаточно стоек для повседневных нужд, но шифровать им данные, остающиеся секретными на протяжении более пяти лет, не рекомендуется.

### *Комбинированные методы шифрования*

Одним из важнейших требований, предъявляемых к системе шифрования, является ее высокая стойкость. Однако повышение стойкости любого метода шифрования приводит, как правило, к существенному усложнению самого процесса шифрования и увеличению затрат ресурсов (времени, аппаратных средств, уменьшению пропускной способности и т.п.).

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

Как показали исследования, стойкость комбинированного шифрования не ниже произведения стойкостей используемых способов.

Вообще говоря, комбинировать можно любые методы шифрования и в любом количестве, однако на практике наибольшее распространение получили следующие комбинации:

1) подстановка + гаммирование;
2) перестановка + гаммирование;
3) гаммирование + гаммирование;
4) подстановка + перестановка.

Типичным примером комбинированного шифра является национальный стандарт США криптографического закрытия данных (DES).

### *Криптографический стандарт DES*

В 1973 г. Национальное бюро стандартов США начало разработку программы по созданию стандарта шифрования данных на ЭВМ. Был объявлен конкурс среди фирм разработчиков США, который выиграла

фирма IBM, представившая в 1974 году алгоритм шифрования, известный под названием DES(Data Encryption Standart).

В этом алгоритме входные 64-битовые векторы, называемые блоками открытого текста, преобразуются в выходные 64-битовые векторы, называемые блоками шифротекста, с помощью двоичного 56-битового ключа К. Число различных ключей DES-алгоритма равно $2^{56}>7*10^{16}$.

Алгоритм реализуется в течение 16 аналогичных циклов шифрования, где на 1-ом цикле используется цикловой ключ $K_i$, представляющий собой алгоритмически вырабатываемую выборку 48 битов из 56 битов ключа $K_i$, I=1,2,...,16.

Алгоритм обеспечивает высокую стойкость, однако недавние результаты показали, что современная технология позволяет создать вычислительное устройство стоимостью около 1 млн. долларов США, способное вскрыть секретный ключ с помощью полного перебора в среднем за 3,5 часа.

Из-за небольшого размера ключа было принято решение использовать DES-алгоритм для закрытия коммерческой (несекретной) информации. Практическая реализация перебора всех ключей в данных условиях экономически не целесообразна, так как затраты на реализацию перебора не соответствуют ценности информации, закрываемой шифром.

DES-алгоритм явился первым примером широкого производства и внедрения технических средств в области защиты информации. Национальное бюро стандартов США проводит проверку аппаратных реализаций DES-алгоритма, предложенных фирмами-разработчиками, на специальном тестирующем стенде. Только после положительных результатов проверки производитель получает от Национального бюро стандартов сертификат на право реализации своего продукта. К настоящему времени аттестовано несколько десятков изделий, выполненных на различной элементарной базе.

Достигнута высокая скорость шифрования. Она составляет в лучших изделиях 45 Мбит/с. Цена некоторых аппаратных изделий ниже 100 долларов США.

Основные области применения DES-алгоритма:

- хранение данных на компьютерах (шифрование файлов, паролей);
- аутентификация сообщений (имея сообщение и контрольную группу, несложно убедиться в подлинности сообщения);
- электронная система платежей (при операциях с широкой клиентурой и между банками);
- электронный обмен коммерческой информацией обмен данными между покупателями, продавцом и банкиром защищен от изменений и перехвата.

Позднее появилась модификация DESa - Triple Des («тройной DES», так как трижды шифрует информацию «обычным» DESом), который свободен от основного недостатка прежнего варианта - короткого ключа; он здесь в два раза длиннее. Но зато, как оказалось, Triple DES унаследовал другие слабые стороны своего предшественника: отсутствие возможности для параллельных вычислений при шифровании и низкую скорость.

### *ГОСТ 28147-89*

В 1989 году в СССР был разработан блочный шифр для использования в качестве государственного стандарта шифрования данных. Разработка была принята и зарегистрирована как ГОСТ 28147-89. Алгоритм был введен в действие в 1990 году. И хотя масштабы применения этого алгоритма шифрования до сих пор уточняются, начало его внедрения, в частности, в банковской системе, уже положено. Алгоритм несколько медлителен, но обладает весьма высокой стойкостью.

В общих чертах ГОСТ 28147 аналогичен DES. Блок-схема алгоритма ГОСТ отличается от блок-схемы DES-алгоритма лишь отсутствием начальной перестановки и числом циклов шифрования (32 в ГОСТ против 16 в DES-алгоритме).

Ключ алгоритма ГОСТ - это массив, состоящий из 32-мерных векторов $X_1$, $X_2$,...$X_8$. Цикловой ключ i-го цикла $K_i$, равен Xs, где ряду значений i от 1 до 32 соответствует следующий ряд значений s: 1,2,3,4,5,6,7,8,1,2,3,4,5,6,7,8,1,2,3,4,5,6,7,8,8,7,6,5,4,3,2,1.

В шифре ГОСТ используется 256-битовый ключ и объем ключевого пространства составляет $2^{256}$. Ни на одной из существующих в настоящее время или предполагаемых к реализации в недалеком будущем компьютерной системе общего применения нельзя подобрать ключ за время, меньшее многих сотен лет. Российский стандарт проектировался с большим запасом, по стойкости он на много порядков превосходит американский стандарт DES с его реальным размером ключа в 56 бит и объемом ключевого пространства всего $2^{56}$(и неудивительно: его ключ длиной 32 байта (256 бит) вчетверо больше ключа DES, необходимое же на перебор всех ключей время при этом возрастает не в четыре раза, а в $256^{32-8}=256^{24}$, что выливается уже в астрономические цифры), чего явно недостаточно. В этой связи DES может представлять скорее исследовательский или научный, чем практический интерес.

В заключение заметим, что обоснованный выбор той или иной системы защиты, в общем-то, должен опираться на какие-то критерии эффективности. К сожалению, до сих пор не разработаны подходящие методики оценки эффективности криптографических систем.

Наиболее простой критерий такой эффективности – вероятность раскрытия ключа или мощности множества ключей (M). По сути это то же самое, что и криптостойкость. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех

ключей. Однако этот критерий не учитывает многих важных требований к криптосистемам [3, 6].

Поэтому желательно использование некоторых интегральных показателей, учитывающих указанные факторы. Но в любом случае выбранный комплекс криптографических методов должен сочетать как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в системе информации.

# Тема 5. Анализ и особенности каналов утечки и несанкционированного доступа к информации в технических информационных системах

## *Особенности современных каналов утечки и несанкционированного доступа к информации*

Для того чтобы построить эффективную систему информационной безопасности, необходимо в первую очередь определить реальные и потенциальные угрозы, каналы несанкционированного доступа и утечки информации. По результатам анализа публикаций последних лет [1 – 22] приведена обобщенная схема возможных каналов утечки и несанкционированного доступа к информации, обрабатываемой в типовом одноэтажном офисе. На данном примере рассмотрим более подробно особенности каналов утечки и несанкционированного доступа к информации, причем для наглядности далее по тексту цифрами в круглых скобках будут обозначаться каналы утечки информации, соответствующие данной схеме.

Одним из основных требований интегральной защиты является системный подход, поэтому при выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п. [1, 2, 6].

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной

сигнализации, электрофикациии, радиофикации, часофикации, электробытовые приборы и др.

В качестве каналов утечки большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

В зависимости от способов перехвата, от физической природы возникновнения сигналов, а также среды их распространения технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрические.

Для электромагнитных каналов утечки характерными являются побочные получения:

- электромагнитные излучения элементов ТСОИ (носителем информации является электрический ток, сила тока, напряжение, частота или фаза которого изменяются по закону информационного сигнала;
- электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС (в результате внешних воздействий информационного сигнала на элементы генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство;
- электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ТСПИ (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах

самовозбуждения, как правило, оказывается промодулированным информационным сигналом.

Возможными причинами возникновения электрических каналов утечки могут быть:

- наводки электромагнитных излучений ТСОИ (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС;
- просачивание информационных сигналов в цепи электропитания (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала;
- а просачивание информационных сигналов в цепи заземления (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п.);
- съём информации с использованием закладных устройств (представляют собой миниатюрные передатчики, устанавливаемые в ТСОИ, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны).

Параметрический канал утечки информации формируется путем «высокочастотного облучения» ТСОИ, при взаимодействии электромагнитного поля которого с элементами ТСОИ происходит переизлучение электромагнитного поля, промодулированного информационным сигналом.

Анализ возможных каналов утечки и несанкционированного доступа, показывает, что существенную их часть составляют технические каналы утечки акустической информации, носителем которой являются акустические сигналы. В зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов технические каналы утечки акустической информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными минипередатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т.п. В этом случае прием осуществляется, как правило, на специальные приемные устройства. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с обычного телефонного аппарата. Для этого их устанавливают либо непосредственно в корпусе телефонного аппарата, либо подключают к телефонной линии в телефонной розетке. Подобные устройства, конструктивно объединяющие микрофон и специальный блок коммутации, часто называют «телефонным ухом». При подаче в линию кодированного сигнала или при дозвоне к контролируемому телефону по специальной схеме блок коммутации подключает микрофон к телефонной линии и осуществляет передачу

акустической (обычно речевой) информации по линии практически на неограниченное расстояние.

В отличие от рассмотренных выше каналов в вибрационных, или структурных, каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела. В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

Электроакустические каналы утечки информации обычно образуются за счет электроакустических преобразований акустических сигналов в электрические по двум основным направлениям: путем «высокочастотного навязывания» и путем перехвата через ВТСС. Технический канал утечки информации путем высокочастотного навязывания образуется путем несанкционированного контактного введения токов высокой частоты от ВЧ-генератора в линии, имеющие функциональные связи с элементами ВТСС, на которых происходит модуляция ВЧ-сигнала информационным сигналом. Наиболее часто подобный канал утечки информации используют для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. С другой стороны, ВТСС могут сами содержать электроакустические преобразователи. К таким ВТСС относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Используемый в них эффект обычно называют микрофонным эффектом. Перехват акустических колебаний в этом случае осуществляется исключительно просто. Например, подключая рассмотренные средства к соединительным линиям телефонных аппаратов с электромеханическими звонками, можно при положенной трубке прослушивать разговоры,

ведущиеся в помещениях, где установлены эти телефоны. О том, каким образом не допустить этого, будет рассказано ниже.

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких, как стекла окон, зеркал, картин и т.п., создается оптико-электронный, или лазерный, канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие, как правило, в ближнем инфракрасном диапазоне волн и известные как «лазерные микрофоны». Дальность перехвата составляет несколько сотен метров.

Параметрический канал утечки информации образуется в результате воздействия акустического поля на элементы высокочастотных генераторов и изменения взаимного расположения элементов схем, проводов, дросселей и т.п., что приводит к изменениям параметров сигнала, например модуляции его информационным сигналом. Промодулированные высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы соответствующими средствами. Параметрический канал утечки информации может быть создан и путем «высокочастотного облучения» помещения, где установлены полуактивные закладные устройства, имеющие элементы, параметры которых (добротность, частота и т.п.) изменяются по закону изменения акустического (речевого) сигнала.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать

компьютерную текстовую информацию, в том числе осуществлять съём информации по системе централизованной вентиляции.

Особый интерес представляет перехват информации при ее передаче по каналам связи. Это вызвано тем, что в этом случае обеспечивается свободный несанкционированный доступ к передаваемым сигналам. Единственным гарантированным методом защиты информации в этом случае является криптографическая защита. В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Этот электромагнитный канал перехвата информации широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям. Этот канал наиболее часто используется для перехвата телефонных разговоров, при этом перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Подобные устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, обычно называются телефонными закладками.

Однако непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком. Поэтому чаще используется индукционный канал перехвата, не требующий контактного подключения к каналам связи. Современные индукционные датчики, по сообщениям открытой печати, способны снимать информацию с кабелей,

защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

В последнее время стало уделяться большое внимание утечке видовой информации, получаемой техническими средствами в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т.п.

Для документирования результатов наблюдения проводится съемка объектов, для чего используются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки.

Заканчивая эту тему, заметим, что число каналов утечки может превысить число 30, но это, к сожалению, не предел.

Приведем этот, пока неполный перечень:

- утечка за счет структурного звука в стенах и перекрытиях;
- съём информации с ленты принтера, плохо стертых дискет и дисков;
- съём информации с использованием видеозакладок;
- программно-аппаратные закладки в ПЭВМ;
- радиозакладки в стенах и мебели;
- съём информации по системе вентиляции;
- лазерный съём акустической информации с окон;
- производственные и технические отходы;
- компьютерные вирусы, «логические бомбы» и т.д.;
- съём информации за счет «Наводок» и «Навязывания» различных услуг;

- дистанционный съём информации (оптика);
- съём акустической информации за счет диктофонов;
- хищение носителей информации;
- высокочастотный канал утечки в бытовой технике;
- съём инфрмации направленным микрофоном;
- внутренние каналы утечки (через обслуживающий персонал);
- несанкционированное копирование;
- утечка за счет побочного излучения терминала;
- съём информации за счет использования телефонного уха;
- съём с клавиатуры и принтера по акустическому каналу;
- съём с дисплея по элктромагнитному каналу;
- визуальный съём с дисплея, сканера, принтера;
- наводки на линии коммуикаций и сторонние проводники;
- утечка по цепям заземления;
- утечка по сети электрочасов;
- утечка по трансляциооной сети и громкоговорящей связи;
- утечка по охранно-пожарной сигнализации;
- утечка по сети электропитания;
- утечка по сети отопления, газа и водоснабжения.

Список может быть продолжен и предела сверху не имеет.

## Тема 6. Аппаратная реализация некоторых современных технических методов несанкционированного доступа к информации

### *Аппаратная реализация современных методов несанкционированного доступа к информации*

Системный подход предполагает последовательный анализ от общего к частному. Результаты общего анализа возможных каналов утечки, приведенные выше, позволяют перейти к частным показателям, к вопросам технической реализации. Однако ограниченные возможности книги не позволяют подробно рассмотреть конкретные характеристики всех возможных каналов утечки информации, поэтому остановимся подробнее лишь на каналах утечки, свойственных средствам вычислительной техники, очень активно используемым в последнее время [1, 2, 6]

Известно, что работа средств вычислительной техники сопровождается электромагнитными излучениями, которые, как показано выше, являются источниками сигнала, способного сформировать определенные каналы утечки информации. Такими источниками могут быть материнские платы компьютеров, блоки питания, принтеры, накопители, плоттеры, аппаратура связи и др. Однако, как показывает статистика, основным источником высокочастотного электромагнитного излучения является дисплей, использующий электроннолучевую трубку. Изображение на экране дисплея формируется так же, как и в телевизионном приемнике, и состоит из светящихся точек на строках. Логическая единица видеосигнала создает световую точку, а логический нуль препятствует ее появлению.

Однако в цепях дисплея помимо видеосигнала присутствуют и тактовые синхроимпульсы, периодичность которых приводит к тому, что энергетический спектр паразитного сигнала содержит гармоники,

интенсивность которых убывает с ростом частоты. Источниками излучения видеосигнала дисплея могут быть элементы обработки сигнала изображения и электромагнитный луч кинескопа. Поскольку видеосигнал перед подачей на электронно-лучевую трубку усиливается до нескольких десятков киловольт, то именно его излучение является наиболее опасным. С увеличением частоты эффективность излучения схем монотонно возрастает со скоростью примерно 20 дБ в декаду до частот в несколько сотен мегагерц. Резонансы из-за паразитных связей могут вызвать усиление излучения на некоторых частотах спектра, что будет также способствовать утечке информации. Результаты экспериментальных исследований показали, что уровень широкополосного излучения дисплея зависит от числа букв на экране, в то время как уровень узкополосных составляющих не зависит от заполнения экрана и определяется системой синхронизации и частотой повторения светящихся точек. Отсюда следует, что видеоусилитель является наиболее мощным источником широкополосного излучения, а система синхронизации – узкополосного. В этом случае возможно восстановление информации по электромагнитному излучению дисплея.

Одним из возможных путей восстановления информации, отображенной на экране дисплея, является использование стандартного телевизионного приемника. Такой приемник обрабатывает небольшую часть спектра шириной около 8 МГц на частотах в диапазонах метровых и дециметровых волн. Необходимо отметить, что в отличие от дисплея максимум видеосигнала в телевизионном приемнике определяет уровень черного, а минимум – уровень белого. Поэтому изображение на экране приемника будет представлять собой копию изображения на экране дисплея и состоять из черных букв на белом (сером) фоне.

Так как принимаемое приемником излучение в данном случае не содержит информации о синхросигнале, то изображение на экране

приемника будет перемещаться в горизонтальном и вертикальном направлениях. Стабилизация изображения достигается путем использования внешнего генератора синхросигналов, подаваемых на приемник. С подобной простой приставкой к обычному телевизору возможно восстановить информацию с дисплея почти любого типа. Сигналы на выходе генератора должны иметь частоты 40...80 Гц для синхронизации кадров и 15...20 кГц – для синхронизации строк. Подобная техническая реализация с использованием ненаправленной антенны позволяет осуществить несанкционированный доступ (перехват) к информации с экрана дисплея на расстоянии 10...50 м соответственно для металлического и пластмассового корпуса ПЭВМ. Использование направленной антенны позволяет значительно расширить дальность перехвата и довести ее до 200 и 1000 м соответственно.

Необходимо отметить, что в настоящее время на коммерческом рынке имеется большое разнообразие средств специальной техники, с помощью которых возможно обеспечить несанкционированный доступ к информации. Поэтому для выбора возможных путей блокирования каналов утечки необходимо знать «противника» в лицо. Основные технические средства добывания информации представлены в таблице 6.1.

Анализ представленных материалов показывает, что в настоящее время номенклатура технических средств добывания информации весьма обширна, что делает задачу надежного блокирования каналов утечки и несанкционированного доступа к информации исключительно сложной. В этих условиях решение подобной задачи становится возможным только с использованием профессиональных технических средств и с привлечением квалифицированных специалистов [6]. В таблицах 6.2 и 6.3 приведены сравнительные характеристики активных и наиболее сложных для обнаружения пассивных средств получения информации.

Таблица 6.1. Основные технические средства добывания информации

| | | | | | |
|---|---|---|---|---|---|
| Радио-микрофоны (закладки) | Электронные "уши" | Средства перехвата телефонной связи | Средства скрытого наблюдения и поиска | Средства контроля компьютеров и сетей | Средства приема, записи, управления и др. |
| С автономным питанием | Микрофоны с проводами | Непосредствен-ного подключения | Оптические | Пассивные средства контроля монитора | Приемники для радиозакладок |
| С питанием от телефонной сети | Электронные стетоскопы | Индукционный датчик | Фотографиче-ские | Активные средства контроля монитора | Устройства накопления и записи |
| С питанием от электросети | Направлен-ные микрофоны | Датчик внутри телефонного аппарата | Тепловизион-ные и ночного видения | Пассивные средства контроля шины (магистрали) | Средства пере-приема (ретрансляторы) |
| Управляемые дистанционно | Лазерные микрофоны | Телефонной радиотрансля-ции | Телевизион-ные | Активные средства контроля шины (магистрали) | Средства уско-ренной передачи |
| С функцией включения по голосу | Микрофоны с передачей по электросети | Перехвата сотовой телефонной связи | Определения местоположе-ния | Аппаратные за-кладки | Устройства дис-танционного управления |
| Полуактивные | С микро-фоном аппарата | Перехвата пей-джинговых со-общений | Маркирова-ния и целеуказания | Программные закладки | Источники пита-ния |
| С накоп-лением и быстрой передачей | Гидроакусти-ческие микрофоны | Многоканаль-ного перехвата | Видеозакла-дочные | Компьютерные вирусы | Вспомогатель-ные и другие средства |

Таблица 6.2. Сравнительные характеристики пассивных средств получения информации

| Электронное средство контроля информации | Место установки | Дальность действия, м | Стоимость | 1. Вероятность применения<br>2. Качество перехвата<br>3. Вероятность обнаружения | Методы защиты информации |
|---|---|---|---|---|---|
| Контроль телефона, факса, модема (телефонная линия в штатном режиме) | | | | | |
| Индуктивный или контактный датчик | Телефонная линия | Регистрирующая аппаратура рядом с датчиком | Низкая | 1. Высокая<br>2. Хорошее<br>3. Не обнаруживается | Шифрование или маскирование (радиотехнических методов нет) |
| Контроль телефона (режим опущенной трубки) | | | | | |
| Контактный датчик | Телефонная линия | Регистрирующая аппаратура рядом с датчиком | Низкая | 1. Низкая<br>2. Хорошее<br>3. Не обнаруживается | Установка фильтров на входе линии |
| Контроль радиотелефона, радиостанции | | | | | |
| Панорамный радиоприемник | Прием из эфира | В пределах дальности станции | Средняя | 1. Высокая<br>2. Хорошее<br>3. Не обнаруживается | Шифрование (маскирование) |
| Нейтронное средство контроля информации | Место установки | Дальность действия, м | Стоимость | 1. Вероятность применения<br>2. Качество перехвата<br>3. Вероятность обнаружения | Методы защиты информации |
| Контроль сотового телефона | | | | | |
| Устройство прослушивания сотовой сети | Прием из эфира | В пределах соты абонента | Высокая | 1. Высокая<br>2. Хорошее<br>3. Не обнаруживается | Шифрование (маскирование) |

*Окончание табл. 6.2*

| | | | | | |
|---|---|---|---|---|---|
| Контроль монитора персонального компьютера | | | | | |
| Широкополосная антенна с регестрирующим устройством | Прием из эфира | 3...20 (определяется качеством экранирования монитора) | Весьма высокая | 1. Низкая<br>2. Посредственное<br>3. Не обнаруживается | Пассивная защита (экранировка помещения) |
| Широкополосный контактный датчик | Питающая электросеть | 0...50 (определяется развязкой по сети питания) | То же | То же | Установка сетевых фильтров |
| Контроль магистрали компьютерной сети | | | | | |
| Индуктивный или контактный датчик | Любое место на кабеле магистрали | Регистрирующая аппаратура рядом с датчиком | Высокая | 1. Высокая<br>2. Хорошее<br>3. Радиотехн. методами не обнаруживается | Шифрование, оргмероприятия (радиотехнических методов нет) |

Таблица 6.3. Сравнительные характеристики активных средств получения информации

| Электронное средство контроля информации | Место установки | Дальность действия, м | Стои-мость | 1. Вероятность применения<br>2. Качество перехвата<br>3. Вероятность обнаружения | Методы защиты информации |
|---|---|---|---|---|---|
| Контроль акустической информации | | | | | |
| Встроенный радиомикрофон | ПЭВМ, каль-кулятор телефон, телевизор, приемник | 200...1000 | Средняя | 1. Высокая<br>2. Хорошее<br>3. Высокая | Активные и пассивные (экранировка помещения) |
| Радиомикрофон с передачей по телефонной сети | Телефон-ный аппа-рат, розетка | 200...500 | Низкая | То же | Активные и пассивные (фильтры) |
| Радиомикрофон длительного действия с цифровой модуляцией, кодированием и дистанционным управлением | Элементы интерьера и строи-тельных конст-рукций | 200...1000 | Высокая | 1. Высокая<br>2. Средняя<br>3. Низкая | Активные и пассивные (экранировка помещения) |
| То же с записью ин-формации в память и с бросом по команде | То же | 200...1000 | Весьма высокая | 1. Низкая<br>2. Хорошее<br>3. Весьма низкая | Тоже |
| Видеоконтроль помещений | | | | | |
| Миниатюрн. камера с передачей изображе-ния по сети питания | Различные электриче-ские устройства | 10...30 | Высокая | 1. Низкая<br>2. Посредственная<br>3. Высокая | Активные и пассивные (сетевые фильтры) |

*Окончание табл. 6.3*

| | | | | | |
|---|---|---|---|---|---|
| То же с передачей изображения по радиоканалу | Предметы интерьера | 50...200 | Высокая | 1. Средняя<br>2. Хорошее<br>3. Высокая | Активные и пассивные (экранировка помещений) |
| Контроль видеоинформации с монитора ПЭВМ | | | | | |
| Передатчик с модуляцией видеосигналом монитора | Монитор ПЭВМ | 50...200 | Высокая | 1. Средняя<br>2. Хорошее<br>3. Высокая | Активные и пассивные, организационные меры (контроль персонала) |
| Контроль информации с внутренней шины ПЭВМ или сетевого сервера | | | | | |
| Передатчик с модуляцией информацией, проходящей по шине | Материнская плата ПЭВМ или сервера | 50...200 | Весьма высокая | 1. Низкая.<br>2. Хорошее.<br>3. Высокая | Активные и пассивные, организационные меры (контроль персонала) |
| Контроль информации с сетевой магистрали | | | | | |
| Передатчик с контактным или индуктивным датчиком на кабеле магистрали | Кабель магистрали или сервер компьютерной сети | 50...200 | Весьма высокая | 1. Средняя.<br>2. Хорошее.<br>3. Высокая (для кабеля), средняя (для сервера) | Активные и пассивные, организационные меры (контроль персонала) |

Программная реализация несанкционированного доступа к информации на основе использования программных закладок

Под несанкционированным доступом (НСД) к ресурсам компьютерной системы понимаются действия по использованию, изменению и уничтожению используемых данных указанной системы,

производимые субъектом, не имеющим права на такие действия. Если компьютерная система содержит механизмы защиты от НСД, то несанкционированные действия могут быть вызваны:

- отключением или видоизменением защитных механизмов нелегальным пользователем;
- входом в систему под именем и с полномочиями реального пользователя.

В первом случае злоумышленник должен видоизменить программу, защитные механизмы в системе (например, отключить программу запросов пользователей), во втором – каким-либо образом выяснить или подделать идентификатор реального пользователя (например, подсмотреть или вычислить пароль, вводимый с клавиатуры).

В обоих случаях НСД можно представить моделью опосредованного доступа, когда проникновение в систему осуществляется на основе некоторого воздействия, произведенного предварительно внедренной в систему программой или несколькими программами.

Основные известные способы внедрения программных закладок приведены в таблице 6.4.

Особый интерес представляют уязвимые места компьютерных систем, используемые для внедрения программных закладок.

Под уязвимостью компьютерной системы понимается некоторая слабость системы безопасности, которая может послужить причиной нанесения компьютерной системе ущерба. Обычно слабые (уязвимые) места в компьютерной системе называются дырами, люками, брешами.

Существующие закладки вирусного типа способны вызывать уничтожение или искажение информации, нарушение сеансов работы. Основную опасность они представляют для абонентских пунктов (АП) сети и рабочих станций ЛВС, так как могут распространяться от одного АП к другому с потоком передаваемых файлов или инфицировать

программное обеспечение рабочей станции при использовании удаленных ресурсов (запуск инфицированных программ в оперативной памяти рабочей станции, причем без экспорта выполняемого модуля с файл-сервера, т.е. в случае удаленного доступа к ресурсам сети).

Таблица 6.4. Способы внедрения программных закладок

| Способ внедрения | Характеристика |
|---|---|
| Внесение программных дефектов вирусного типа | Внедрение возможно на всех участках жизненного цикла ПО: эскизного и технического проектирования; рабочего проектирования; внедрения; эксплуатации, включая сопровождение и модернизацию |
| Несанкционированный доступ к ресурсам компьютерной системы | НСД к ресурсам компьютерной системы – действия по использованию, изменению и уничтожению используемых модулей и массивов данных, производимые субъектом, не имеющим права на такие действия |
| Несанкционированное вмешательство в процесс обмена сообщениями между углами связи ЛВС | Осуществляется путем передачи следующих сообщений: разрушающих; искажающих; имитирующих; хаотических |

Изо всех известных угроз наиболее часто встречаются программные кладки типа «троянского коня» и «компьютерного червя». Закладки типа «троякого коня» проявляют себя в определенных условиях (по времени, ключевым сообщениям и т.д.) и могут разрушать (искажать) информацию, копировать фрагменты конфиденциальной информации или пароли (ключи), засылать сообщения не по адресу или блокировать прием (отправку) сообщений.

Закладки типа «компьютерного червя» нацелены на проникновение системы разграничения доступа пользователей к ресурсам сети, могут приводить к утере матриц установления полномочий пользователей, к нарушению работы всей сети в целом и системы разграничения доступа в частности.

Для того чтобы закладка смогла выполнить какие-либо функции по отношению к прикладной программе, она должна получить управление на себя, т.е. процессор должен начать выполнять инструкции (команды), относящиеся к коду закладки. Это возможно только при одновременном выполнении двух условий:

- закладка должна находиться в оперативной памяти до начала работы программы, которая является целью воздействия закладки, следовательно, она должна быть загружена раньше или одновременно с этой программой;
- закладка должна активизироваться по некоторому общему как для закладки, так и для программы событию, т.е. при выполнении ряда условий в программно-аппаратной среде управление должно быть передано на программу-закладку.

К способам задействования программных закладок можно отнести:

- запуск программы;
- прерывания;
- определенное сочетание входных данных;
- определенное сочетание условий применения системы.
- По времени пребывания программной закладки в оперативной памяти можно выделить следующие типы закладок:
- резидентного типа – находятся в памяти постоянно с некоторого момента времени до окончания сеанса работы ПК (включения питания или перегрузки). Закладка может быть загружена в память при начальной загрузке ПЭВМ, загрузке операционной среды или запуске некоторой

программы (которая по традиции называется вирусоносителем), а также запущена отдельно;

- нерезидентного типа – начинают работу по аналогичному событию, но заканчивают ее самостоятельно по истечении некоторого промежутка времени или некоторому событию, при этом выгружая себя из памяти целиком.

Таким образом, программные закладки в настоящее время являются наиболее мощным и эффективным инструментом в реализации компьютерных угроз, защита от которых должна быть динамичной и постоянно совершенствоваться. Одним из наиболее эффективных способов борьбы с сетевыми угрозами, в том числе с программными закладками, является совершенствование методов и средств контроля доступа в сети.

## Тема 7. Современные технические средства обнаружения угроз

Заметное ухудшение криминогенной обстановки в обществе, экологии, социальной стабильности привели к усилению внимания к техническим средствам поиска и обнаружения угроз безопасности. Детекторы и обнаружители являются сегодня основными элементами большинства систем безопасности.

На рисунке 7.1 приведены основные технические средства обнаружения угрозы безопасности, предлагаемые сегодня российским коммерческим рынком.[1,2]

Наиболее обширную группу образуют технические средства, используемые для обеспечения информационной безопасности, в частности для обнаружения радио-, видео- и телефонных закладок (жучков). Прежде всего это устройства поиска по электромагнитному излучению: приемники, сканеры, шумометры, детекторы инфракрасного излучения, анализаторы спектра, частотомеры, панорамные приемники, селективные микровольтметры и т.д. Общим для всех этих устройств является задача обнаружения сигнала.

Специальные приемники для поиска работающих передатчиков в широком диапазоне частот на российском рынке представлены рядом фирм США, Германии и Японии. Подобные широкополосные приемники (сканеры), как правило, обладают частотным диапазоном не менее 30... 1500 МГц и чувствительностью порядка 1 мкВ. Поэтому сканеры − довольно сложные и дорогие устройства. Так, самый дешевый компактный японский сканер AR-8000 стоит порядка 700 долл., а самый дорогой IC-R9000 - порядка 7500 долл.

Процесс обнаружения закладок методом радиомониторинга еще более упрощается при использовании сканеров, реализующих дополнительную функцию измерения частоты (так называемых частотомеров) [5, 6].


Рис.7.1. Технические средства обнаружения угроз безопасности

Этот профессиональный частотомер работает со скоростью 200 млн. измерений в секунду. Имеется порт связи с персональным компьютером. Габаритные размеры прибора составляют 135x100x34 мм. Основные характеристики наиболее популярных сканеров приведены в таблице 7.1.

Таблица 7.1. Технические характеристики сканеров

| Модель | Диа-пазон, МГц | Вид модуляции | Чувствит., мкВ (с/ш=1) | Шаг настройки, кГц | Колич. каналов в памяти | Габариты, мм | Вес, кг |
|---|---|---|---|---|---|---|---|
| IC-R9000 | 0,03... 1999 | AM,FM, CW,FS, SSB,WFM | 0,3...6 | 0,01; 0,11; 10; 12,5; 20; 25; 100 | 1000 | 424x150x365 | 20 |
| FSM-8.5 | 26... 1000 | AM, FM, WFM | 1...10 | Ручная плавная | - | 210x158x52 | |
| IC-R7100 | 25... 199,9 | AM,FM, WFM,SSB | 0,2...1,6 | От 0,1 до 1000 | 900 | 241x94x239 | 6 |
| IC-R7000 | 25...999,9 1025... 1999 | AM,FM, WFM,SSB | 0,3...1 | 99 | | 286x110x276 | 8 |
| IC-R100 | 0,1...1856 | AM,FM | 0,2...3,2 | 1,5; 8; 9; 10 | 121 | 150x50x181 | 1,4 |
| AR-3000A | 0,1...2036 | AM,FM, WFM | 0,25...3 | От 0,05 до 995 по 0,05 | 400 | 200x138x80 | 1,2 |
| TRM-230 | 20...1000 | AM,FM, WFM | 1 | - | 30 | 188x71x212 | 3 |
| TRM-231 | 20...1000 | AM,FM, WFM | 0,5 | - | 100 | 433x132x465 | 15 |
| EB-100 Miniport | 20...1000 | AM,FM, WFM, SSB,FSK, CW | 1...9999 | - | 30 | 188x71x212 | 3 |
| STV-401 | 26...300 | AM,FM, WFM | 2 | Плавная ручная | - | 360x320x130 | 7 |
| AR-8000 | 0,5...1900 | AM,FM, WFM, SSB | 0,25...3 | От 0,05 до 500 | 1000 | 150x60x40 | 0,6 |
| IC-R1 | 0,2...1580 | AM,FM, WFM | 0,2...3 | От 0,5 до 50 | 100 | 150x65x45 | 0,65 |

Отдельную группу составляют приборы на основе приемников-сканеров, реализующие одновременно несколько функций по поиску закладок, ярким представителем которых является комплекс OSCOR-5000. Этот комплекс автоматически проводит мониторинг источников опасности 24 ч. в сутки. Он сканирует звуковой диапазон частот 50 Гц...15 кГц, радиочастоты 10 кГц...3000 МГц, ИК-диапазон длин волн – 850...1070 нм. Конструктивно прибор выполнен в корпусе кейса, общий вес комплекса составляет 12,7 кг.

Существенно облегчить просмотр радиодиапазона позволяют анализаторы спектра, среди которых можно отметить отечественные разработки анализаторов СМ-4-2 и СМ-4-21. Профессиональный анализатор спектра СМ-4-2 имеет диапазон частот от 2 до 1000 МГц и обеспечивает просмотр спектра принимаемых сигналов на электронно-лучевой трубке. Цифровой дисплей, автономное питание, сравнительно небольшие габариты (345х290х140 мм) и вес (14 кг) делают его переносным. Однако несмотря на хорошие характеристики и невысокую стоимость, в отличие от сканеров анализаторы спектра обладают слабыми резонансными функциями.

Дли решения задач скрытного выявления радиопередатчиков в ближней зоне (вблизи носимого радиопередатчика, на малоразмерных объектах) успешно используются детекторы электромагнитного поля. Операция выявления в этом случае заключается в обнаружении радиопередатчика по увеличению напряженности электромагнитного поля в ближней зоне антенны передатчика. Детекторы поля, как правило, изготавливаются и используются в носимом варианте с размещением их в часах (Ej-6), в авторучке (РК 860), в пачке сигарет (РК 865), на теле оператора (DM-19), в кейсе (VL-22H) или в книге (VL-34), но могут использоваться и в стационарном варианте с размещением их в коробке

сигар (РК 865-3), в цифровых часах (V-4330) и т.п. Характерной особенностью детекторов поля является широкая полоса тракта приема и отсутствие настройки на частоты сигналов. Известные детекторы поля в основном контролируют области частот в диапазонах 1…750 МГц и 1...1000 МГц, хотя встречаются и образцы в диапазонах 0,05...800 МГц (MTD) и 0,1...100 МГц (TS-2000). Недостаточная чувствительность детекторов поля и наличие ложных срабатываний приводят к снижению надежности обнаружения и увеличению времени поиска. Кроме того, подобные устройства не обнаруживают передатчиков с программным и дистанционным управлением.

Свободными от указанных недостатков являются обнаружители, принципы работы которых основаны на эффекте «нелинейной радиолокации». Принцип действия таких устройств (нелинейных радиолокаторов) основан на том факте, что при облучении радиоэлектронных устройств, содержащих нелинейные элементы, такие, как диоды, транзисторы и т.д., происходит отражение сигнала на высших кратных гармониках. Отраженные сигналы регистрируются локатором независимо от режима работы радиоэлектронного устройства (включено/выключено). Основные характеристики нелинейных локаторов, имеющихся сегодня на российском рынке, приведены в таблице 7.2.

Таблица 7.2.Основные характеристики нелинейных радиолокаторов

| Наименование (страна) | Частота сигнала, МГц | Мощность сигнала, Вт | Вид излучения | Номера гармоник приема | Чувствительность, Вт | Тип питания | Масса, кг |
|---|---|---|---|---|---|---|---|
| Supercout-C1 (США) | 915 | 0,3; 2 | Непрерывный | 2;3 | | Сеть и аккумулятор | 18 (полный комплект); 6,4 (от сети); 7,4 (от аккумулятора) |
| Supercout (США) | 915 | 0,016; 0,065 | То же | 2;3 | | То же | 17,7 (полный комплект) |
| Supercout (1995) (США) | 915 | 3 | | 2;3 | | Аккумулятор | 20 (полный комплект) |
| Broom (Великобритания)) | 888,5 (для США - 915) | 0,02...0,03; 0,06…0,9 (регулир.) | | 2;3 | 10 в степени -15 | То же | 10,2 (полный комплект); 7 (без упаковки) |
| SupebBroom (Великобритания) | 888,5 | 0,03…3 (регулир.) | Непрерывный | 2;3 | | Сеть и аккумулятор | |
| «Переход» (Россия) | 910 | 0,4; 0,8 | То же | 2 | 3х10 в степени -15 | То же | 13 (полный комплект); 7 (без упаковки) |
| «Родник-ПМ» (Россия) | 910 | 0,4; 0,8 | | 2 | Глубина регулироки 45 дБ | | 12 (полный комплект); 7 (без упаковки) |
| «Энвис» (Россия) | 910 | 0,04; 0,4; 0,08...0,8 (регулир.) | | 2;3 | 3х10 в степени -15 | | 15,5 (полный комплект); 8(без упаковки) |
| «Обь» (Россия) | 1000 | 0,25 | | 2 | 3х10 в степени -15 | Аккумулятор | |
| «Лотос» (Россия) | 895 | 30...250; 150...1250 (регулир.) | Импульсный | 2 | 10 в степени -11 | Сеть | 5 (без упаковки) |
| «Циклон-М» (Россия) | 680 | 50...300 (регулир.) | То же | 2 | 10 в степени -11 | | 3,5 (без упаковки) |
| «Октава» (Россия) | 890 | 30...300; 90...900 (регулир.) | | 2 | 10 в степени -11 | Сеть и аккумулятор | 13 (полный комплект); 5 (без упаковки) |
| «Люкс-3М» (Россия) | 915 | 2...20 | | 2;3 | -135 дБ/Вт | Аккумулятор | 1,2 (не более) |

Проведенный анализ показывает, что технические характеристики отечественных разработок нелинейных локаторов находятся на уровне мировых образцов, причем цены на них значительно ниже зарубежных. В настоящее время нелинейные локаторы в России активно совершенствуются и находят применение в следующих областях:

- обнаружение и определение местоположения скрытых электронных средств промышленного шпионажа (объекты обнаружения − приемопередающие устройства подслушивания и передачи данных, магнитофоны);
- обнаружение электронных компонентов и радиоаппаратуры при попытках скрытно провести их через контрольно-пропускные пункты заводов, складов и таможен;
- обнаружение несанкционированного выноса маркированных предметов и служебных помещений (объекты обнаружения − материальные и культурные ценности, снабженные нелинейными пассивными маркерами);
- дистанционный контроль багажа авиапассажиров (объекты контроля и радиоэлектронные системы, входящие в состав взрывных устройств, размещенные в багаже);
- поиск маркированных нелинейными пассивными маркерами людей в снежных завалах, разрушенных зданиях и др.

Особое место среди обнаружителей угроз безопасности занимают детекторы паразитных излучений аппаратуры, предназначенные для выявления работающих средств приема и регистрации аудио-, видео- и иной информации. Среди них на практике в основном используются детекторы магнитофонов и обнаружители телекамер. Детекторы магнитофонов применяются, как правило, для скрытного выявления носимых магнитофонов и конструктивно выполняются как в носимом, так

и в стационарном варианте. Операция вычисления заключается в обнаружении паразитного излучения генераторов стирания, двигателей магнитофонов, электронных схем и т.п. Так, например, детектор магнитофонов отечественного производства PTRD-12 обнаруживает списывающие устройства на фоне внешних помех, в 10 тыс. раз превосходящих уровень сигнала, исходящего от работающего двигателя. Причем дальность обнаружения магнитофонов составляет 40...60 см. По принципам построения, реализации и использованию эти средства обнаружения идентичны детекторам электромагнитного поля, рассмотренным выше, и отличаются от них только диапазоном частот приема, миниатюрностью, простотой эксплуатации и конструктивным исполнением (РК 645 – носимый вариант, РК 630 – стационарный вариант). Обнаружение магнитофона обычно индифицируется вибрацией корпуса (DM-3, TRD-009, TRD-800), а интенсивность излучения – яркостью свечения светодиода (РК-645). Кроме того, магнитофоны могут обнаруживаться также детекторами металла и локационными обнаружителями.

Контроль паразитных излучений аппаратуры, как правило, осуществляют многофункциональные системы. В частности, устройство контроля CRM 700 в диапазоне 200 Гц...3 ГГц с чувствительностью 1 мкВ обнаруживает излучения компьютеров, радиоэлектронной аппаратуры, радиозакладок, видео-, факсимильных и телексных передатчиков. Прибор TSD-5000 дополнительно к функциям защиты телефонной линии обнаруживает работающие магнитофоны на линии, передающие ТВ-камеры и радиопередатчики по их излучению. Система противодействия АСМ-3 обнаруживает радиопередающие устройства в диапазоне до 1,5 ГГц, а также излучение магнитофонов, ТВ-камер и другой аппаратуры. Рассмотренные средства, кроме того, обнаруживают сигналы передатчиков

во всех проводных линиях помещений, в том числе телефонных линиях, проводах электрической сети, линиях пожарной и охранной сигнализации, а также линиях внутренней связи. Необходимо отменить, что в настоящее время существуют приборы, производящие анализ телефонной линии на предмет обнаружения закладок с использованием нелинейной локации, однако они не получили широкого распространения в связи со сложностью работы и недостаточной надежностью результатов.

Завершая обзор средств обнаружения угроз информационной безопасности нельзя не остановиться на средствах антивирусной защиты. Современные технологии компьютерной вирусологии продолжают совершенствоваться. Начало 1999 г. ознаменовалось появлением целого букета вирусов, весьма агрессивно настроенных. В частности, первый «современный» Интернет-червь обнаружен «в живом виде» в январе 1999 г. Во второй половине января злоумышленниками были разосланы письма, зараженные этим вирусом, на несколько Интернет-серверов международных агентств новостей. Наибольшее количество сообщений о появлении в компьютерах «червя» было зарегистрировано в европейских сетях Интернета, особенно во Франции. Вирус распространяется как вложенный в письмо exe-файл с именем HAPPY99.EXE, который при запуске вызывает видеоэффект, напоминающий фейерверк, и поздравляет с новым, 1999 г. Помимо этого, «червь» вызывает процедуру инсталляции своего кода в систему: копирует себя в системный каталог Windows, перехватывает функции работы в Интернете, конвертирует свой код в формат почтового вложения и добавляет его к отсылаемым письмам. Таким образом, «червь» рассылает свои копии по всем адресам, на которые пользователь посылает сообщения.

Вирус «Caligula» принадлежит к новейшему классу вирусов, которых специалисты называют вирусами-шпионами. Эти вирусы создаются с целью похищения информации, хранимой на чужих компьютерах. Вирус

«Caligula» предназначенный для похищения ключей системы шифрования PGP, попадает на ПК вместе с зараженным документом в формате Microsoft Word. Оказавшись на новом компьютере, макровирус проверяет, не установлена ли в ней копия ПО PGP. В случае успешного обнаружения такой системы, используемые в ней закрытые ключи к шифрам будут потихоньку скопированы на один из ftr-серверов в сети, с которого они и попадут к злоумышленнику.

Много шума наделал новый макровирус WIN 95.CIH, который весьма уверенно продемонстрировал, что компьютерные вирусы в настоящее время могут успешно бороться не только с программным обеспечением – им теперь под силу и аппаратная часть компьютеров. Этот вирус в режиме записи разрушает микросхему перепрограммируемой памяти (Flash BIOS), расположенную на материнской плате.

В годовщину чернобыльской трагедии 26 апреля 1999 г. весь мир облетела весть о появлении новой разновидности вируса «Чернобыль», который удивил всех своей плодовитостью: только на территории Китая от него пострадало около 100 тыс. компьютеров. Ровно через год этот вирус опять напомнил о себе, причем нанесенный урон оказался еще большим.

Огромные убытки корпорациям нанес вирус типа «I Love You». Так, например, 5 мая 2000 г. компьютерная скорая помощь университета Карнеги – «Мелона» (США) зафиксировала заражение 270 тыс. компьютеров. Среди пострадавших – компания «Форд», ЦРУ, конгресс США. Кроме США, случаи заражения отмечены в Канаде, Азии, Скандинавии, Германии, Франции, Великобритании и т.д. (всего более 20 стран).

Необходимо отметить, что новые вирусы становятся все более изощренными и опасными. Так, если появившийся в 1999 г. вирус «Melissa» поразил около 20% компьютеров США, то вирус «I Love You»

2000 г. – свыше 50%. Для борьбы с рассмотренными выше вирусами разработаны отечественные антивирусные программы в пакетах Dr. Web 4.01 («ДиалогНаука») и AVP («Лаборатория Е. Касперского»). На российском рынке в настоящее время присутствуют также зарубежные программные средства обнаружения и обезвреживания компьютерных вирусов, представленные в таблице 7.3.

Таблица 7.3. Зарубежные антивирусные программные средства

| Программное средство | Страна-производитель | Фирма-разработчик |
|---|---|---|
| Vet-Anti-Virus | США | Computer Associates |
| F-Secure Anti-Virus | Финляндия | Data Fellows |
| NOD32 v1.27 | Словакия | ESET |
| F-Prot | Исландия | FRISK Software |
| AVG | Чехия | Grisoft |
| VirusScan, NetShield, McAfee, Total Virus Defence, RomShield | США | Network Associates (McAfee) |
| Sophos Anti-Virus | Великобритания | Sophos |
| NortonAV, Central Point | США | Symantec |

Учитывая сложную криминогенную обстановку в России, отметим, что в последнее время все большее внимание привлекают технические средства обнаружения угроз безопасности объектов. Это, в первую очередь, относится к металлодетекторам, портативным средствам контроля корреспонденции, портативным рентгеновским установкам и т.п. Население стало активно интересоваться, какие же средства сегодня существуют, чтобы предотвратить возможности террористических актов с применением оружия и боеприпасов, чтобы защитить свой дом,

автомобиль, себя и своих близких. Для этих целей современный российский рынок предлагает большой выбор средств обнаружения угроз.

Таблица 7.4. Особенности и возможности металлоискателя Intelliscan 12000

| Особенности | Возможности |
|---|---|
| Многозонная технология | Точное определение местонахожденияметаллических предметов в любой точке арки детектора |
| 18 (6x3) пространственных зон обнаружения | Устранение ложных срабатываний на ключи, монеты, часы и т. п. |
| Цифровая фильтрация шумового сигнала | Надежная защита от помех работающего поблизости оборудования |
| Максимальная чувствительность к различным типам металлов | Возможность настройки на металлы любых типов (ферромагнитные, немагнитные и т. п.) |
| Высокая пропускная способность | До 50 человек в минуту |
| Детекторные панели на основе двойных детекторных головок с самобалансировкой | Равномерная защита в любой точке арки (от уровня пола до верха, от одной стойки до другой) |
| Независимая регулировка чувствительности по зонам | Позволяет получить 100 %-ное обнаружение предметов в нижней зоне рядом с полом или небольших предметов, скрытых в волосах |
| Максимальная надежность во всем диапазоне скоростей | Сохранение параметров в широком диапазоне скоростей (от шага до бега) |
| Минимально возможный уровень магнитного поля | Абсолютная безопасность для людей с кардиостимуляторами, для дисков и пленок |
| Кодовый пароль | Уполномоченный персонал имеет 6-значный код допуска |
| Автокалибровка и полное самотестирование | Выполняется при каждом включении автоматически |
| Простая сборка и запуск в эксплуатацию | Процедура занимает всего 15 мин |

На примере металлоискателя Intelliscan 12000 фирмы RANGER в таблице 7.4 представлены особенности построения и основные возможности современных технологий создания средств обнаружения угроз безопасности объектов.

Современная цифровая технология пространственного обнаружения, использованная при создании металлоискателя Intelliscan 12000, позволяет со 100%-ной надежностью обнаруживать и мгновенно локализовать оружие при вносе его на объект. Однако в последнее время весьма актуальной становится проблема локализации взрывчатки, пересылаемой по почте, основными способами борьбы с этой проблемой на сегодняшний день являются: визуальный осмотр корреспонденции с целью обнаружения подозрительных конвертов, бандеролей; техническая проверка, проводимая после визуального осмотра, осуществляется в специальном взрывобезопасном боксе.

Особое место среди технических средств обнаружения угроз занимают приборы психофизиологического исследования человека, так называемые детекторы лжи. Впервые портативные чернилопишущие полиграфы, предназначенные для выявления у человека скрываемой им информации, появились в США в середине 30-х гг. Эти приборы позволяют регистрировать на бумажной ленте в виде полиграмм традиционные для психофизиологического метода «детекции лжи» процессы: дыхание, сердечно-сосудистая деятельность, изменение физических свойств кожи (кожно-гальванический рефлекс), двигательная активность человека.

Развитие электронно-вычислительной техники привело к появлению компьютерных полиграфов (КП), обладающих значительно большими возможностями. В таблице 7.5 дан перечень сравнительных характеристик современных КП.

Таблица 7.5. Сравнительные характеристики компьютерных полиграфов

| Характеристики | Фирма-изготовитель (базовая модель) | | | | | |
|---|---|---|---|---|---|---|
| | «Геолид» (Барьер-14) | «Инекс» (PM-004) | «Эпос» («Эпос-5») | «Гротек» (МЦП-2611) | Axcition Systems | Lafayette Insrument |
| Регестрируемые физические показатели | | | | | | |
| дыхание:<br>грудное<br>диафрагмальное | <br>+<br>+ | <br>+<br>+ | <br>+<br>+ | <br>+<br>+ | <br>+<br>+ | <br>+<br>+ |
| кожное сопротивление:<br>физическое<br>тоническое | <br>+<br>+ | <br>+<br>Нет | <br>+<br>+ | <br>+<br>+ | <br>+<br>Нет | <br>+<br>Нет |
| автоматическая фиксация противодействия | + | | Нет | Нет | | |
| артериальное давление | + | | | | + | + |
| фотоплетизмо грамма | + | + | + | + | + | + |
| тремор | + | Нет | + | + | + | + |
| оценка функцио нального состояния в реальном времени | + | | + | Нет | Нет | Нет |
| Технические характеристики | | | | | | |
| интерфейс обмена | RS 232 | RS 232 | RS 232 | Сист. шина | RS232 | RS 232 |
| гарантия | 3 года | 1 год | 1 год | 1 год | 3 года | 1 год |
| цена, USD | 4200 | 4600 | 4900 | 11200 | 13500 | 9890 |
| страна-изготовитель | Россия | Россия | Россия | Россия | США | США |
| опыт массового применения | Есть | Нет | Есть | Нет | Есть | Есть |

Рассмотренные КП в настоящее время могут быть успешно использованы при решении следующих задач: профессиональный отбор кадров, профилактика правонарушений на производстве, расследование криминальных случаев (нанесение ущерба, разглашение информации, хищения). Достоверность сведений, получаемых в результате полиграфического обследования, для опытного оператора доходит до 97%. Как показывает зарубежный и отечественный опыт использования КП эффективность их использования в конечном счете зависит от профессионализма оператора, поэтому вопросам подготовки и повышения квалификации операторов необходимо уделять особое внимание.

Учитывая мировой опыт эксплуатации полиграфов, необходимо признать, что проверки на полиграфе относятся к «технологиям двойного назначения», поэтому КП используются не только правоохранительными органами и спецслужбами, но и отечественными предпринимателями для обеспечения своей коммерческой безопасности. В этом случае в среднем на 25% повышается вероятность того, что нанимаемый сотрудник окажется честным человеком.

Подводя итоги, можно заключить, что в настоящее время российский рынок средств поиска угроз безопасности уже стабилизировался и достаточно адекватно реагирует на изменение обстановки, предоставляя заинтересованным лицам соответствующие средства для выбора.

## Тема 8. Современные технические сребдства обеспечения безопасности в каналах информационно-технических систем, телекоммуникаций и ПЭВМ

Эволюция технологии обеспечения безопасности связи показывает, что только концепция комплексного подхода к защите информации может обеспечить современные требования безопасности в каналах телекоммуникаций. Комплексный подход подразумевает комплексное развитие всех методов и средств защиты и требует проведения их классификации. Результаты проведенного анализа современных методов и средств позволяют представить процесс обеспечения безопасности в каналах телекоммуникаций, методы и средства, его реализующие, в следующем виде (рис. 9.1).


Рис. 9.1. Методы и средства обеспечения безопасности в каналах ИВС и телекоммуникаций

Рассмотрим кратко основное содержание представленных методов и средств обеспечения безопасности в каналах телекоммуникаций.

Управление доступом – метод защиты информации регулированием использования всех ресурсов системы (элементов БД, 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 работы, отказ в запросе) при попытках несанкционированных действий.

Маскировка – метод защиты информации в каналах телекоммуникаций путем ее криптографического закрытия. Этот метод защиты широко применяется за рубежом как при обработке, так и при хранении информации, в том числе на гибких магнитных дисках. При передаче информации по каналам телекоммуникаций большой протяженности этот метод является единственно надежным. В отечественных коммерческих системах этот метод используется еще достаточно редко из-за недостатка технических средств криптографического закрытия и их высокой стоимости в настоящее время.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму [1,6].

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

Побуждение – такой метод защиты, который побуждает пользователя и персонал системы не нарушать сложившиеся моральные и этические нормы (как регламентированные, так и «неписаные»).

Рассмотренные выше методы обеспечения безопасности в каналах телекоммуникаций реализуются на практике применением различных средств защиты, таких как технические, программные, организационные, законодательные и морально-этические.

Рассмотрим основные средства, используемые для создания механизмов защиты.

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить схемы контроля информации по четности, схемы защиты полей памяти по ключу и т.п.

Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации. Программные средства представляют собой ПО, специально предназначенное для выполнения функций защиты информации [1,6].

Указанные выше средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. Первоначально программные механизмы защиты включались, как правило, в состав ОС, управляющих ЭВМ, или систем управления и данных. Практика показала, что надежность подобных механизмов является явно недостаточной. Особенно слабым звеном оказалась защиту по паролю. Поэтому в дальнейшем механизмы защиты становились все более сложными, с привлечением других средств обеспечения безопасности. Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека. Наиболее показательным примером таких норм является кодекс профессионального поведения членов Ассоциаций пользователей ЭВМ США.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

В заключение необходимо также отметить, что все рассмотренные средства защиты делятся на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Таким образом, сопоставление существующих методов и средств защиты и эволюции технологии обеспечения безопасности связи в каналах ИВС и телекоммуникаций показывает, что на первой фазе развития этой технологии преимущественное развитие имели программные средства, вторая фаза характеризовалась интенсивным развитием всех основных методов и средств защиты, на третьей фазе развития все определенней вырисовываются следующие тенденции:

- аппаратная реализация основных функций защиты; создание комплексных средств защиты, выполняющих несколько защитных функций; унификация и стандартизация алгоритмов и технических средств.

В силу своей специфики информация о возможных каналах утечки и несанкционированного доступа длительное время была недоступна широкому пользователю, что, безусловно, способствовало росту злоумышленных воздействий. Совершенно очевидно, что для успешной защиты своей информации пользователь должен иметь абсолютно ясную картину о возможных каналах утечки, чтобы соответствующим образом предпринять контрмеры по пресечению несанкционированного доступа (усилить программную защиту, использовать антивирус программы, сменить алгоритм закрытия, усилить пароли и т.п.). Основными путями несанкционированного получения информации являются:

- перехват электронных излучений; принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей; применение подслушивающих устройств (закладок); дистанционное фотографирование; перехват акустических излучений и восстановление текста принтера; хищение носителей информации и производственных отходов; считывание данных в массивах других пользователей; чтение остаточной информации в памяти системы после выполнения санкционированных запросов; использование недостатков языков программирования и ОС;
- включение в библиотеки программ специальных блоков типа «троянского кон»;
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерного вируса, так как с учетом большого числа его модификаций надежной защиты против него не удалось разработать. Все остальные пути несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности. В последующих разделах будут более подробно рассмотрены современные методы и средства обеспечения безопасности при обработке и передаче информации по каналам телекоммуникаций.

### *Технические средства обеспечения безопасности ЭВМ*

По данным ФБР, в США ежегодные потери от преступлений, совершаемых с помощью вычислительной техники, составляют 100 млрд. долл., при этом средняя сумма одной кражи равна 430 тыс. долл. Шансы

найти преступника чрезвычайно малы: согласно оценкам, один случай из 25 тысяч.

Несколько лет назад доступ к конфиденциальным и финансовым данным имел лишь ограниченный круг лиц: высшее руководящее звено и технический персонал вычислительного центра (ВЦ). В настоящее время в связи с появлением ПЭВМ численность этой группы быстро увеличивается. ЭВМ становится обычной принадлежностью учреждений, в результате чего доступ к информации о чужой собственности получает большое число лиц – владельцев данных, представляющих значительный интерес. Наряду с этим техника защиты намного отстает от уровня развития гибкости самих вычислительных систем. По общему мнению специалистов, в 80% всех преступлений, совершенных с помощью вычислительных средств, преступники находятся среди персонала учреждения. В результате большая часть устройств защиты данных не может выполнять свои функции. Сложные схемы охраны доступа и подключения к машине, предназначенные для предотвращения несанкционированного пользования данными, бесполезны, когда наибольшую опасность представляют сотрудники самих вычислительных комплексов.

Внутренние меры предосторожности также не нужны, если они, как это часто случается, небрежно применяются или игнорируются, например, пароль воспроизводится на дисплеях или даже стенах учреждения. Поэтому при внедрении средств защиты данных необходимо четко понимать характер преступлений, совершаемых с помощью вычислительной техники. Однако в настоящее время руководители ВЦ в основном не принадлежат к поколению, знакомому с этой техникой. Анализ совершенных преступлений такого рода показал следующее:

- в большинстве вычислительных комплексов значительное число лиц имеет доступ к системе в различных точках линии связи. Это приводит преступника к выводу, что трудно обнаружить сам факт манипулирования данными или их кражи, т.е. преступнику не грозит опасность оставить «следы» на месте преступления;
- вследствие «неосязаемого» характера кража практически остается незамеченной, поскольку ни сами данные, ни форма их представления, ни место хранения не исчезают и не изменяются, а поэтому нет и причин для проведения следствия;
- неправильное манипулирование данными ЭВМ может быть вначале вызвано ошибкой, и, если она останется незамеченной и неисправленной,
- это может вызвать такие поступки служащих, которые до этого считались бы невозможными;
- боязнь неблагоприятной реакции акционеров или разглашения конфиденциальных сведений, ознакомления широкой публики с недостатками ВЦ приводит к тому, что не всегда сообщается об установленных фактах совершения компьютерных преступлений, что значительно затрудняет поиск преступника;
- существенным недостатком стандартных программ ведения бухгалтерских расчетов является отсутствие следов ревизии счетов, без которых нельзя восстановить входное сообщение, приведшее к изменению файла, и идентифицировать преступника.

Очевидно, пока не существует средств, которые полностью бы исключили возможность совершения компьютерного преступления, но сократить их число можно за счет усиления ответственности персонала, тщательной проверки лиц, принимаемых на работу в ВЦ, постоянной смены персонала, работающего на особо важных участках, правильного использования паролей и регистрации пользователей, ограничения доступа к данным на основе только рабочей необходимости, шифрования данных и

обеспечения программ проверки. Необходимо уделять внимание проблеме сохранения данных на носителе большой емкости, например на гибких дисках, о которых при установлении средств защиты данных часто забывают.

Большую опасность с точки зрения возможности получения несанкционированного доступа к данным представляют собой локальные сети связи, в которых каждая ЭВМ сети имеет доступ ко всем остальным. Уже существуют поставщики устройств, обеспечивающих возможность подключения к сети без нарушения ее работы. Одним из решений задачи защиты данных локальных сетей является применение коаксиального кабеля замкнутой ТВ-системы и волоконно-оптического кабеля. Лучшей защиты можно достичь путем применения закрытых металлических объединительных блоков и гибких металлических цилиндров при присоединении кабеля к распределительной коробке.

Фирмой «Sipher Designs» создана система управления локальной сетью NBS, предназначенная для защиты данных линий связи в случае их неисправности. Система NBS обеспечивает ее устранение путем реконфигурации сети с помощью локального устройства управления или дистанционного программирования, такого как ПЭВМ. Система также дает возможность пользователю переключать режим неавтономной работы машины на автономный.

Фирма «Modular Technology» предлагает систему передачи данных с помощью ИК-излучения (на расстояние до 200 м) или модулированного лазерного лучика (на расстояние до 1 км). К системе, названной Free Space Communication System, могут подключаться цифровые дисплеи или видеокаректоры, в том числе и камеры замкнутых ТВ-систем, расположенные на расстоянии 15 м друг от друга и присоединенные к центральному пульту управления, цифровому дисплею или системе речевого управления. Скорость передачи данных равна 2,5 Мбит/с.

Благодаря использованию светового излучения для передачи данных система обеспечивает высокую скрытность передачи и трудность несанкционированного подключения. Гибкость системы, возможность передачи речевых и видеосигналов, а также цифровых данных, быстрого монтажа (несколько часов) и простота сопряжения с другими устройствами обусловливают перспективность применения системы в экстренных ситуациях. Основным ее недостатком является необходимость размещать приемник и передатчик в пределах прямой видимости. К другим проблемам относится обеспечение незаметной прокладки линий связи и зависимость их характеристик от воздействия окружающей среды. Фирмой «Schlage Electronics Europe» выпущен новый вариант программы управления защитой данных SE5795, которая может выполняться на ПЭВМ типа PC/XT и AT фирмы «IBM». С помощью программы SE5795 можно записывать и хранить на твердых дисках описания до 300 тыс. случаев вызова системы управления, возбуждения сигнала тревоги и принятия административных решений. Одним из основных достоинств программы является простота и высокое быстродействие при вызове события. По команде система немедленно устанавливает исходное состояние необходимых данных и затем проверяет хранимые сведения со скоростью 3 события в одну секунду. Путем удлинения временного интервала, ключевых слов и чисел пользователи могут вызывать либо все, либо избранные события в пределах определенного периода времени.

Сообщения, генерируемые программой SE5795A, могут воспроизводиться на экране ЭЛТ, выводиться на печатное устройство или записываться в накопитель на гибких дисках для обработки на других машинах. Персональная ЭВМ типа XT или AT, работающая с программой SE5795A, может быть использована в качестве терминала для задания или изменения конфигурации средств управления доступом и контроля опасной ситуации. Предусмотрены средства защиты с помощью пароля.

Фирма «Timplex» выпустила систему набора SDS с защитой от несанкционированного подключения к сети передачи данных, позволяющую получать доступ к средствам передачи данных с помощью определенного телефонного номера или утвержденного пароля пользователя. Система обеспечивает также контроль и регистрацию данных. При наборе номера абонента система SDS сразу же запрашивает пароль. Если последний находится на координатной сетке, пользователю предлагается ждать соединения. В противном случае соединение с системой прерывается. Доступ к средствам контроля пароля и управления рабочими параметрами также обеспечивается с помощью пароля.

В фирме «Automated Desigh and Manufacturing» создана двухканальная система засекречивания связи, подключаемая к телефонной сети. Система предотвращает доступ к главному терминалу, периферийным устройствам и ЭВМ благодаря тому, что сигнал запроса и кодированный сигнал передаются по разным телефонным каналам и в разное время. Воспроизвести кодированный сигнал и генерирующие его аппаратные средства на основе данных, полученных путем незаконного подключения ко второму каналу, практически невозможно.

Защита главной ЭВМ от несанкционированного доступа достигается с помощью следующих трех мероприятий:

- организации связи с главной ЭВМ по телефонному каналу через модем; устройство защиты данных, контролирующее связь по этому каналу, не допускает соединения с модемом без кодированного сигнала, поступающего по второй телефонной линии (лица, пытающиеся незаконно получить доступ к ЭВМ чаще пользуются одной телефонной линией);
- применения специальных аппаратных средств генерации кодированных сигналов и передачи их по второму телефонному каналу, а также оборудования с декодирующими устройствами, установленными в ЭВМ, к которой имеет доступ только определенная группа пользователей;

- использования устройств защиты, препятствующих декодированию сигналов, передаваемых по второй линии связи.

Кроме того, в устройство пользователя могут входить генератор НЧ, генератор импульсов с регулируемым рабочим циклом, модулятор и трехразрядный декодер. При объединении этих блоков формируется система, выходной сигнал которой почти невозможно воспроизвести. Так, с выхода генератора НЧ может сниматься нестандартный сигнал, который затем модулируется любым известным методом, совместным с передачей сигнала по телефонной линии связи (например, с помощью частотной, импульсной, фазовой модуляции, частотной манипуляции и т. п.).

Блок защиты данных расположен вне главной ЭВМ и используется совместно с телефонным ответчиком. При испытании системы различными независимыми учреждениями и ведомствами ни одному пользователю не удалось получить несанкционированный доступ к главной ЭВМ.

Фирма «Fischer-Innis Systems» выпустила версию программы обеспечения безопасности Watchdog 4.1, в которой предусмотрен новый автоматический метод расширения средств защиты для предотвращения стирания новых и старых справочных данных, хранимых в накопителях на жестких дисках. Программа может управляться данными, записанными в накопители на жестких дисках ПЭВМ. При этом пользователи должны периодически менять пароль программы.

Защита записанных на жесткие диски справочных данных осуществляется автоматически в соответствии с указываемыми пользователем сведениями при необходимости применения и копирования файлов или создания новых рамочников.

В новом алгоритме обеспечения безопасности предусмотрена возможность вписывать по желанию пользователя на жесткие диски программы проведения ревизии, доступ к которым осуществляется с

помощью данных, хранимых па жестком диске. Программа ревизии контролирует применение средств, доступ к которым можно получить с помощью меню выбора обслуживающей программы.

Средства защиты данных предусматривают идентификацию пользователя и контроль доступа с помощью пароля, автоматическое кодирование и декодирование данных и применение многоуровневой системы считывания записи и формирования/стирания разрешений файла.

Программа не позволяет без разрешения использовать программу FORMAT (формирование) для стирания данных, хранимых на жестком диске.

В фирме «SPL Software Protect» (Швейцария) предполагается решить проблему защиты программного обеспечения путем шифрования программ с помощью произвольного генерируемого ключа. Это означает, что одну и ту же программу можно выполнять только на оборудовании с одинаковыми кодами и микропроцессором фирмы «SPL».

Фирмой «RAM Software» разработан пакет программ защиты данных микро-ЭВМ, используемых для проведения деловых операций. Пакет, названный FORTRESS, предотвращает несанкционированный доступ к данным микро-ЭВМ и обеспечивает автоматическое кодирование и декодирование всех данных и программ в реальном масштабе времени.

Все рассмотренные средства защиты предназначены в конечном счете для предотвращения замены данных, хранимых в основном в накопителях на магнитных носителях. Такая возможность может быть исключена при использовании оптических накопителей, в которых информация хранится на диске из стекла или пластмассы. На поверхности такого диска с помощью сфокусированного лазерного пучка малого диаметра выжигается пятно, изменяющее показатель отражения поверхности в этой точке. Пятно представляет собой хранимую на диске единицу информации, которую можно считать излучением маломощного лазера. Данные, записанные на

диске, нельзя стереть, их можно только считывать. Теоретически можно записывать новые данные на диск с уже имеющимися записями, но при этом все записи, накладываясь одна на другую, потеряют смысл. Поскольку объем хранимых на оптическом диске данных велик (до $10^8$ мегабайт на одной стороне диска диаметром 30,5 мм), то не возникает острой необходимости стирания информации для записи новой. Испытания оптических дисков показали, что срок хранения данных на них без деградации достигает 10 лет. На оптический диск может быть записана полная и неуязвимая программа выявления следа ревизии всех входных сообщений, приводящих к изменению файла, независимо от того, насколько тривиальным было такое сообщение. Оптические диски легко сопрягаются с существующими ЭВМ. Единственная проблема, которую необходимо решить, заключается в модификации ОС и прикладного ПО для записи на нестираемый носитель.

Фирма «Identex» выпустила систему проверки и идентификации модели IDX-10, отличающуюся высоким уровнем обеспечения безопасности и простотой работы. Система состоит из терминалов, содержащих устройство для получения данных отпечатка пальца и аппаратные средства анализа. Терминалы подключены с помощью локальной сети к главной ЭВМ, в качестве которой используется ПЭВМ типа PC/XT фирмы «IBM», оснащенная клавишной панелью, накопителями на жестких дисках емкостью 10 Мбайт и на гибких дисках емкостью 350 кбайт. Решение о предоставлении доступа принимается на основе отпечатка пальца лица, запрашивающего разрешение, и сравнения его с хранимым в памяти главной ЭВМ «шаблоном» (математическим описанием преобразованной в цифровой вид информации). Для записи в память данных об отпечатке пальца и идентификационного номера требуется менее 1 мин, проверка по отпечатку пальца занимает менее 6 с.

В случае совпадения вводимых и хранимых данных система IDX-10 возбуждает команду на доступ к терминалу.

Военные ведомства давно разрабатывают средства защиты вычислительных систем от электронных подслушивающих устройств. Однако пока имеется лишь дорогостоящее оборудование, блокирующее ВЧ-излучение экранов видеотерминалов. При наличии модифицированного телевизора, тюнера и антенны, находясь за пределами учреждения, можно зафиксировать текст и данные, воспроизводимые на экране видеотерминала. В результате такого подслушивания можно узнать номер счета или пароль, обеспечивающий доступ к вычислительной системе.

Исследования фирмы «Datasafe» показали, что степень излучения экрана зависит от разрешения и скорости обновления данных: чем эти параметры выше, тем лучше изображение, принимаемое подслушивающим устройством. Для предотвращения указанного подслушивания фирма выпустила устройство защиты размером 112x114x40 мм и массой 250 г, работающее от сети. Это устройство создает защитное электромагнитное поле, размещается у терминала и искажает излучаемые им сигналы. При этом воспроизводимые и хранимые в ЭВМ данные не изменяются. В настоящее время использование подобных устройств защиты (генераторов шума) является основным направлением обеспечения безопасности информации в ВЦ.

Таким образом, краткий обзор современных технических средств защиты ЭВМ показывает, что проблема предотвращения компьютерных преступлений становится все более актуальной, но ее эффективное решение в настоящее время возможно лишь при комплексном подходе.

***Анализ типовых мер обеспечения безопасности ПЭВМ***

В связи с получившим за последние годы широким применением персональных ЭВМ (ПЭВМ) и локальных вычислительных сетей (ЛВС) в государственных учреждениях и промышленных фирмах особую важность приобретает решение проблемы защиты от несанкционированного доступа к ним для предупреждения возможности утечки или кражи коммерческих, финансовых и других ценных данных.

Аналогичные проблемы существуют и для больших ЭВМ, но для них разработаны эффективные аппаратные и программные средства, предотвращающие или сводящие к минимуму подобную опасность. В отличие от них для персональных компьютеров на рынке пока еще не много аппаратных и программных средств, предупреждающих потери данных или несанкционированный доступ к ним. Положение усугубляется еще и тем, что сами пользователи не осознают в достаточной мере возможной опасности, связанной с обработкой данных на ПЭВМ. В самом деле, информация, хранящаяся в центрах обработки данных, представляет собой, как правило, не поддающиеся непосредственному восприятию необработанные данные, требующие инженерного анализа и структурирования перед их использованием, в то время как личная информация пользователя содержит преимущественно уже оформленные, готовые к использованию оперативные данные.

Необходимо учитывать и специфические особенности ПЭВМ: персональные компьютеры − это небольшие системы (часто портативные) для непосредственной обработки и подготовки текстов с автоматизированным составлением документации для последующего ее редактирования и печатания. Они используются также для подготовки чертежей, распределения и передачи данных другому пользователю в рамках локальной сети. Несмотря на присущие им некоторые ограничения

в скорости обработки данных и возможности расширения памяти, по своей производительности они относятся к системам обработки данных в реальном масштабе времени. Очевидно, что безопасность любой компьютерной системы зависит в первую очередь от ее аппаратных и программных средств и от их взаимодействия. Поэтому предусмотренные в самой аппаратуре (встроенные) или установленные в непосредственной близости от нее внешние средства безопасности обеспечивают более высокий уровень ее, нежели меры безопасности, принимаемые уже после утечки информации. При разработке эффективных мер и средств защиты аппаратных и программных средств должны быть учтены все уязвимые места процедуры обработки данных на ПЭВМ, которые следует устранить или свести к минимуму еще на стадии проектирования.

Косвенную опасность представляет собой все электрооборудование, включенные электронные приборы и устройства, подверженные электрическому или электромагнитному воздействию. Выдаваемые ими электромагнитные сигналы могут быть перехвачены и расшифрованы. Между каналами связи могут возникнуть перекрестные помехи или произойти утечка данных и перехват другим каналом связи. Утечка данных возможна в результате несанкционированного доступа к системам обработки данных, центральному процессору и другим устройствам (включая принтер, жесткие и гибкие диски, магнитные ленты и т.д.). Источником утечки данных могут оказаться и программные средства, так как существует возможность изменения готовых программ или использования собственных программ пользователя при санкционированном доступе к ним.

Главным объектом «атаки» является устройство контроля доступа, предусмотренное для систем обработки данных, которое злоумышленники стремятся любым способом обойти или отключить для получения доступа к секретным данным. Однако поскольку большинство ПЭВМ не имеет

таких систем контроля доступа, возможность незаконного получения важных данных упрощается. Она может быть реализована путем применения хранимых программ (например, сервисных или подобных им) для копирования данных.

Конфиденциальные сведения могут быть получены при несанкционированном использовании пароля. Они могут быть получены и непреднамеренным путем, например при чистке памяти только путем считывания логически обрушенных файлов, содержащихся в оперативной памяти ЭВМ или в периферических и внешних запоминающих устройствах (магнитные лепты, гибкие и жесткие диски и т. д.).

Другими объектами доступа к данным могут служить копии или распечатки или же данные более общего характера, сброшенные безо всякого учета и контроля. Их анализ может позволить получить ценные сведения.

Полная сохранность информации при использовании ПЭВМ, очевидно, возможна лишь в том случае, если с ними работает персонал, заслуживающий полного доверия, и если существует хорошо продуманная всеобщая система информационной защиты, реализуемая в рамках всей фирмы или государственного учреждения, одним из важнейших аспектов которой должно стать определение степени конфиденциальности всех обрабатываемых данных с учетом следующих моментов:

- данные, накопленные в файлах, должны оцениваться, как более важные, нежели единичные;
- объединенные в массив данные также классифицируются выше, чем единичные;
- отдельные части файлов оцениваются по их большей или меньшей конфиденциальности;
- высшую степень секретности должны получать комбинации файлов различных ПЭВМ или из различных отделов фирмы.

- Всеобщая система информационной защиты должна предусматривать и другие меры безопасности, в частности следующие:
- запрет несанкционированного доступа к конфиденциальным данным и ПЭВМ;
- ограничение доступа к особо важным данным (доступ может быть разрешен лишь ограниченному числу лиц);
- все ежедневные информационные операции на ПЭВМ должны регистрироваться с указанием личности пользователя, времени работы и применяемой программы, а также сопровождаться анализом этих сведений.

Все требования по обеспечению информационной защиты должны быть систематизированы и изданы в качестве руководства (или инструкции), обязательного для исполнения каждым пользователем учреждения или фирмы с обязательным указанием степени конфиденциальности обрабатываемой и хранимой информации и уязвимых мест. В идеальном варианте система защиты может охватывать все сферы работы с ПЭВМ. Для всех уровней пользователей, начиная с верхних эшелонов и кончая рядовыми работниками, должны быть созданы специальные учебные программы и тренинги. Вся общая система информационной защиты должна периодически пересматриваться и обновляться с учетом изменившихся условий.

Наряду с предупредительными мерами система должна включать и ряд конкретных контрмер чисто технического характера, максимально учитывающих особенности ПЭВМ и условия их работы. Прежде всего нужно иметь в виду, что по выполняемым функциям ПЭВМ во многом сходны с большими ЭВМ: они могут обрабатывать миллионы различных команд за удивительно короткий промежуток времени, используют те же периферийные аппаратные средства и компоненты, в них могут быть предусмотрены внутренние защитные средства, такие, как средства

мультипрограммирования, программирования по привилегированной команде и защиты памяти. В то же время они значительно меньше больших ЭВМ по своим габаритам, что обеспечивает их высокую мобильность. С ПЭВМ должен работать только один пользователь, являющийся одновременно оператором, системным прикладным программистом, администратором БД и охранным администратором. Он также должен вести фактический учет всех микрокомпонентов, принимая во внимание порядковые номера, технические описания системы и ее блоков, все текущие изменения и добавления.

Каждая система должна проходить периодическую проверку и инвентаризацию. Инвентаризационный список должен проверяться соответствующим уполномоченным работником службы охраны данных по возможности чаще. Кроме того, доступ в помещения, где находятся ПЭВМ, должен быть ограничен, они должны запираться (для этого предусмотрены специальные ключи). Посетители и обслуживающий персонал могут иметь доступ в эти помещения в сопровождении уполномоченных лиц. Идеальным вариантом является наличие в конструкции ПЭВМ встроенного запорного механизма, открываемого вручную, или уставка электронного средства безопасности.

Все аппаратные средства ПЭВМ должны быть надежно экранированы от всяких манипуляций, т.е. изолированы таким образом, чтобы любая попытка доступа к ним становилась очевидной. Должна быть защита во всех местах доступа, апертурах и каналах связи для использования дополнительной памяти.

В зависимости от степени секретности данных целесообразно предусмотреть систему сигнализации для обзора контрольной зоны ПЭВМ и других ее компонентов.

Для защиты данных, хранимых на сменных или фиксированных носителях (например, гибких или жестких дисках), от возможного

копирования с постоянного носителя на гибкий диск или кражи самого диска щелевое отверстие дисковода должно запираться ключом.

Одной из мер безопасности, предупреждающей несанкционированный доступ к носителям, является шифрование пользователем всех данных с помощью встроенного или дополнительного аппаратного средства. Диски, дискеты, магнитные ленты и другие носители должны иметь маркировку, указывающую на степень секретности содержащихся в них сведений (например, очень удобны цветные дискеты с метками различных размеров. Можно использовать для этой цели порошок, чувствительный к ультрафиолетовым лучам, который добавляется в жидкий лак, наносимый на поверхность корпуса дискеты в виде специального рисунка. Полученная метка является невидимой, ее можно обнаружить с помощью ультрафиолетовой лампы и сравнить с личным клеймом пользователя. Совместное пользованием гибкими дисками недопустимо, может быть разрешено лишь совместное пользование жесткими носителями, если предусмотрена система контроля доступа.

В связи с этим возникает проблема остаточной информации в памяти или на носителе. Команды «стирания» большинства ОС лишь обеспечивают соответствующую отметку в каталоге файлов – они не уничтожают данные физически и не обеспечивают перезапись данных по специальному образцу. Операция обратного преобразования этих индикаторов для получения важных данных сравнительно проста. Проблема может быть решена с помощью пользовательской или любой имеющейся программы, которые обеспечивают перезапись всех файлов данных по специальному образцу в распределенную длину.

Для безопасного хранения банков данных и носителей необходимо иметь библиотекаря, ответственного за сохранность библиотеки данных.

Он должен контролировать все входящие и исходящие данные, регистрировать их в специальном журнале, допускать к носителям данных только лиц, имеющих разрешение, следить за своевременным возвратом носителей.

Обеспечение безопасности работы ПЭВМ предполагает проведение регулярной проверки действующих программных средств на основе уже имеющихся данных для оценки правильности выполняемых расчетов и выводимых формул. Контроль предполагает хранение результатов проверки для последующей проверки вариантов, выданных пользователем, на основе тех же исходных данных. Для большей надежности рекомендуется закрепить за каждой ПЭВМ свои собственные проверенные программные средства, доступ к которым возможен только через библиотекаря. Результаты программирования должны выдаваться только в преобразованном или транслированном вариантах; пользователь не должен иметь доступ к исходной программе.

Идеальным вариантом информационной защиты ПЭВМ является интеграция средств контроля доступа в ее ОС. Система контроля доступа как ресурс должна включать четкую организацию проверки пользователей по паролю в соответствии со списком пользователей, имеющих доступ к ОС.

И наконец, все виды операций, выполняемых на ПЭВМ, должны строго учитываться и периодически проверяться.

Ввиду обилия и разнообразия вносимых в регистрационные журналы данных очевидна необходимость копирования всех регистрируемых записей с занесением их в резервный носитель, находящийся в ведении служащего безопасности, а также включения в систему информационной защиты средств автоматизированного анализа этих данных для их эффективной оценки.

Несомненно, что такая универсальная система информационной защиты, включающая и ряд электронных устройств, может повлиять на характеристики ПЭВМ и несколько снизить ее эффективность. Но это единственный путь создания надежной защиты при обработке важных информационных данных.

## Тема 9. Современные технические средства защиты информации от несанкционированного доступа в сетях ЭВМ

### *Методы и средства зашиты информации от несанкционированного доступа в сетях ЭВМ*

*Современный подход к обеспечению сетевой зашиты информации*

В настоящее время все больше стирается грань между ЛВС и региональными глобальными сетями. Современные сетевые ОС, такие, как NetWare версии 4.x фирмы «Novell» или Vines версии 4.11 фирмы «Banyan Systems», позволяют поддерживать функционирование ЛВС с выходом на региональный уровень. Наличие в сетях серверов удаленного доступа приближает их по характеристикам к глобальным сетям.

Постоянно растущие технические возможности ЛВС, построенных на базе ПЭВМ, требуют расширения, усложнения, совершенствования методов защиты информации в них. Однако в силу высокой структурной сложности, пространственной распределенности и разнообразия режимов функционирования вычислительных сетей используемое ПО и обрабатываемая в них информация может оказаться весьма уязвимой.

Сложности, возникающие при организации защиты информации в сетях ЭВМ, обусловлены большими размерами и сложностью систем.

Основные факторы, оказывающие существенное влияние на безопасность распределенных систем, которые необходимо учитывать при выборе и создании средств защиты, таковы:

1. Большое количество разнообразных субъектов, имеющих доступ к системе. Количество пользователей и персонала различных категорий, имеющих доступ к ресурсам сети, может достигать значительной величины. Во многих случаях доступ к сети могут иметь неопределенное количество неконтролируемых лиц.

2. Значительный объем ресурсов сосредоточенных в сети. Концентрация в БД больших объемов информации наряду с возможностью размещения необходимых пользователю данных в различных удаленных узлах сети.
3. Большое количество и разнообразие средств, наличие оборудования разных производителей. Хотя производители обычно декларируют свою приверженность стандартам, на практике функционирование оборудования разных фирм в одной системе может оказаться слабо совместимым.
4. Большой объем программного обеспечения, сложность и многоуровневость ПО, высокая степень разнообразия, наличие в сети ПО разных производителей.
5. Большое разнообразие вариантов доступа. Требуется обеспечить большое количество разнообразных вариантов доступа к ресурсам сети. Это определяется большим числом ресурсов в сети, большим числом пользователей сети и разнообразием их потребностей.
6. Значительная территориальная разнесенность элементов сети. Узлы системы могут находиться на большом расстоянии друг от друга, возможно и разных странах. Наличие протяженных линий связи.
7. Интенсивный обмен информацией между компонентами сети.
8. Совместное использование ресурсов. Совместное использование большого количества ресурсов значительным количеством пользователей увеличивает риск несанкционированного доступа (НСД).
9. Распределенная обработка данных (технология клиент-сервер). Распределенная обработка информации требует согласованного совместного функционирования нескольких узлов сети. Это приводит к появлению дополнительных возможностей для НСД и

возникновению несогласованности в данных, расположенных в разных узлах

10. Расширенный объем контроля.
11. Практически бесконечное множество комбинаций различных программных аппаратных средств и режимов их работы. Соединение в сеть нескольку систем, даже однородных по характеру, увеличивает уязвимость систем, в целом. Каждая отдельная система настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимыми с требованиями других систем. В случае соединения разнородных систем риск повышается[1,6].
12. Неизвестный периметр. Легкая расширяемость сетей ведет к тому, что определить границы сети подчас сложно; один и тот же узел может быть доступен пользователям разных сетей. Более того, для многих из них всегда можно определить, сколько пользователей имеют доступ к определенному узлу и кто они. Границы системы становятся неопределенными, особенно при необходимости обеспечения доступа по коммутируемым линиям связи.
13. Множество точек атаки. Данные могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Размерность множества возможных точек атаки многократно возрастает при наличии доступа по коммутируемым линиям связи. Такой способ легко реализуем, но трудно контролируем: он считается одним из наиболее опасных. Линии связи и коммутационное оборудование относятся к наиболее уязвимым местам сети.
14. Сложность управления и контроля доступа к системе. Атаки на сеть могут осуществляться без получения физического доступа к определенному узлу, а из удаленных точек. В этом случае проведение идентификации может оказаться очень сложной задачей. Кроме того,

время атаки может оказаться слишком мало для принятия адекватных мер защиты.

Защищать сеть необходимо от таких угроз, как:

- считывание данных в массивах других пользователей;

- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

- копирование носителей информации с преодолением мер защиты;

- маскировка под зарегистрированного пользователя;

- мистификация (маскировка под запросы системы);

- использование программных ловушек;

- использование недостатков языков программирования и ОС;

- включение в библиотеки программ специальных блоков типа «троянского коня» (называемых в некоторых источниках «троянскими программами»);

- злоумышленный вывод из строя механизмов защиты;

- внедрение и использование компьютерных вирусов.

В системе защиты сети каждый ее узел должен иметь индивидуальную защиту в зависимости от выполняемых функций и возможностей сети, на каждом отдельном узле необходимо организовать:

- администрирование системы защиты (обеспечение включения данных по санкционированным пользователям в БД системы защиты, в том числе идентификатор пользователя, данные (зашифрованные) о паролях и/или других идентифицирующих пользователя параметрах, данные по правам доступа);

- идентификацию и аутентификацию пользователей, получающих доступ к данному узлу из сети;

- контроль доступа ко всем файлам и другим наборам данных, доступным из локальной сети и других сетей;

- контроль сетевого трафика (объем информации, передаваемый за определенное время по какому-то или по нескольким каналам);

- контроль доступа к ресурсам локального узла, доступным для применения пользователями сети;

- контроль за распространением информации в пределах локальной сети и связанных с нею других сетей.

В структурно-функциональном составе сети, как правило, принято выделять следующие компоненты:

- рабочие станции или удаленные абонентские пункты сети;

- серверы (хост-машины) – высокопроизводительные ЭВМ, поддерживающие сетевые службы управления файлов, печати, БД и т.п.;

- межсетевые шлюзы (мосты, центры коммутации пакетов), обеспечивающие прозрачное соединение нескольких сетей передачи данных либо нескольких сегментов одной и той же локальной сети, имеющих различные протоколы взаимодействия;

- каналы связи (локальные, телефонные коммутируемые каналы).

Первые 3 компонента могут строиться на базе ПЭВМ с использованием специального программного обеспечения. Для защиты данных компонентов от побочных электромагнитных излучений и наводок применимы требования и рекомендации, используемые для ПЭВМ, обрабатывающих конфиденциальную информацию [1, 6].

Для обработки конфиденциальной информации необходимо использовать ПЭВМ, которые прошли специальные исследования и защищены по их результатам.

Вопрос о необходимости и достаточности мер защиты ПЭВМ решается по результатам их специальных исследований и на основании анализа условий расположения здания, размера контролируемой (проверяемой) зоны, типа и состава ПЭВМ, а также состава вспомогательных технических средств.

Структурно-функциональный состав сети в значительной степени влияет на средства защиты программного и информационного обеспечения. Программные средства защиты при этом могут быть как комплексными, предназначенными для всей сети в целом (например, такие, как штатные средства защиты сетевых ОС), так и единичными, ориентированными на обеспечение безопасности отдельных компонентов.

Важным требованием, предъявляемым к средствам защиты, может служить их функциональная полнота.

Можно выделить следующие основные функции защиты программного и информационного обеспечения, характерные для вычислительной сети как сложного объединения средств электронно-вычислительной техники:

- администрирование сети;
- обеспечение идентификации и аутентификации пользователей;
- разграничение доступа к ресурсам сети;
- очистка «мусора»;
- обеспечение защиты данных, передаваемых между элементами сети;
- регистрация действий, требующих доступа к защищаемым ресурсам, выявление фактов нарушений;
- контроль целостности (корректности процесса изменения состояний) наиболее важных компонентов программного и информационного обеспечения вычислительной сети.

Администрирование – один из очевидных и первых встроенных в систему компонентов, который обеспечивает основу системы безопасности сети. Администратор сети создает новых пользователей, назначает им права, возможное время и возможные рабочие станции для доступа, устанавливает лимиты ресурсов сети. Гибкие средства администрирования позволяют эффективно управлять ресурсами сети и доступом пользователей к ним.

Средства администрирования сети должны обеспечивать возможность включения в БД системы защиты данных о пользователях, в том числе идентификатора пользователя, паролей и других параметров, применяемых для аутентификации пользователей, данных о правах пользователя и т.д. Для больших сетей отсутствие развитых средств делает администрирование трудно решаемой, изобилующей ошибками задачей.

Целью аутентификации является идентификация пользователя перед предоставлением ему доступа к информации в сети. Для работы с файлами, директориями и утилитами, находящимися в сети, пользователь должен получить, разрешение от ОС. Если необходимо, пароли могут быть зашифрованы перед передачей по каналу и перед записью на диск. Могут быть установлены минимальная длина пароля, требования периодической смены пароля и уникальности пароля.

Периодическая смена паролей пользователями уменьшает риск их раскрытия, а большая длина паролей затрудняет разгадывание. Возможность регистрации пользователей может быть ограничена по времени (например, только рабочее время) и месту (только с определенных рабочих станций). Набор средств, определяющий (образующий) уровень проверки полномочий, применяющий идентификатор и пароль пользователя, является базовым средством защиты в любой сети. Первое, на что необходимо обратить внимание при защите сети, – это аутентификация. Без нее нельзя управлять полномочиями, доступом или поддерживать контрольный журнал. В любом случае первая задача при предоставлении доступа – это подтверждение прав на него. Обеспечение контроля доступа в вычислительных сетях заключается в управлении доступом к ресурсам сети. Эта функция должна быть реализована путем проверки подлинности пользователей при начале работы с сетью (идентификация и аутентификация пользователя), проверки подлинности при соединениях (контроль соединений) и собственно организацией

контроля разграничения) доступа (контроль передаваемой информации, управление файлами, контроль прикладных программ).

Идентификация и аутентификация пользователя при начале работы с сетью основываются на системе паролей, на значения которых должны накладываться различные условия, либо их генерация должна осуществляться с помощью специальных средств. При задании паролей пользователями они должны проверяться на возможность их легкого угадывания. Более подробно рекомендации по использованию паролей рассмотрены ниже.

Для проверки подлинности при работе с удаленных рабочих станций нужно использовать модемы «с обратным вызовом» или коммуникационные пакеты, реализующие это программно с помощью стандартных модемов.

В общем случае необходимым условием обеспечения требуемого уровня защищенности от НСД процедуры аутентификации удаленных пользователей является применение средств шифрования на основе индивидуальных и открытых ключей. Корректное применение средств шифрования в комплексе с другими средствами позволяет обеспечить необходимый уровень защиты данных.

Путем разграничения доступа устанавливается факт, разрешено или нет пользователю иметь доступ к некоторому ресурсу сети.

Механизмы разграничения доступа могут охватывать как объекты ЛВС в целом (серверы, сетевые печатающие устройства и т.д.), так и объекты на файл-сервере (процессы, файлы, атрибуты файлов и т.д.).

Разграничение доступа к ресурсам вычислительной сети реализуется, как правило, на нескольких уровнях.

Для обеспечения защиты данных, передаваемых между элементами сети, необходимо осуществлять меры:

- по предотвращению раскрытия содержимого передаваемых сообщений;
- предотвращению анализа потоков сообщений, потоков информационного обмена (трафика);
- предотвращению и выявлению попыток модификаций потока сообщений;
- предотвращению и обнаружению прерываний передачи сообщений;
- обнаружению инициирования ложного соединения.

Для решения задачи по обеспечению защиты данных, передаваемых между элементами сети, хранения критических данных на долговременных запоминающих устройствах, защиты целостности программного обеспечении сообщений используются криптографические методы.

Средства регистрации для вычислительных сетей должны обеспечивать возможность автоматического протоколирования обращений к системе разграничения доступа как легальных, так и попыток несанкционированного доступа к ресурсам сети. Средства регистрации должны обеспечивать возможность сбора информации о нарушениях в масштабах всей сети. Доступ к журналам регистрации должен быть ограничен средствами разграничения.

Для поддержания средств регистрации и анализа собранной в них информации должны быть разработаны процедуры, построенные на сочетании программных средств обработки и организационных мер безопасности.

Применение метода контроля целостности в условиях сети значительно расширяется и усложняется в реализации, так как помимо контроля информации, важной с точки зрения защиты на отдельных компьютерах сети, необходимо контролировать целостность сетевого программного обеспечения.

Помимо этого, в связи с распространением компьютерных вирусов возрастаем значение данного метода как одного из средств антивирусной защиты ЛВС.

До недавнего времени, несмотря на наличие программных средств защиты, претендовавших при соответствующей настройке на универсальное решение задач безопасности сети, сетевые ОС реально не обеспечивали сколько-нибудь приемлемого уровня защищенности систем. По шкале федеральных стандартов США, принятых Национальным центром компьютерной безопасности, средства защиты сетевых ОС в лучшем случае располагались на нижних отметках. В настоящее время появились сетевые ОС, получившие сертификат уровня С2. Примером такой ОС является NetWare 4.1.

*Современные технические средства сетевой зашиты компьютерной информации*

Достижения новых информационных технологий позволили сегодня создать целый ряд необходимых инструментальных средств реализации механизмов защиты. Здесь под инструментальными средствами понимаются программные, программно-аппаратные и аппаратные средства, функциональное наполнение которых позволяет эффективно решать поставленные перед службой безопасности задачи информационной защиты. Современный рынок предлагает достаточно широкий спектр технических средств контроля безопасности сети, основные из которых представлены на рисунке 9.1.

Реализацию механизмов защиты от атак в современных компьютерных сетях обеспечивают межсетевые экраны. Этот класс продуктов производит анализ всего входящего и исходящего трафика, сравнивая его с данными БД типовых атак и настроек правил

безопасности, и лишь после этого отправляет адресату. Попытки атак как из внешней сети, так и из локальной сети предотвращаются и протоколируются. Настройки и функции управления межсетевым экраном производятся с рабочего места администратора сети. В том направлении можно отметить эффективные разработки компании «Network-1» (мультипротокольный межсетевой экран Firewall/Plus).


Рис. 9.1. Технические средства контроля уровня безопасности компьютерной сети

Автоматизировать процессы настроек ОС помогают системы аудита безопасности серверных платформ. Система OmniGuard/ Enterprise Security Manager компании «Axent» предназначена для анализа и контроля уровня

безопасности гетерогенных сетей Netware, Windows NT, Unix. Основным назначением системы является поиск уязвимостей текущих настроек ОС, которые могут использоваться злоумышленником для получения НСД. Система автоматически анализирует настройки сети, контролирует изменения, произошедшие с момента предыдущего анализа.

Основным недостатком систем классического аудита является то, что между фиксацией события и анализом проходит определенное время. Системы аудита безопасности реального времени, примером которых служит OmniGuard/Intruder Alert компании «Axent», функционируют по принципиально иной схеме. Основное назначение таких систем – эффективный, круглосуточный и круглогодичный мониторинг безопасности и аудита локальных и распределенных сетей в режиме реального времени.

Известно, что большинство атак связано со своими пользователями. Поэтому защита рабочих станций от НСД с функциями разграничения прав и протоколизацией действий пользователей, с антивирусной защитой представляет собой необходимый элемент обеспечения комплексной безопасности. Среди современных средств защиты от НСД можно отметить программно-аппаратный комплек Dallas Lock for Administrator с использованием электронных идентификаторов iButton (Touch Memory) или Proximity-карт. Этот же комплекс производит настройку и управление, анализ протоколов, просмотр экранов рабочих станций и многое другое.

Как правило, современные инструментальные средства строятся на базе программно-аппаратных технологий. В настоящее время наибольшее применение инструментальные средства находят в следующих направлениях: генерация тестов, имитация угроз, анализ текстов программ.

Методы применения генераторов тестов достаточно хорошо отработаны и широко используются при проведении испытаний функциональных возможностей информационных систем. Генераторы

стохастических тестов эффективно применяются прежде всего при исследовании качества и надежности функционирования информационных систем. В приложении к анализу безопасности информационных технологий более удобными являются генераторы целенаправленных тестов. Помимо испытаний функциональных механизмов безопасности, областью применения генераторов тестов является также анализ текстов программ для выявления недекларированных возможностей и закладных элементов.

Имитаторы угроз предназначены для натурного моделирования воздействования на информационные технологии типовых угроз. Посредством имитаторов угроз проверяются механизмы от программных вирусов, средства экранирования от проникновения из внешних вычислительных сетей и т.д.

Наиболее сложной областью применения инструментальных средств является исследование недекларированных возможностей информационных технологий, поиск закладных устройств и анализ уязвимых мест в ПО.

Для автоматизации исследования исходных текстов программ применяются статические и динамические анализаторы. Статические анализаторы предназначены для оценки корректности структуры построения программ, выявления участков программного кода, в которых отсутствует обращение установления точек входа и выхода из программ, не предусмотренных спецификациями, проверки полноты описания и использования программных переменных, поиска специальных программных конструкций, которые могут быть идентифицированы как программные закладки. Динамические анализаторы используются для трассировки выполнения программ, выявления критических путей, оценки полноты покрытия возможных ветвей программ при функциональном тестировании.

Создание анализаторов исходных текстов программ представляет собой сложную задачу. Опыт применения анализаторов программ показал их исключительно высокую эффективность. Время проведения анализа программы сокращается практически на порядок, результаты анализа документируются, что обеспечивает их контроль и, при необходимости, повторение.

Постоянное изменение состояния сети (появление новых рабочих станций, реконфигурация их программных средств и т.д.) может привести к появлению новых угроз и уязвимых мест в системе защиты. В связи с этим особенно важно своевременное их выявление и внесение изменений в соответствующие настройки комплекса и его подсистем (в том числе и подсистемы защиты). Помочь в этом случае могут специальные средства анализа ее защищенности. Они позволяют оперативно проверить десятки и сотни территориально разнесенных узлов сети. При этом они не только выявляют большинство угроз и уязвимых мест информационной системы, но и предлагают рекомендации администратору безопасности по их устранению. Подобное ПО, получившее название сканера безопасности, по сути, воспроизводит действия хакера, моделируя всевозможные атаки на сетевые ресурсы и выявляя уязвимости в тестируемой системе до того, как их обнаружит хакер.

Первым и до сих пор используемым средством сканирования сетей была система, относящаяся к категории freeware (свободно распространяемого ПО) – Security Administrator Tool for Analyzing Networks (SATAN). Эта система работает под управлением ОС Unix и осуществляет проверку любой компьютерной сети, подключенной к Интернету. SATAN сообщает пользователю этой сети об уязвимых местах и предлагает способы их устранения. Наличие удобного пользовательского интерфейса облегчает доступ ко всем сервисным возможностям программы.

До запуска SATAN необходимо установить параметры проверки, заполнив несколько простых форм. В них указывается имя файла для хранения собранных данных и определяются рабочие характеристики программы. Например, определяются компьютеры, подлежащие проверке, и то, насколько глубоко она должна проводиться. В зависимости от сделанного выбора и размера сети проверка может занять от нескольких минут до часа. SATAN информирует о потенциально опасных сетевых услугах, способных поставить под угрозу безопасность работы Интернета, определяет уязвимые места в средствах защиты и предлагает советы по их устранению.

Конечно, наличие хорошо документированной информации к программе вызывает опасения, что SATAN будет использоваться хакерами для выявления уязвимых мест в средствах защиты. Однако именно благодаря этой программе все больше системных администраторов стали всерьез беспокоиться о повышении безопасности сетей. К тому же SATAN устроена так, что как только выявляется проблема в обеспечении безопасности, сразу дается ссылка на соответствующее место в документации, разъясняющее, каким образом хакер может воспользоваться этой слабостью.

В результате исследования защищенности почти 2 тыс. узлов с помощью программы SATAN выявлено, что около двух третей протестированных узлов потенциально уязвимы для хакерских атак из-за наличия известных документированных, но не исправленных администраторами изъянов.

В настоящее время на рынке присутствует большое количество продуктов, относящихся к категории средств поиска уязвимости сетей, некоторые из которых представлены в таблице 9.1.

Таблица 9.1. Средства поиска уязвимости сетей (сканеры безопасности)

| Наименование продукта | Фирма-производитель |
|---|---|
| Internet Security Scanner | Internet Security Sistems |
| NetRecon | Axent |
| NetProbe | Qualix |
| Baltista | Secure Networks |
| NetGuard | Network Guardians |
| NetSonar | WheetGroup |

Основные свойства и возможности сканеров безопасности покажем на примере сканера NetSonar фирмы «WheelGroup». В отличие от многих других продуктов сканер NetSonar способен не только идентифицировать IP-адреса в сети, но и распознавать хосты (в том числе их ОС) и сетевые устройства, такие, как коммутаторы или маршрутизаторы. Сканер обеспечивает следующие категории распознаваемых сетевых устройств: Unix-хосты, Windows NT-хосты, Web-серверы, FTR-серверы, Mail-серверы, межсетевые экраны, маршрутизаторы, коммутаторы. Процесс тестирования одного хоста занимает лишь несколько минут. Большим достоинством данного сканера является то, что администратор может посредством специализированного языка Vulnernet Description Language самостоятельно моделировать атаки. По результатам тестирования формируется отчет, содержащий всю необходимую информацию об обнаруженных уязвимостях и рекомендации по их устранению.

В настоящее время для анализа защищенности IP-сетей (в частности, Интернет) наибольшей популярностью пользуются продукты американской компании «Internet Security Systems» (http://www.iss.net), входящие в семейство SAFEsuite: Internet Scanner и System Security Scanner.

Internet Scanner предназначен для определения уязвимых мест в средствах защиты Web-серверов, межсетевых экранах (firewall), серверах и рабочих станциях, работающих под управлением ОС Windows NT, SunOS, Solaris, Linux, HP UX, Windows 95 и т.д. Принцип работы Internet Scanner основан на моделировании известных методов, используемых для несанкционированного проникновения в компьютерные системы. База данных, содержащая информацию о вариантах взлома сети, постоянно пополняется и на настоящий момент содержит сведения о более чем 300 методах.

Результатом работы программ, входящих в систему Internet Scanner, является отчет о найденных уязвимых местах анализируемого модуля сети (межсетевые экраны, Web-сервер и т.д.). Также по требованию администратора в отчет включается перечень необходимых для повышения уровня защищенности системы мер. Информация в созданном отчете может быть отсортирована по ряду признаков (по степени риска, типу угроз и т.д.) Он может быть представлен как в текстовом, так и в HTML-форматах. По желанию администратора созданные отчеты могут быть сохранены в БД для их последующего сравнения и анализа.

Система Internet Scanner состоит из трех подсистем: Web Security Scanner, Firewall Scanner, Intranet Scanner. Рассмотрим их более подробно.

Подсистема Web Security Scanner предназначена для тестирования внешних и локальных WWW-серверов. В процессе анализа подсистема Web Security Scanner проверяет настройки сервера, его файловый модуль, HTML-страницы, соответствующие сервисы WWW-сервера: RPC, NFS, Send-Mail, X Windows, Netbios, Rsh и Rlogin, CGI-скрипты, Finger, а также те блоки, которые могут быть использованы злоумышленником для взлома.

Firewall Scanner предназначен для тестирования межсетевых экранов (как снаружи корпоративной сети, так и изнутри ее), операционной

системы, под управлением которой он работает, и прикладных программ, доступных через него. Подсистема позволяет проверять сервисы, доступные через межсетевые экраны, правила фильтрации и т.п.

Подсистема Intranet Scanner применяется для тестирования любого устройства, имеющего IP-адрес (рабочая станция, сервер, интеллектуальный принтер и т.п.), и определения тех их настроек, которые могут быть использованы злоумышленником для взлома сети.

System Security Scanner предназначена для контроля защищенности отдельных ЭВМ, хостов, работающих под управлением ОС Unix (в ближайшее время появится версия для Windows NT). В процессе анализа она сверяет права доступа одного или нескольких пользователей по отношению к системным и прикладным файлам. При этом фиксируются наличие «троянских коней», настройки ОС, целостность файлов и паролей, признаки взлома анализируемого компьютера и т.п. Отличительной особенностью данной системы является возможность оперативного устранения выявленных недостатков.

Таким образом, в настоящее время инструментальные программно-аппаратные средства являются весьма эффективными и перспективными для использования в компьютерных сетях. Проведенный анализ угроз и методов защиты от них показал, что использование современных достижений информационных технологий в настоящее время позволяет обеспечить требуемый уровень безопасности, однако для этого необходимо выполнить ряд условий, в том числе обеспечить комплексный подход, непрерывность контроля, постоянное совершенствование защиты путем перманентного внедрения новых информационных технологий.

# Тема 10. Основные понятия теории моделирования больших систем. Математическое моделирование больших систем на основе математических моделей:D-схем и Q-схем

## *Математические схемы моделирования систем*

*Основные подходы к построению математических моделей систем*

Исходящей информацией при построении математических моделей процессов функционирования систем служат данные о назначении и условиях работы исследуемой (проектируемой) системы S. Эта информация определяет основную цель моделирования системы S и позволяет сформулировать требования к разрабатываемой математической модели М. Причем уровень абстрагирования зависит от круга тех вопросов, на которые исследователь системы хочет получить ответ с помощью модели, и в какой-то степени определяет выбор математической схемы [7].

Математическую схему можно определить как звено при переходе от содержательного к формальному описанию процесса функционирования системы с учетом воздействия внешней среды, т.е. имеет место цепочка «описательная модель – математическая схема – математическая (аналитическая или (и) имитационная) модель».

Модель объекта моделирования, т.е. системы S, можно представить в виде множества величин, описывающих процесс функционирования реальной системы и образующих в общем случае следующие подмножества: совокупность входных воздействий на систему

$$x_i \in X,\ i = \overline{1, n_x};$$

совокупность воздействий внешней среды

$$v_l \in V,\ l = \overline{1, n_V};$$

совокупность внутренних (собственных) параметров системы

$$h_k \in H,\ k = \overline{1, n_H};$$

совокупность выходных характеристик системы

$$y_j \in Y,\ j = \overline{1, n_Y};$$

$$h_k \in H,\ k = \overline{1, n_H}.$$

Причем в перечисленных подмножествах можно выделить управляемые и неуправляемые переменные. В общем случае $x_j$, $v_l$, $h_k$, $y_j$ являются элементами непересекающихся подмножеств и содержат как детерминированные, так и стохастические составляющие.

При моделировании системы S входные воздействия, воздействия внешней среды E и внутренние параметры системы являются независимыми (экзогенными) переменными, которые в векторной форме имеют соответственно вид $\vec{x}(t) = (x_1(t), x_2(t), ..., x_{nX}(t))$; $\vec{v}(t) = (v_1(t), v_2(t), ..., v_{nV}(t))$; $\vec{h}(t) = (h_1(t), h_2(t), ..., h_{nH}(t))$, а выходные характеристики системы являются зависимыми (эндогенными) переменными и в векторной форме имеют вид $\vec{y}(t) = (y_1(t), y_2(t), ..., y_{nY}(t))$.

Процесс функционирования системы S описывается во времени оператором $F_S$, который в общем случае преобразует экзогенные переменные и эндогенные в соответствии с соотношениями вида

$$\vec{y}(t) = F_S(\vec{x}, \vec{v}, \vec{h}, t). \qquad (1)$$

Совокупность зависимостей выходных характеристик системы от времени $y_i(t)$ для всех видов $i = \overline{1, n_Y}$ называется выходной траекторией $\vec{y}(t)$. Зависимость (1) называется законом функционирования системы S и обозначается $F_S$. В общем случае закон функционирования системы $F_S$ может быть задан в виде функций, функционала, логических условий, в

алгоритмической и табличной формах или в виде словесного правила соответствия.

Весьма важным для описания и исследования системы S является понятие алгоритма функционирования $A_S$, под которым понимается метод получения выходных характеристик с учетом входных воздействий $\vec{x}(t)$, воздействий внешней среды $\vec{v}(t)$ и собственных параметров системы $\vec{h}(t)$. Очевидно, один и тот же закон функционирования $F_S$ системы S может быть реализован различными способами, т.е. с помощью множества различных алгоритмов функционирования $A_S$.

Соотношения (1) являются математическим описанием поведения объекта (системы) моделирования во времени t, т.е. отражают его динамические свойства. Поэтому математические модели такого вида принято называть динамическими моделями (системами).

Для статических моделей математическая модель (1) представляет собой отображение между двумя подмножествами свойств моделируемого объекта Y и $\{X,V,H\}$, что в векторной форме может быть записано как

$$\vec{y} = f(\vec{x},\vec{v},\vec{h}). \qquad (2)$$

Соотношения (1) и (2) могут быть заданы различными способами: аналитически (с помощью формул), графически, таблично и т.д. Такие соотношения в ряде случаев могут быть получены через свойства системы S в конкретные моменты времени, называемые состояниями. Состояние системы S характеризуется векторами

$\vec{z}' = (z'_1, z'_2, \ldots, z'_k)$ и $z'' = (\vec{z}''_1, \vec{z}''_2, \ldots, z''_k)$, где $z'_1 = z_1(t')$, $z'_2 = z_2(t')$, … , $z'_k = z_k(t')$ в момент $t'' \in (t_0, T)$; $z''_1 = z_1(t'')$, $z''_2 = z_2(t'')$, … , $z''_k = z_k(t'')$ в момент $t'' \in (t_0, T)$ и т.д., $k = \overline{1, n_Z}$.

Если рассматривать процесс функционирования системы S как последовательную смену состояний $z_1(t)$, $z_2(t)$, … , $z_k(t)$, то они могут быть интерпретированы как координаты точки в k-мерном фазовом

пространстве. Причем каждой реализации процесса будет соответствовать некоторая фазовая траектория. Совокупность всех возможных значений состояний $\{\vec{z}\}$ называется пространством состояний объекта моделирования Z, причем $z_k \in Z$.

Состояние системы S в момент времени $t_0 < t^* \le T$ полностью определяется начальными условиями $\vec{z}^{\,0} = (z_1^0, z_2^0, \ldots, z_k^0)$ [где $z_1^0 = z_1(t_0), z_2^0 = z_2(t_0), \ldots, z_k^0 = z_k(t_0)$], входными воздействиями $\vec{x}(t)$, внутренними параметрами $\vec{h}(t)$ и воздействиями внешней среды $\vec{v}(t)$, которые имели место за промежуток времени $t^* - t_0$, с помощью двух векторных уравнений

$$\vec{z}\,(t) = \Phi\,(\vec{z}^{\,0}, \vec{x}, \vec{v}, \vec{h}, t)\,;$$

$$\vec{y}(t) = F(\vec{z}, t)\,.$$

Первое уравнение по начальному состоянию $\vec{z}^{\,0}$ и экзогенным переменным $\vec{x}, \vec{v}, \vec{h}$ определяет вектор-функцию $\vec{z}(t)$, а второе по полученному значению состояний $\vec{z}(t)$ – эндогенные переменные на выходе системы $\vec{y}(t)$. Таким образом, цепочка уравнений объекта «вход – состояния – выход» позволяет определить характеристики системы

$$\vec{y}(t) = F\left|\Phi\left(\vec{z}^{\,0}, \vec{x}, \vec{v}, \vec{h}, t\right)\right|.$$

В общем случае время в модели системы S может рассматриваться на интервале моделирования (0,T) как непрерывное, так и дискретное, т.е. квантованное на отрезке длиной $\Delta$t временных единиц каждый, когда T=m$\Delta$t, где $m = \overline{1, m_T}$ – число интервалов дискретизации.

Таким образом, под математической моделью объекта (реальной системы) понимают конечное подмножество переменных $\left\{\vec{x}(t), \vec{v}(t), \vec{h}(t)\right\}$ вместе с математическими связями между ними и характеристиками $\vec{y}(t)$.

Если математическое описание объекта моделирования не содержит элементов случайности или они не учитываются, т.е. если можно считать,

что в этом случае стохастические воздействия внешней среды $\vec{v}(t)$ и стохастические внутренние параметры $\vec{h}(t)$ отсутствуют, что характеристики однозначно определяются детерминированными входными воздействиями

$$\vec{y}(t) = f(\vec{x}, t). \qquad (3)$$

Очевидно, что детерминированная модель является частным случаем стохастической модели.

Приведенные математические соотношения представляют собой математические схемы общего вида и позволяют описать широкий класс систем. Однако в практике моделирования объектов в области системотехники и системного анализа на первоначальных этапах исследования системы рациональнее использовать типовые математические схемы: дифференциальные уравнения, конечные и вероятностные автоматы, системы массового обслуживания и т.д.

Не обладая такой степенью общности, как рассмотренные модели, типовые математические схемы имеют преимущества простоты и наглядности, но при существенном сужении возможностей применения. В качестве детерминированных моделей, когда при исследовании случайные факторы не учитываются, для представления систем, функционирующих в непрерывном времени, используются дифференциальные, интегральные, интегродифференциальные и другие уравнения, а для представления систем, функционирующих в дискретном времени, – конечные автоматы и конечноразностные схемы. В качестве стохастических моделей (при учете случайных факторов) для представления систем с дискретным временем используются вероятностные автоматы, а для представления системы с непрерывным временем – системы массового обслуживания и т.д.

Перечисленные типовые математические схемы, естественно, не могут претендовать на возможность описания на их базе всех процессов, происходящих в больших информационно-управляющих системах, к

которым относятся АСУ. Для таких систем в ряде случаев более перспективным является применение агрегативных, обобщенных моделей.

Таким образом, при построении математических моделей процессов функционирования систем можно выделить следующие основные подходы: непрерывно-детерминированный (например, дифференциальные уравнения); дискретно-детерминированный (конечные автоматы); дискретно-стохастический (вероятностные автоматы); непрерывно-стохастический (системы массового обслуживания); обобщенный или универсальный (агрегатные системы) [7].

Мы ограничимся рассмотрением лишь двух подходов – на базе D-схем и Q-схем.

*Непрерывно-детерминированные модели (D-схемы)*

Рассмотрим особенности непрерывно-детерминированного подхода на примере использования в качестве математических моделей дифференциальных уравнений.

Обычно в таких математических моделях в качестве независимой переменной, от которой зависят неизвестные искомые функции, служит время t. Тогда математическое соотношение для детерминированных систем (3) в общем виде будет

$$\vec{y}' = \vec{f}(\vec{y}, t);\ \vec{y}(t_0) = \vec{y}_0,$$

где $\vec{y}' = d\vec{y} / d\vec{t}$, $\vec{y} = (y_1, y_2, \ldots, y_n)$ и $\vec{f} = (f_1, f_2, \ldots, f_n)$ - n мерные векторы; $f(\vec{y}, \vec{t})$ - вектор-функция, которая определена на некотором (n+1)-мерном $(\vec{y}, t)$ множестве и является непрерывной. Так как математические схемы такого вида отражают динамику изучаемой системы, т.е. ее поведение во времени, то они называются D-схемами.

В простейшем случае обыкновенное дифференциальное уравнение имеет вид,

$$y' = f(y,t)$$

Наиболее важно для системотехники приложение D-схем в качестве математического аппарата в теории автоматического управления. Для иллюстрации особенностей построения и применения D-схем рассмотрим простейший пример формализации процесса функционирования двух элементарных систем различной физической природы: механической $S_M$ (колебания маятника, рис. А) и электрической $S_k$ (колебательный контур, рис. Б).

Процесс малых колебаний маятника описывается обыкновенным дифференциальным уравнением

$$m_M l_M^2 \left[ d^2\theta(t)/dt^2 \right] + m_M g l_M \theta(t) = 0,$$

где $m_M, l_M$ - масса и длина подвеса маятника; g – ускорение свободного падения; $\theta(t)$ - угол отклонения маятника в момент времени t.

Из этого уравнения свободного колебания маятника можно найти оценки интересующих характеристик. Например, период колебания маятника

$$T_M = 2\pi\sqrt{l_M / g}$$

где $m_M, l_M$ - масса и длина подвеса маятника; g – ускорение свободного падения; $\theta(t)$ - угол отклонения маятника в момент времени t.

Из этого уравнения свободного колебания маятника можно найти оценки интересующих характеристик. Например, период колебания маятника

$$T_M = 2\pi\sqrt{l_M / g}\,.$$

Аналогично, процессы в электрическом колебательном контуре описываются обыкновенным дифференциальным уравнением

$$L_K\left[d^2q(t)/dt^2\right]+\left[q(t)/C_K\right]=0,$$

где $L_K, C_K$ - индуктивность и емкость конденсатора; q(t) – заряд конденсатора в момент времени t.

Из этого уравнения можно получить различные оценки характеристик процесса в колебательном контуре. Например, период электрических колебаний

$$T_K = 2\pi\sqrt{L_K C_K}\,.$$

Очевидно, что введя обозначения $h_0 = m_M l_M^2 = L_K$, $h_1 = 0$, $h_2 = m_M g l_M = 1/C_K$, $\theta(t) = q(t) = z(t)$, получим обыкновенное дифференциальное уравнение второго порядка, описывающее поведение этой замкнутой системы:

$$h_0\left[d^2z(t)dt^2\right]+h_1\left[dz(t)/dt\right]+h_2z(t)=0, \qquad (4)$$

где $h_0, h_1, h_2$ – параметры системы; $z(t)$ – состояние системы в момент времени t.

Таким образом, поведение этих двух объектов может быть исследовано на основе общей математической модели (4).

Если изучаемая система S, т.е. маятник или контур, взаимодействует с внешней средой E, то появляется входное воздействие x(t) (внешняя сила для маятника и источник энергии для контура) и непрерывно-детерминированная модель такой системы будет иметь вид

$$h_0\left[d^2z(t)/dt^2\right]+h_1\left[dz(t)dt\right]+h_2z(t)=x(t).$$

С точки зрения общей схемы математической модели x(t) является входным (управляющим) воздействием, а состояние системы S в данном случае можно рассматривать как выходную характеристику, т.е. полагать, что выходная переменная совпадает с состоянием системы в данный момент времени y=z.

При решении задач системотехники важное значение имеют проблемы управления большими системами. Следует обратить внимание

на системы автоматического управления – частный случай динамических систем, описываемых D-схемами и выделенных в отдельный класс моделей в силу их практической специфики [1].

Описывая процессы автоматического управления, придерживаются обычно представления реального объекта в виде двух систем: управляющей и управляемой (объекта управления). Структура многомерной системы автоматического управления общего вида представлена на рис. 2, где обозначены эндогенные переменные: $\vec{x}(t)$ – вектор входных (задающих) воздействий; $\vec{v}(t)$ – вектор возмущающих воздействий; $\vec{h}'(t)$ – вектор сигналов ошибки; $\vec{h}''(t)$ – вектор управляющих воздействий; экзогенные переменные: $\vec{z}(t)$ - вектор состояний системы S; $\vec{y}(t)$ – вектор выходных переменных, обычно $\vec{y}(t) = \vec{z}(t)$.

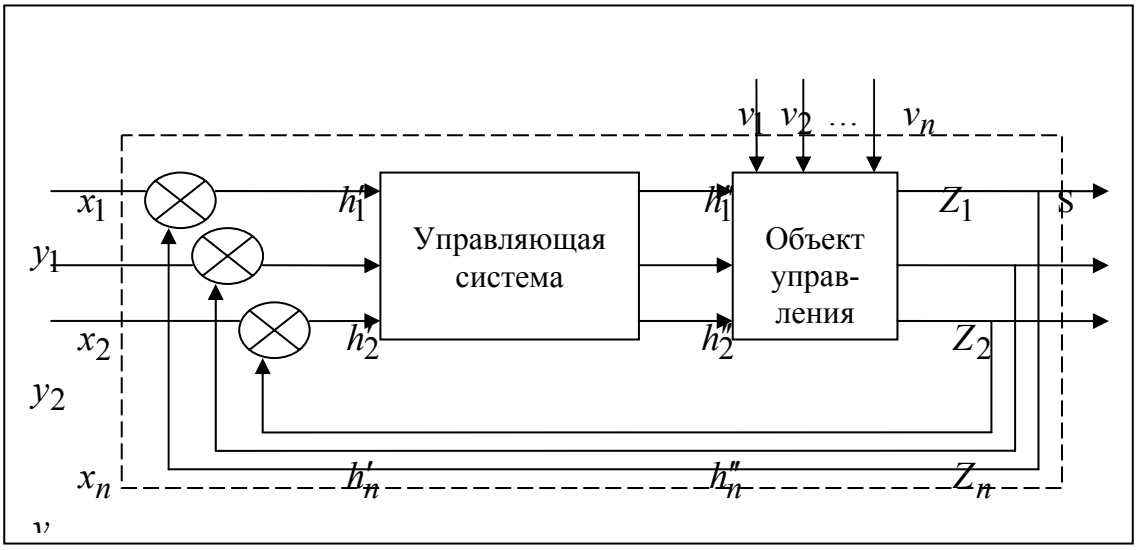
Современная управляющая система – это совокупность программно-технических средств, обеспечивающих достижения объектом управления определенной цели. Насколько точно объект управления достигнет заданной цели, можно судить для одномерной системы по координате состояния y(l). Разность между заданным $y_{зад}(t)$ и действительным $\vec{y}(t)$ законом изменения постоянной величины есть ошибка управления $h'(t) = y_{зад}(t) - y(t)$. Если предписанный закон изменения управляемой величины соответствует закону изменения входного (задающего) воздействия, т.е. $x(t) = y_{зад}(t)$, то $h'(t) = x(t) - y(t).$

Системы, для которых ошибки управления $h'(t) = 0$ во все моменты времени, называются идеальными. На практике реализация идеальных систем невозможна. Таким образом, ошибка $h'(t)$ – необходимый субстат автоматического управлениями, основанного на принципе отрицательной обратной связи, так как для приведения в соответствие с выходной переменой y(t) ее заданному значению используется информация об отклонении между ними. Задачей системы автоматического управления

является изменение переменной $\vec{y}(t)$ согласно заданному закону с определенной точностью (с допустимой ошибкой). При проектировании и эксплуатации систем автоматического управления необходимо выбрать такие параметры системы S, которые обеспечили бы требуемую точность управления , а также устойчивость системы в переходном процессе.

Если система устойчива, то представляет практический интерес поведение системы во времени, максимальное отклонение регулируемой переменной $y(t)$ в переходном процессе, время переходного процесса и т.п. Выводы о свойствах систем автоматического управления различных классов можно сделать по виду дифференциальных уравнений, приближенно описывающих процессы в системах. Порядок дифференциального уравнения и значения его коэффициентов полностью определяются статическими динамическими параметрами системы S.

Рис. 10.2. Структура системы автоматического управления




*Основные понятия систем массового обслуживания (Q-схемы)*

СМО – системы, процесс функционирования которых состоит в обслуживании, путем однотипных действий, случайного потока требований, (заявок), входящих в систему.

Примерами СМО служат любые ремонтные мастерские, торговые предприятия, морские порты, аэродромы, вокзалы, вычислительные системы, вычислительные комплексы и т.д.

В общем случае СМО состоит из следующих компонентов:

1. Входящий поток требований (заявок).
2. Приборы, каналы обслуживания.
3. Очередь из требований, ожидающих обслуживания.
4. Выходящий поток требований, покидающих систему.

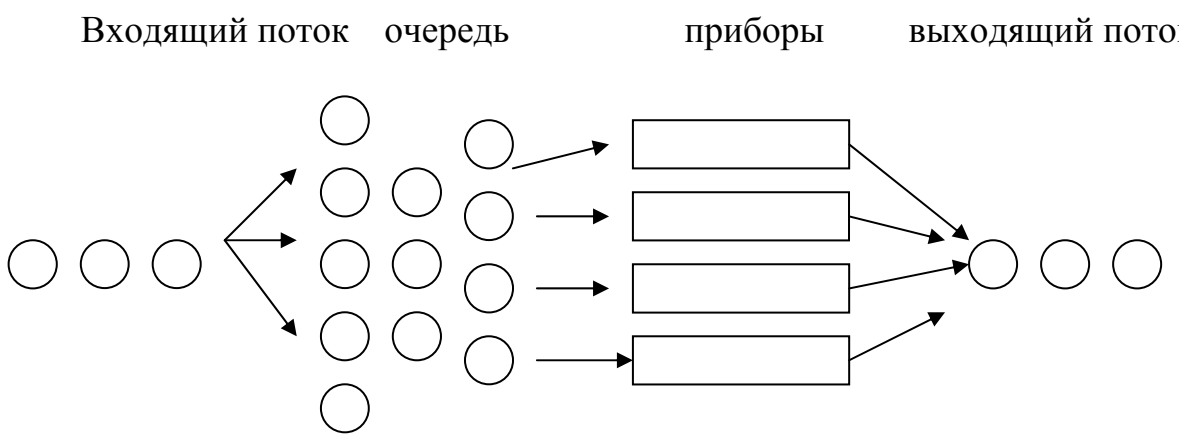



Рис. 10.3.Блок-схема системы массового обслуживания

Входящий поток требований СМО – случайный дискретный процесс с непрерывным временем. Элементами такого процесса являются события, заключающиеся в приходе очередного требования.

Заданием потока будет набор чисел $\{t_0, t_1, t_3, \ldots, t_m\}$, которые являются случайными моментами времени прихода заявок.


Рисунок 10.4. Дискретный процесс прихода заявок в систему

Процесс поступления требований на обслуживание – случайный процесс, который может быть описан некоей функцией x(t), определяющей число требований, нуждающихся в обслуживании за промежуток (0, t)

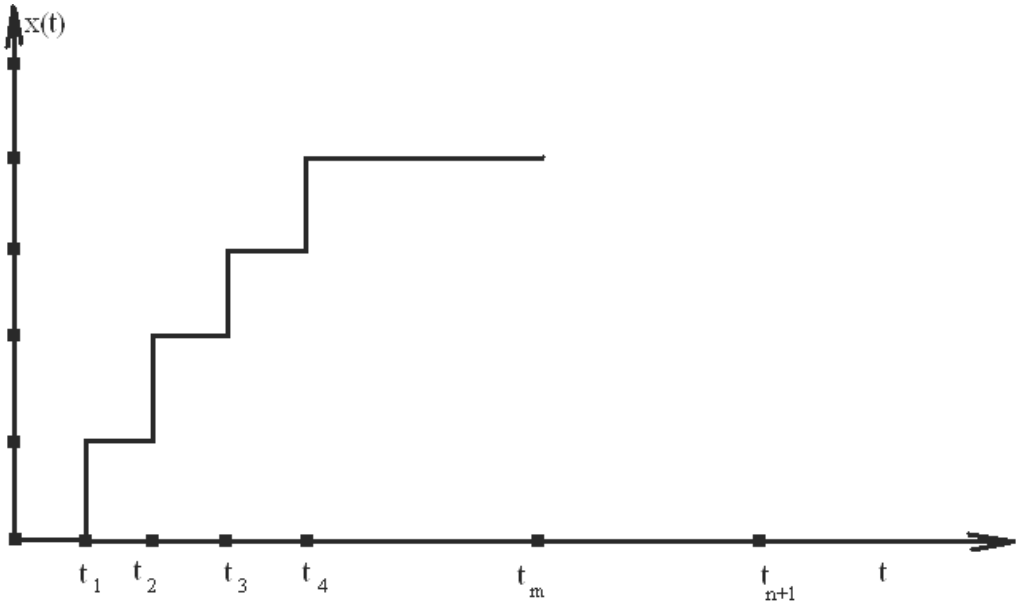



Рис. 10.5. Интегральная функция x (t) числа требований, приходящих в систему

Основной характеристикой потока является плотность вероятности случайной величины $Q_i = t_{i+1} - t_i$, где $Q_i$ – случайная величина, характеризующая интервал времени между приходом i-ого и i+1-ого требования.

Поскольку $t_{i+1} \geq t_i$, то величина $Q \geq 0$, и для этой величины можно ввести функцию $P(Q)$, которая является аналогом плотности вероятности для величины Q.

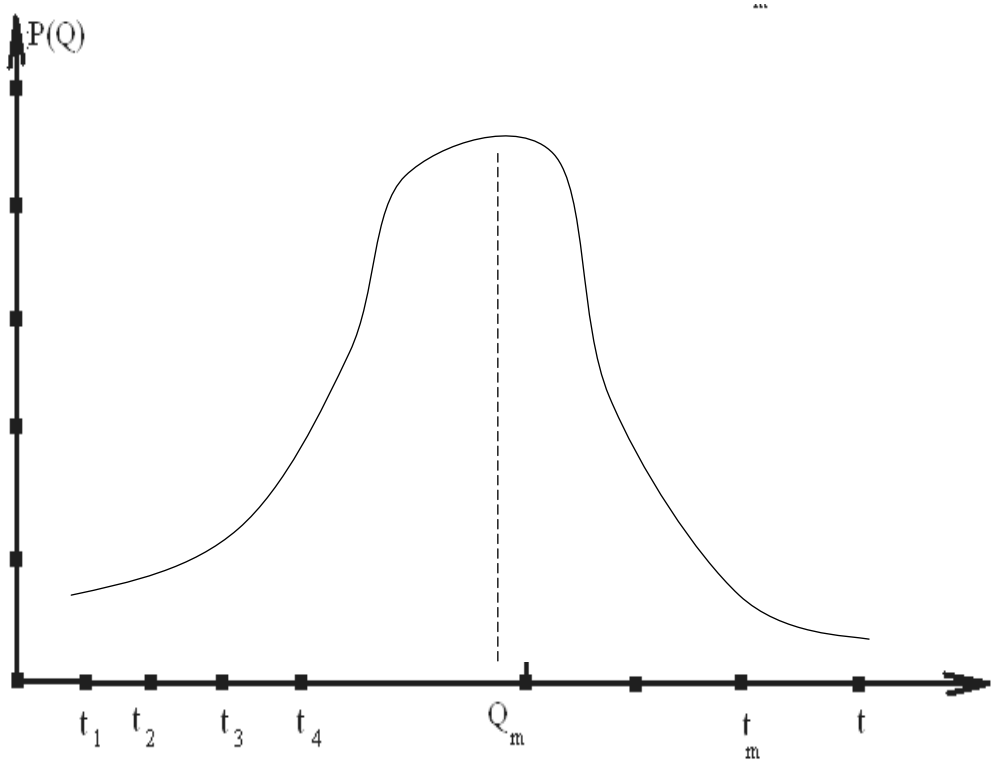



Рис. 10.6. Плотность вероятности величины Q

Максимальная вероятность, соответствующая максимальному интервалу времени между заявками.

Другой важной характеристикой потока является интенсивность потока, которая характеризует среднее количество приходящих заявок в единицу времени и описывается величиной:

$$\lambda_i = \frac{1}{m_i(Q)}$$

$m_i(Q)$ – среднее число заявок, приходящих за интервал Q; $\lambda_i$ – интенсивность потока.

Потоки можно разделить на два класса:

1. Стационарные потоки.

Потоки, для которых $f_i(t_{i+1} - t_i) = f(\tau)$, то есть плотность вероятности не зависит от индекса i, а зависит от случайного интервала времени прихода двух соседних заявок.

Такие потоки называют стационарными, и их интенсивность не зависит от времени и поэтому $\lambda i = \lambda = const$, то есть введенный нами один из параметров потока $\lambda$ – постоянная величина.

2. Нестанционарные потоки.

На практике любой поток является нестационарным, то есть его параметры являются функциями времени, но, как правило, всегда стремятся без потери точности решения задачи за счет выбора подходящей величины времени $\tau$ превратить этот поток в стационарный.

Другая важная группа характеристики работы СМО связана с основным понятием СМО, с «очередями».

Очередь образуется перед СМО вследствие того, что процесс поступления требований на обслуживание и время обслуживания любой заявки являются случайными величинами, при этом возникает рассогласование между моментами окончания обслуживания предыдущего требования и начала обслуживания последующего.

Следствием чего и является возникновение очереди, которая будет ограничена.

Ограничение очереди возникает при ограниченном числе мест ожидания, например размеров площадки перед погрузочно-разгрузочным пунктом добывающего предприятия.

По времени пребывания требования в системе системы массового обслуживания (СМО) делится на следующие виды:

1. СМО с отказами (потерями).

2. СМО с неограниченным временем ожидания.

3. СМО смешанного типа.

СМО с отказами – если требование приходит в момент, когда каналы и накопители заняты, то оно получает отказ и покидает систему.

В системах с неограниченным временем ожидания, требования, поступившие в систему, когда заняты все каналы, ожидают своей очереди до тех пор, пока не освободится какой-либо из обслуживающих каналов, приборов, и поступают на обслуживание.

В смешанных системах требование, поступившее в систему и заставшее все обслуживающие приборы занятыми, становятся в очередь, но в ней оно находится ограниченное время, после чего, не дождавшись обслуживания, покидает систему.

Важной характеристикой функционирования многоканальных СМО является дисциплина обслуживающих каналов, то есть правила, согласно которым, привлекаются к обслуживанию требований свободные каналы СМО.

Выходящий поток СМО – это поток требований, покидающих систему. Требования этого потока могут быть обслужены каналами СМО или не обслужены.

Основной задачей теории СМО является разработка методов определения количественных показателей функционирования СМО и установление связи этих показателей со структурой СМО. Решение таких задач позволит найти наиболее эффективную структуру СМО, улучшить качество обслуживания СМО, улучшить эффективность самой СМО.

Под эффективностью СМО понимают характеристику уровня обслуживания, уровня выполнения этой СМО тех функций, для которых она предназначена. Выбор показателей эффективности СМО определен задачами исследования и целями самой СМО. Показатель эффективности зависит от трех групп факторов:

1. Характеристик качества и надежности СМО.

2. Экономических показателей (стоимость обслуживания приборов, убытки от потери необслуженных клиентов и так далее).

3. От особенностей конкретных ситуаций, в которых эксплуатируется СМО.

Наиболее используемые показатели эффективности СМО:

1. Среднее число требований, которые может обслуживать СМО в единицу времени (абсолютная пропускная способность).

2. Отношение среднего числа требований обслуживания СМО в единицу времени к среднему числу поступивших за это время требований (относительная пропускная способность).

3. Среднее число требований, находящихся в очереди.

4. Среднее число занятых каналов.

5. Среднее время ожидания в очереди.

6. Средняя прибыль, принос СМО в единицу времени.

Для исследования СМО, в силу большого количества нестандартных ситуаций и задач, необходимо применять методы имитационного моделирования в сочетании с аналитическими методами.

*Основы имитационного моделирования СМО*

В основе аналитических методов расчета СМО лежит понятие графа состояния системы, которое мы вкратце рассмотрим на примере одноканальной СМО с постоянной интенсивностью $\lambda$ ~ входящего потока требований и постоянной интенсивностью обслуживания $\mu$ ~ выходящего потока требований.

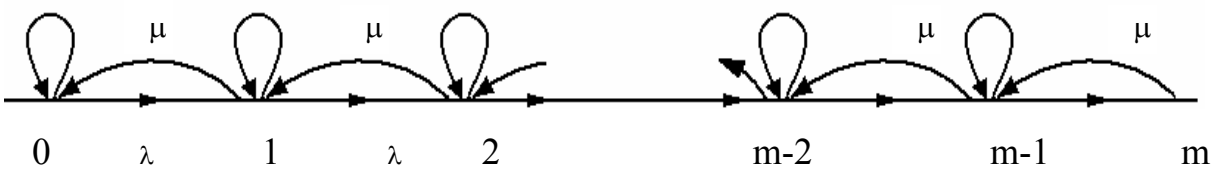



Рис. 10.7. Граф состояний одноканальной СМО

Система может находиться в следующих состояниях:

"О"– канал обслуживания свободен, очереди нет;

"1"– канал обслуживания занят, очереди нет;

"2"– канал обслуживания занят и занято одно место в очереди;

"3"– канал обслуживания занят и занято два места в очереди.

……

"m +1" – канал обслуживания занят и заняты все m мест в очереди.

В общем случае, если интенсивности обслуживания $\lambda$, $\mu$ – являются переменными величинами – $\lambda(t), \mu(t)$, на графе добавляется индексация параметров $\lambda$ $\mu$.

На основании такого графа может быть составлена так называемая система уравнений Колмогорова для вероятностей всех перечисленных состояний:

$$\frac{dP_0}{dt}(\lambda, \mu, P_0) = P_1(t)\mu_1 - P_0(t)\lambda_0$$

……

$$\frac{dP_n}{dt}(\lambda, \mu, P_0, ...P_{n-1}) = P_{n-1}(t)\lambda_{n-1} - P_n(t)\mu_n$$

Эта система может быть составлена и решена на основании приведенного графа состояний марковского процесса и с использованием ограничения $\sum_{i=0}^{n} P_i = 1$ найдены значения всех вероятностей состояний: $P_0$, $P_1,\ldots,P_n$

Отметим, что процесс называется марковским, если для любого момента времени t вероятность нахождения системы в данном состоянии, не зависит от того, когда и каким образом система пришла в это состояние.

С другой стороны методы расчета СМО основаны на предположении, что поток входящих требований является пуассоновским,

то есть таким потоком, в котором вероятность поступления в промежутке t ровно k требований, описывается законом Пуассона:

$P_k(t) = \frac{(\lambda t)^k}{k!} * e^{-\lambda t}$, $\lambda$ – интенсивность входящего потока.

К тому же необходимо отметить, что плотность вероятности входящего потока требований. $f_1(t) = \lambda e^{-\lambda t}$, $\lambda$=const. Плотность вероятности выходящего потока так же экспоненциальна, но с параметром

$\mu$ = const, $f_2(t) = \mu e^{-\mu t}$

В большинстве случаев все процессы являются немарковскими, поэтому вместо разработанного классического алгоритма используется метод моделирования случайных процессов любой природы, метод статистического моделирования или метод временных диаграмм.

Используя этот метод, можно определить большую часть основных показателей эффективности, учесть процессы отказа и восстановления СМО немарковского типа.

## Тема 11. Основные понятия теории надежности систем. Метод расчета надежности систем на базе построения логической функции системы

Как известно, надежность системы – это способность системы выполнять множество заданных алгоритмов переработки информации с заданной достоверностью или это свойство системы сохранять собственную работоспособность на некотором отрезке времени в заданных условиях эксплуатации.

Взлом системы, незаконное проникновение в нее, в подавляющем большинстве случаев (даже при проникновении типа «прослушивание») через какое-то время должен привести от малозаметного до внушительного роста числа отказов в системе, вследствие (даже незначительных) колебаний в режимах работы системы [7].

Это утверждение совершенно очевидно, если незаконное проникновение совершается, например, с использованием особых электромагнитных каналов, что немедленно приводит к выходу за допустимые пределы таких параметров, как сила тока в узле проникновения или напряжения, которые входят в число обязательно контролируемых параметров системы. Хорошо известно, что высокий уровень надежности (0,99999) требует абсолютно точного нахождения всякого контролируемого параметра в пределах определенного допуска, что контролируется системой управления объекта. Отказ – основополагающее понятие теории надежности – внезапный или постепенный (метрологический) при взломе системы с необходимостью отреагирует на это возрастанием интенсивности отказов λ, равному среднему числу отказов в единицу времени. Но надежность системы ($P=e^{-\lambda t}$), как видно, с увеличением λ, будет по величине уменьшаться.

Известно, что для расчета надежности системы давно и очень успешно, применяется методика, основанная на составлении структурной схемы системы (блок-схемы), адекватной самой системе. По этой схеме рассчитывается соответствующая этой схеме так называемая логическая функция работоспособности, из которой после ряда математических операций (с участием логических символов $\wedge$, $\vee$, $-$ ) рассчитывается надежность системы.

В основе нашей методики расчета лежит представление нашей системы блок-схемой, аналогичной вышеупомянутой (т.е. блок-схемой, описывающей распространение информации по системе от входа до выхода), но в качестве параметра каждого блока будет рассматриваться не значение его надежности ($P_{б/о}$ ), а вероятность взлома данного блока ($P_{взл.}$), рассчитываемая, естественно, заранее. Результирующая логическая функция «взлома» – $L_{взл.}$ обрабатывается полностью аналогично логической функции работоспособности, широко используемой в теории надежности.

Запишем в виде алгоритма последовательность операций для расчета надежности сложной кибернетической системы:

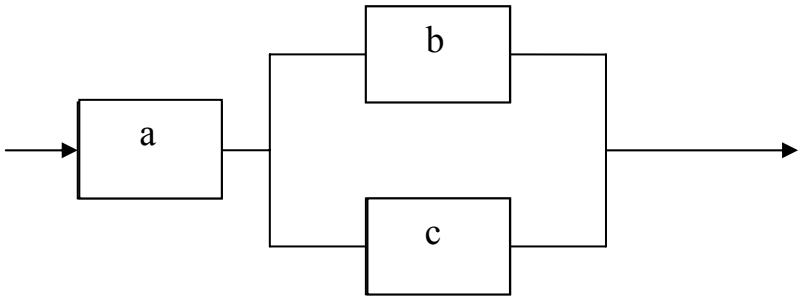
1. Сформулировать словесно условие работоспособности системы, изделия, прибора.
2. На основании словесной формулировки записать логическую функцию работоспособности.
3. Используя набор разрешенных постулатов, соответствующих алгебре логики, попытаться преобразовать, упростить логическую функцию $F_л$, привести ее к бесповторной форме, не подлежащей упрощению, или, другими словами, необходимо функцию $F_л$ минимизировать.
4. В $F_л$ заменить логические операции на соответствующие им арифметические, соединенные знаками «+,–, * …».

5. В арифметической функции $F_A$ заменить простые события, соединенные арифметическими знаками, на их вероятности.
6. По формуле для $F_A$, рассчитать интересующую нас вероятность работоспособности, путем замены соответствующих вероятностей на их числовые оценки.

Данная таблица постулатов применяется при расчете сложных систем.

1. $a \vee b = b \vee a$
2. $ab = ba$
3. $a \vee (b \vee c) = (a \vee b) \vee c$
4. $a \vee (b \wedge c) = (a \vee b)(a \vee c)$
5. $a(b \vee c) = ab \vee ac$
6. $a \vee \bar{a} = 1;\ a \vee 0 = a,\ a \wedge 0 = 0$
7. $a \cdot 1 = a,\ a \vee 1 = 1$ - закон поглощения
8. $a \cdot \bar{a} = 0$
9. $a \vee a\bar{b} = a \vee b$
10. $a \vee a = a$
11. $a \cdot a = a$
12. $\overline{(a \vee b)} = \bar{a}\bar{b}$
13. $\overline{(ab)} = \bar{a} \vee \bar{b}$
14. $ab \vee a\bar{b} = a$
15. $a(a \vee b) = a$
16. $F_л(a,b,c,...k) = aF_{л1}(1,b,c,...k) \vee \bar{a}F_{л2}(0,b,c,...k)$

Каждому постулату может быть поставлена в соответствие некоторая структурная схема (и наоборот), например:



При этом постулат № 5 $a(b \vee c) = ab \vee ac$ описывает условие ее работоспособности.

Ясно, что система работоспособна, т.е. передает информацию, если работоспособны a и b, или a и c, или работоспособны все три элемента, поэтому данному словесному высказыванию можно поставить в соответствие такую логическую функцию:

$$F_л = ab \vee ac \vee abc = ab \vee ac = a(b \vee c).$$

Мы привели нашу логическую функцию $F_л$ к элементарной, минимальной форме, от которой можно совершить переход к арифметической функции $F_A$, используя стандартный набор арифметических постулатов:

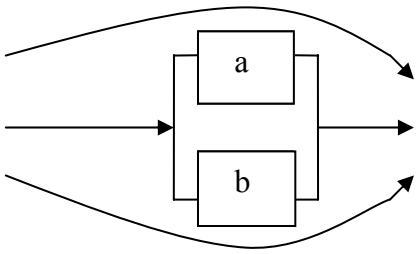
$a \vee b = a + b - ab$

$a \wedge b = ab$

$\bar{a} = 1 - a$

Задача № 1

Определить вероятность работоспособного состояния системы, если известно, что надежность элементов «a» и «b» таковы: $P_a = 0{,}8$ и $P_b = 0{,}8$.




Первый способ решения:

$F_л = a \vee b \vee ab$

$F_л = a\{1 \vee b \vee 1 * b\} \vee \bar{a}\{0 \vee b \vee 0 * b\} \Rightarrow a * 1 \vee \bar{a} * b \Rightarrow a \vee \bar{a}b \Rightarrow a \vee b$

Перейдем к арифметической логической функции:

$$F_a = a + b - ab = P_a + P_b - P_a * P_b = 0{,}8 + 0{,}8 - 0{,}8 * 0{,}8 = 1{,}6 - 0{,}64 = 0{,}96$$

Надежность (вероятность безотказной работы) равна 0,96

Второй способ решения:

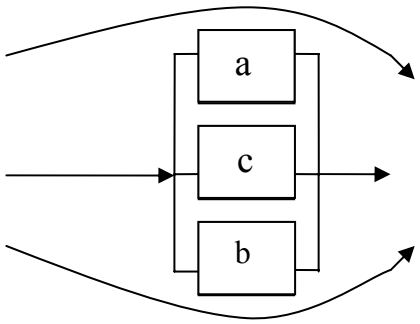
$F_л = a \vee b \vee ab \Rightarrow a(1 \vee b) \vee b(1 \vee a) \Rightarrow a * 1 \vee b * 1 \Rightarrow a \vee b$.

Переходя к арифметической логической функции $F_a$, получим

$$\text{Р}_{\text{б/о}} = P_a + P_b - P_a * P_b \cong 0{,}96$$

Задача № 2

Рассчитать надежность следующей схемы,если $P_a = P_b = P_c = 0{,}8$.




Нетрудно видеть, что $F_л = a \vee b \vee c \vee ab \vee ac \vee bc \vee abc$. Используя постулат 16: $F_л(a,b,c) = aF_1(1,b,c) \vee \bar{a}F_2(0,b,c)$, получим:

$$F_л(a) = a * 1 \vee \bar{a}(b \vee c) \Rightarrow a \vee b \vee c.$$

Мы получили элементарную, примитивную формулу для логической функции. Переходя к арифметической логической функции $F_a = a + b + c - ab - bc - ac + abc$, подставляя вместо $a \to P_a = 0{,}8$, $b \to P_b = 0{,}8$, $c \to P_c = 0{,}8$, приходим к $P_{б/о} = 0{,}992$.

Используя данную методику расчета логической функции работоспособности структурной схемы, можно рассчитать надежность и более сложных структурных схем – например схемы логического моста, треугольника и т.д. [7(доп)] Очевидно, что данный принцип расчета надежности может быть применен к расчету вероятности взлома некоторой системы, если эту систему мы представим в виде некоторой структурной схемы, содержащей ее каналы несанкционированного доступа [1].

## Тема 12. Метод расчета вероятности взлома системы на основе логической функции системы

Данная задача целиком находится в классе задач по моделированию угроз воздействия на всевозможные источники информации: моделирование способов проникновения к месту скопления информации (например, кабинет руководителя); моделирование оптических каналов утечки (окна, двери, телевизионное закладное устройство); моделирование акустических каналов утечки; моделирование радиоэлектронных каналов утечки. Этот перечень может быть продолжен и дальше. Однако возможны самые различные варианты выбора как вида канала утечки (оптический, радиоэлектронный и т.д.), так и (в общем случае случайного числа) одновременно взламываемых каналов [7(доп)]. Если попытаться прояснить вероятность взламывания всей системы, то при таком подходе (от «частного к общему») это сделать затруднительно, ибо модель всей системы в данных способах взлома отсутствует изначально, а вся проблема оценки вероятности взлома (как и вероятности взлома отдельных каналов) относится к классу слабоформализуемых задач [1].

Однако, если посмотреть на оценку вероятности взлома системы, оставаясь в рамках рассмотренного выше системного подхода, который может быть реализован в виде некоторой структурной схемы системы (где в роли отдельных блоков выступают отдельные каналы незаконного проникновения в систему), то задачу общей, интегральной оценки взлома всей системы можно решить с той или иной степенью точности, в зависимости от корректности самой блок-схемы, составленной из каналов взлома. Этот способ состоит в использовании стандартной структурной схемы системы и составлении, в соответствии с материалом предыдущего раздела, логической функции работоспособности, с ее дальнейшей стандартной обработкой. При этом надежность каждого блока структурной схемы должна быть заменена на вероятность несанкционированного проникновения через данный блок ($P_{i\,взл}$). Далее необходимо следовать строго по пунктам (1– 6) алгоритма, приведенного в предыдущем разделе.

## Тема 13. Концепция интегральной защиты информации

Активное внедрение в нашу повседневную жизнь новых сетевых информационных технологий в условиях массового использования персональных компьютеров, открытых компьютерных сетей и общедоступных каналов связи способствует еще большему обострению проблемы обеспечения безопасности. Так, например, проведенное фирмой «ICSA» (International Computer Security Assotiation) исследование 200 Internet-серверов позволило установить, что более 70% из них имеют изъяны безопасности, что делает их уязвимыми перед атаками извне, даже при том, что большинство абонентских пунктов были оборудованы межсетевыми экранами. Для эффективного решения проблемы обеспечения безопасности необходим соответствующий современный уровень технологий, технических средств и услуг безопасности, основной тенденцией развития которых является бурно развивающийся процесс тотальной интеграции. В настоящее время ею охвачены микро- и радиоэлектроника, сигналы и каналы, появились интегральные технологии, многофункциональные интегральные устройства, интегральные сети и системы, стали предоставляться интегральные услуги обеспечения безопасности [6].

Сегодня, наряду с интеграцией функциональной, схемотехнической, сетевой, активно развивается интегральная безопасность, характеризующая такое состояние жизнедеятельности человека, а также функционирования объектов и информации, при котором они надежно защищены ото всех возможных видов угроз в ходе непрерывного жизненного процесса и решения поставленных задач. По существу, интегральная безопасность в пределе аккумулирует в себе все необходимые для решения данной задачи виды безопасности (охранная,

пожарная, экологическая, личная, информационная и т.п.). Понятие интегральной безопасности предполагает обязательную непрерывность процесса обеспечения безопасности как во времени, так и в пространстве по всему технологическому циклу деятельности с обязательным учетом всех возможных видов угроз (утечки информации, несанкционированного доступа, терроризма, пожара, аварий, и т. п.). Поэтому, например, при обеспечении интегральной безопасности организации, фирмы, любой коммерческой структуры в обязательном порядке должны учитываться одновременно вопросы как обеспечения информационной безопасности, так и защиты объекта и персонала, что, к сожалению, в настоящее время еще, как правило, не соблюдается [1,6].

Интегральная защита – это монолитная непроницаемая защита. Аналогом ее может служить монолитный забор по периметру зоны безопасности. В реальной же жизни обычно строятся мощные ворота на дорогах, объехать которые по бездорожью «нет проблем». Реальная система безопасности сегодняшнего дня больше напоминает изгородь на отдельных участках с зияющими в ней дырами. Ярким примером подобной реальной системы безопасности может служить, например, организация с мощной системой контроля доступа, системой видеонаблюдения, криптозащитой и т.п., но без блокирования каналов утечки, например за счет побочных излучений мониторов компьютеров. В этом случае все конкуренты, расположенные в радиусе до 1,5 км, имеют реальную возможность, используя соответствующие технические средства, читать всю информацию с экрана дисплеев конкурентов, не покидая своих офисов. При интегральном подходе к созданию системы безопасности подобные казусы исключены.

Большие надежды специалисты в области обеспечения безопасности возлагают на внедрение новых интегральных технологий и электронных средств защиты. Как было показано выше, существенно повысить эффективность систем безопасности в последнее время стало возможным с использованием интегрального подхода и нового понятия, которое находит все большее применение, – понятия интегральной безопасности. Основной смысл этого понятия состоит в необходимости обеспечить такое состояние условий функционирования человека, объектов и информации, при котором они надежно защищены ото всех возможных видов угроз в ходе непрерывного производственного процесса и жизнедеятельности (для информационной безопасности – это процесс подготовки, хранения, передачи и обработки информации). Используя понятие интегральной безопасности, можно сказать, что конечной целью интегральной защиты является создание таких условий, при которых будет невозможен как перехват, так и видоизменение и уничтожение информации, причем действие интегральной защиты должно быть непрерывно как во времени, так и в пространстве. Поскольку основным принципом интегрального подхода является блокирование всех возможных каналов утечки, информации, то для создания эффективных систем безопасности в первую очередь необходимо исследовать особенности возможных каналов утечки информации. Анализ рассмотренных каналов утечки и возможных методов защиты от них позволяет получить предварительные результаты, приведенные в таблице 13.1.

Таблица 13.1. Основные методы и средства получения и защиты информации

| № n/n | Типовая ситуация | Каналы утечки информации | Методы и средства получения информации | Методы и средства защиты информации |
|---|---|---|---|---|
| 1 | Разговор в помещении и на улице | Акустика; Гидроакустика; Виброакустика; Акустоэлектро-ника | Подслушивание, диктофон, микрофон, направленный микрофон, полуактивная система; стетоскоп, вибродатчик; гидроакустиче-ский датчик; радиотехниче-ские спецприемники | Шумовые генераторы, поиск закладок, защитные фильтры, ограничение досупа |
| 2 | Разговор по проводному телефону | Акустика; электросигнал в линии; наводки | Аналогично п.1; параллельный телефон, прямое подключение, электромагнит-ный датчик, диктофон, телефонная закладка; радиотехниче-ские спецустройства | Аналогично п.1; маскирование, скемблирование, шифрование; |
| 3 | Разговор по радиотелефону | Акустика; электромагнитн ые волны | Аналогично п.1; радиоприемные устройства | Аналогично п. 1; Аналогично п. 2; |
| 4 | Документ на бумажном носителе | Наличие документа | Кража, визу-ально, копиро-вание, фотогра-фирование | Ограничение доступа, спецтехника |
| 5 | Изготовление документа на бумажном носителе | Наличие документа; продавливание ленты и бумаги; акустический шум принтера; паразитные сигналы, наводки | Аналогично п. 4; кража, визуально; аппаратура акустического контроля; специальные радиотехничекие устройства | Аналогично п. 4; оргтехмероприятия; шумоподавление; экранирование; |

*Окончание табл. 13.1*

| № n/n | Типовая ситуация | Каналы утечки информации | Методы и средства получения информации | Методы и средства защиты информации |
|---|---|---|---|---|
| 6 | Почтовое отправление | Наличие документа | Кража, прочтение | Специальные методы защиты |
| 7 | Документ на небумажном носителе | Носитель | Хищение, копирование, считывание | Контроль доступа, криптозащита, физическая защита |
| 8 | Изготовление документа на небумажном носителе | Изображение на дисплее; паразитные сигналы, наводки; электрические сигналы; логика программ | Визуально, копирование, фотографирование; специальные радиотехнические устройства; аппаратные закладки; Программные закладки | Контроль доступа, криптозащита, поиск закладок |
| 9 | Передача документа по каналу связи | Электрические и оптические сигналы | Несанкционированное подключение, имитация зарегистрированного пользователя | Криптозащита |
| 10 | Производственный процесс | Отходы, излучения и т.п. | Спецаппаратура различного назначения | Оргтехмероприятия, физическая защита |
| 11 | Работа с удаленными базами данных, работа в сети | Электросигналы, наводки | Программные и аппаратные закладки, несанкционированный доступ, компьютерные вирусы | Криптозащита, спецматобеспечение, ограничение доступа, оргтехмероприятия, антивирусная защита. |

Интегрально оценивая методы и средства получения и защиты информации в типовых ситуациях и не вдаваясь в подробности приведенных в таблице данных, можно сделать вывод, что в настоящее время основным противодействием утечки информации является обеспечение физической защиты (технические средства, линии связи, персонал) и логической защиты (операционная система, прикладные программы и данные) информационных ресурсов. При этом безопасность достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий. Результаты анализа современного рынка технических средств защиты информации приведены в таблице 13.2.

Таблица 13.2. Современные технические средства защиты информации

| Технические средства | Краткие характеристики | Разработчики (поставщики) | Примечания:<br>1. Рекомендация по применению<br>2. Имеющиеся на рынке аналоги |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Активные и пассивные средства защиты от утечки по физическим полям | | | |
| ГШ 1000<br>ГШ 1000К | Генератор шума автономный; генератор шума, встраиваемый в ПК | СКБ ИРЭ РАН | 1. Для ПК, абонентских пунктов и центра автоматизированной сети<br>2. «Смог», «Гном-3», «Гром-ЗИ-4», «Волна» |
| ФСПК-100<br>ФСПК-200 | Сетевые помехоподавляющие фильтры | | 1. Для ПК и терминалов<br>2. CAG 60 4 |
| «Салют» | Устройство защиты от побочных излучений | НТФ «Криптон» | 1. Для ПК и терминалов.<br>2. «Корунд», «Криптон» |
| «Корунд» | Устройство защиты от перехвата речевой информации через телефон | ТОО «Реном» | 1. Для защиты от утеки через телефон.<br>2. «Барьер-3», «Протон», «СТО-24» |

*Продолжение табл. 13.2*

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Сертифицированные по требованиям безопасности средства | Доработанные или специальной сборки вычислительные средства | АО «ДОС»<br>АО «Ланит»<br>АО «Свемел»<br>АО «РНТ» | 1. Для абонентских пунктов и обрабатывающего центра АС |
| «Гранит-N» | Устройство защиты от утечки по вспомогательным средствам | НТСЦ «Заслон»<br>СНПО «Элерон» | 1. Для обрабатывающих средств в категорированных помещениях |
| «Кабинет» | Система вибрационной и акустической защиты | СНПО «Элерон» | 1. Для защиты речевой информации.<br>2. «Заслон», VNG-006, ANG-2000 |
| TRD-017 | Устройство защиты от несанкционированной записи на диктофоны | «Дивекон» | 1. Для блокирования несанкционированной записи на диктофоны.<br>2. «Рубеж-1», «Буран-2», УПД-1 |
| Технические средства поиска каналов утечки информации | | | |
| «Обь» | Нелинейный радиолокатор | «Защита информации» | 1. Для поиска радио-, видеозакладок<br>2. «Октава», «Переход», «Лотос» |
| SEDIF PRO | Программа управления сканирующим приемником | То же | 1. для поиска каналов утечки.<br>2. SEDIF SCJUT, SEDIF PLUS |
| OSCOR OSC-5000 | Многофункциональный спектральный коррелятор | «Дивекон» | 1. Для поиска каналов утечки.<br>2. CMP-700 |
| Программные и программно-аппаратные средства разграничения доступа к информации | | | |
| Secret Net 1.0 (2.0) | Устройство защиты от несанкционированного доступа | «Информзащита» | 1. Для защиты ПК от несанкционированного доступа.<br>2. «Сезам», «Страж-1», «Аккорд», SKIP |
| Программные и программно-аппаратные средства ЗИ и подтверждения её подлинности | | | |
| «Верба-0» | Системы электронной цифровой подписи | ПНИЭИ МО | 1. Для идентификации информации при передаче ее по каналам связи<br>2. «Маскарад», «Нотариус» |

*Окончание табл. 13.2*

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| «Базальт» | Устройство защиты речевой информации | «Автоматика» | 1. Для защиты речевой информации.<br>2. УЗТП, АКТП |
| «Спринт» | Шифратор (до 10 Мбит/с) | АО «Инфотекс» | 1. Криптозащита<br>2. «Криптон», «Град», «Удача» |
| Программно-аппаратные средства обеспечения целостности продукта и защиты от копирования | | | |
| Электронные ключи на основе HASP технологии | Средства предотвращения несанкционированного копирования и НСД | АО «Аладдин» | 1. Для терминалов корпоративных и автоматизированных сетей |
| Автоидентификаторы на основе Touch Memoury | Средства защиты от несанкционированного доступа к информации | Dallas Semiconductor, «Конфидент» | 1. Для защиты от несанкционированного доступа.<br>2. Информзащита, АРТИ, РНТ |
| Программные средства защиты от программ-вирусов и других вредоносных программ | | | |
| Dr.Web | Программный продукт для защиты от вирусов | ЗАО «ДиалогНаука» | 1. Для защиты ПК от компьютерных вирусов.<br>2. Aidstest, Adinf, Sherif |
| AVP (антивирус Касперского) | То же | ЗАО «Лаборатория Касперского» | То же |
| Физико-химические средства защиты и подтверждения подлинности документов | | | |
| Голографические метки на основе технологии Advateq | Средства идентификации подлинности объекта и контроля НСД | НТЦ ФАПСИ | 1. Специальные тонкопленочные материалы с изменяющейся цветовой гаммой |
| Защищенные общесистемные программные продукты, исключающие недекларированность | | | |
| Операционная система МС ВС | Сертифицированное системное обеспечение | ВНИИС | 1. При обработке конфиденциальной информации |
| СУБД ЛИНТЕР | Сертифицированное ПО | НПО «РЭЛЭКС» | То же |

Таблица 13.3. Соотношение методов и средств защит и добывания информации

| Методы и средства добывания защиты информации: | Спецрежим работы | Детекторы металла | Поиск визуальный | Экстранир. помещений | Экстранир. Кабелей, техник | Генераторы шума | Виброгенераторы | Генераторы радиопомех | Воздействие на микрофон | Детекторы поля | Селекторы сигналов | Локаторы | Стирание записи | Детекторы излучения | Контроль параметров ТЛ | Тестирование ТЛ | Нарушение режима ТСДИ | Уничтожение ТСДИ | Прослушивание ТЛ | Фильтрация сигналов | Техническое закрытие | Криптозащита | Антивирусы |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Радиомикрофон | | | | | | | | | | | | | | | | | | | | | | | |
| Радиомикрофон | | | | | | | | | | | | | | | | | | | | | | | |
| Радиомикрофон | | | | | | | | | | | | | | | | | | | | | | | |
| Микрофон | | | | | | | | | | | | | | | | | | | | | | | |
| Направленный микрофон | | | | | | | | | | | | | | | | | | | | | | | |
| Радиостетоскоп | | | | | | | | | | | | | | | | | | | | | | | |
| Специальный эндоскоп | | | | | | | | | | | | | | | | | | | | | | | |
| Лазерные средства | | | | | | | | | | | | | | | | | | | | | | | |
| Миниатюрные магнитофоны | | | | | | | | | | | | | | | | | | | | | | | |
| Проводные линии объекта | | | | | | | | | | | | | | | | | | | | | | | |
| Микрофон с передачей по ТЛ | | | | | | | | | | | | | | | | | | | | | | | |
| Контроль телефонной линии | | | | | | | | | | | | | | | | | | | | | | | |
| Контроль телекса и факса | | | | | | | | | | | | | | | | | | | | | | | |
| Бесконтактный контроль ТЛ | | | | | | | | | | | | | | | | | | | | | | | |
| Визуальный контроль (ТВ, ИК) | | | | | | | | | | | | | | | | | | | | | | | |
| Приемники излучения | | | | | | | | | | | | | | | | | | | | | | | |
| Хищение письма, ленты, дискеты | | | | | | | | | | | | | | | | | | | | | | | |
| Контроль монитора ПЭВМ | | | | | | | | | | | | | | | | | | | | | | | |
| Копирование информации | | | | | | | | | | | | | | | | | | | | | | | |
| Программные закладки, вирусы | | | | | | | | | | | | | | | | | | | | | | | |

Необходимо отметить, что абсолютных средств защиты в природе не существует, эффективность методов и средств защиты целиком зависит от конкретных используемых методов и средств добывания, поэтому и рассматривать их необходимо в тесной взаимосвязи. Указанный подход использован в данной работе. С этой целью для предварительной оценки и выбора методов и технических средств защиты информации в зависимости от известного (установленного) или предполагаемого средства добывания (канала утечки) (табл. 13.2) приведено соотношение методов и средств защиты и добывания информации, при этом использованы следующие сокращения: ТСДИ – технические средства добывания информации; ТЛ – телефонная линия; ТВ – телевизионный; ИК – инфракрасный.

Материалы таблицы являются рекомендательными и в сжатом виде показывают, что, например, для комплексной защиты информации от воздействия радиомикрофонов с автономным питанием целесообразно использовать следующие методы и средства защиты:

- визуальный поиск;
- экранирование;
- генераторы шума и радиопомех;
- селекторы сигналов;
- воздействие на микрофон;
- детекторы поля и излучения;
- нелинейные локаторы.

Не останавливаясь на других возможных каналах утечки, рассмотрим более подробно методы и средства блокирования каналов утечки информации с экрана монитора ПЭВМ (эта ситуация подробно рассмотрена выше). Как видно, для защиты информации необходимо использовать как пассивные методы (экранирование монитора и помещения, фильтрацию сигналов по сетям питания), так и активные методы (зашумление, поиск радиозакладок, техническое закрытие).

Наиболее универсальным методом блокирования в данном случае является экранирование. Эффективность экранирования прямо пропорциональна толщине экрана в диапазоне частот от сотен килогерц до нескольких гигагерц. В настоящее время имеется широкий ассортимент экранирующих материалов и средств защиты мониторов, в том числе экраны с покрытием золотом, проволочные сетки для установки перед экраном дисплея, вентиляционные решетки с ячейками малых размеров, электрические фильтры для уменьшения излучения от кабелей и проводов питания, специальные материалы для соединения различных частей экранирующих конструкций и т.п. Однако эффективное экранирование является весьма дорогим и может не только удвоить, но и утроить цену дисплея в зависимости от требуемого уровня защиты.

Весьма привлекательным для коммерческого применения методом блокирования каналов утечки информации с экрана монитора является метод зашумления, реализация которого достигается с использованием специальных, шумовых генераторов. В настоящее время на российском рынке имеется достаточный выбор указанных приборов. В частности, можно отметить такие средства маскировки побочных электромагнитных излучений работающих ЭВМ, как стационарные шумогенераторы ГШ-1000 и Гном-3, а также встраиваемые в ПЭВМ шумогенераторы ГШ-К-1000 и UM 061 [Л 12]. В качестве примера в таблице 13.4. приведены основные характеристики устройства защиты компьютера от систем дистанционного считывания содержимого дисплея UN 061, представляющего собой широкополосный передатчик реального белого шума и предназначенного для предотвращения дистанционного съема информации с ПЭВМ.

Таблица 13.4. Основные характеристики устройства защиты компьютера

| Основные характеристики | Параметры |
|---|---|
| Ширина спектра подавления, МГц | 0,1…800 |
| Спектральная мощность шума, дБ | 25…70 (зависит от частоты) |
| Мощность передатчика, Вт | 3,5 |
| Конструкция | Плата IBM контроллера |
| Напряжение питания, В | 12 (от блока питания ПЭВМ) |

Данные таблицы показывают, что шумогенераторы являются простыми, но достаточно эффективными устройствами блокирования каналов утечки информации с ПЭВМ.

Анализируя методы блокирования каналов утечки информации с экрана монитора, нельзя не остановиться еще на одном весьма эффективном методе защиты с использованием технического кодирования. Как было показано выше метод построения изображения на экране дисплея и телевизионного приемника является общим. Поэтому, если изменить последовательность строк изображения на экране дисплея, то с помощью обычного ТВ-приемника нельзя будет восстановить информацию с экрана. Последовательность строк изображения дисплея можно менять с помощью кодового ключа, вводимого в дисплей, причем кодовый ключ может меняться по случайному закону. По оценкам специалистов, после подобной доработки цена дисплея увеличится всего лишь на 20 долл.

Таким образом, изо всех рассмотренных выше методов блокирования каналов утечки информации с экрана дисплея ПЭВМ самым дешевым оказался метод с использованием технического кодирования, наиболее дорогим, но универсальным – метод экранирования и наиболее используемым на практике (наиболее удобным) - метод зашумления эфира.

Однако в повседневной практике возникает естественный вопрос: «А какова же реальная дальность перехвата с конкретного образца дисплея?»

Для ответа на этот вопрос может быть использована измерительная установка, приведенная на рисунке 13.1.

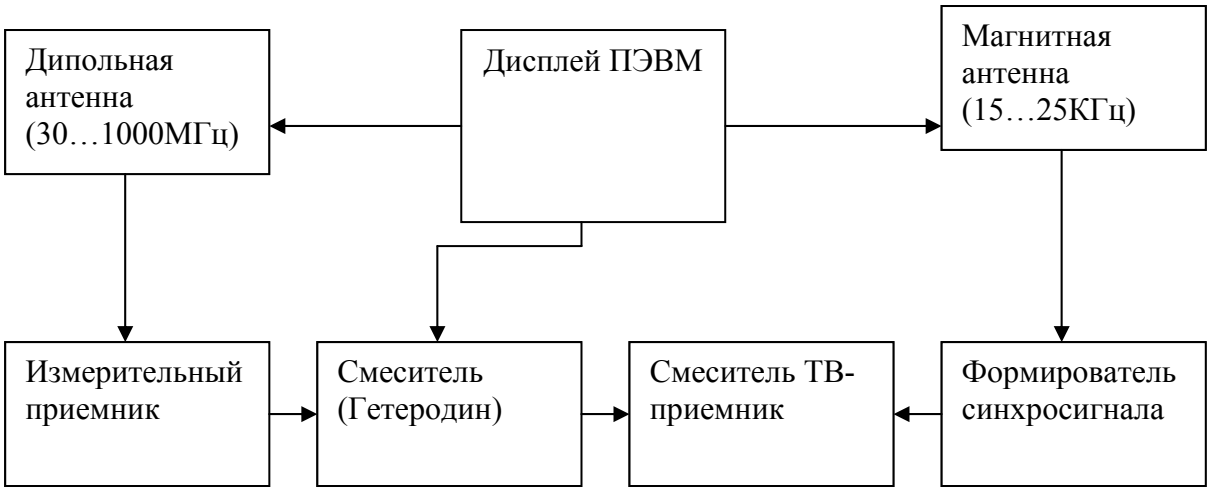



Рис. 13.1. Блок-схема измерения параметров канала утечки информации с дисплея

Как видно из блок-схемы использование двух приемников позволяет не только восстанавливать изображение, но и проводить измерения напряженности электрического поля и сравнивать ее значения с качеством восстановления. Для получения количественных характеристик каналов утечки исследуемый дисплей необходимо располагать на высоте 1 м над заземленным металлическим листом, находящимся на полу измерительной площадки. Использование полученных характеристик гарантирует обеспечение заданного уровня безопасности.

С учетом вышеизложенного, можно сделать общий вывод о том, что реальные характеристики каналов утечки информации существенно влияют на эффективность систем безопасности, поэтому создание систем эффективной защиты должно происходить с учетом особенностей реальных каналов. Этот вывод не является тривиальным, как может показаться с первого взгляда. Так, например, сам факт излучения дисплея еще не говорит об утечке информации. Все определяется конкретным

уровнем напряженности поля за пределами зоны безопасности и техническими возможностями противника. Поэтому окончательный вывод об утечке информации может сделать только квалифицированный специалист, использующий специальные технические средства. С другой стороны, особенности реальных каналов утечки информации могут быть успешно использованы и противником для обеспечения несанкционированного доступа к информации, о чем необходимо постоянно помнить. Так, например, акустические каналы утечки информации могут быть осуществлены через стекла окон, строительные, сантехнические, вентиляционные, теплотехнические и газораспределительные конструкции, с использованием для передачи радио, радиотрансляционных, телефонных и компьютерных коммуникаций, антенных и телевизионных распределительных сетей, охранно-пожарных и тревожных сигнализаций, сетей электропитания и электрочасов, громкоговорящей и диспетчерской связи, цепей заземления и т. п. Поэтому процесс защиты информации становится все более сложным, так как случайный пропуск хотя бы одного возможного канала утечки может снести к нулю все затраты и сделать систему защиты неэффективной.

Таким образом, достижения науки и техники, создание новых технологий постоянно способствуют появлению все новых каналов утечки информации и делают задачу блокирования каналов утечки постоянно актуальной, технически сложной, требующей к себе пристального внимания.

## Тема 14. Компьютерная стеганография как перспективное, современное техническое и программное средство защиты информации от несанкционированного доступа

Компьютерная стеганография – современная технология защиты информации от несанкционированного доступа – является одной из древнейших, но не решенных до настоящего времени проблем. Способы и методы сокрытия секретных сообщений известны с давних времен, и данная сфера человеческой деятельности получила название «стенографии». В переводе с греческого означает «тайнопись», и не исключено, что методы стеганографии появились, вероятно, раньше, чем сама письменность. С течением времени, по мере развития технического прогресса, возникли и стали использоваться такие эффективные методы сокрытия информации, как криптография и кодирование [2, 6]. Известно, что цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. Стеганография имеет другую задачу – скрыть сам факт существования секретного сообщения. Но при этом оба способа могут быть объединены и использованы для повышения эффективности защиты, например при передаче криптографических ключей.

Стеганография во все времена занимала свою нишу в обеспечении безопасности и сокрытии информации.

В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации возникли новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т.п. Это дает возможность говорить о синтезе нового направления – компьютерной стеганографии.

Как и любое новое направление, компьютерная стеганография, несмотря на большое количество открытых публикаций и ежегодные конференции, долгое время не имела единой терминологии. Ее главный термин – стегосистема был введен в 1996 году на конференции Hiding.

Стеганографическая система или стегосистема – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

При построении стегосистемы должны учитываться следующие положения:

1) противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;

2) если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;

3) потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

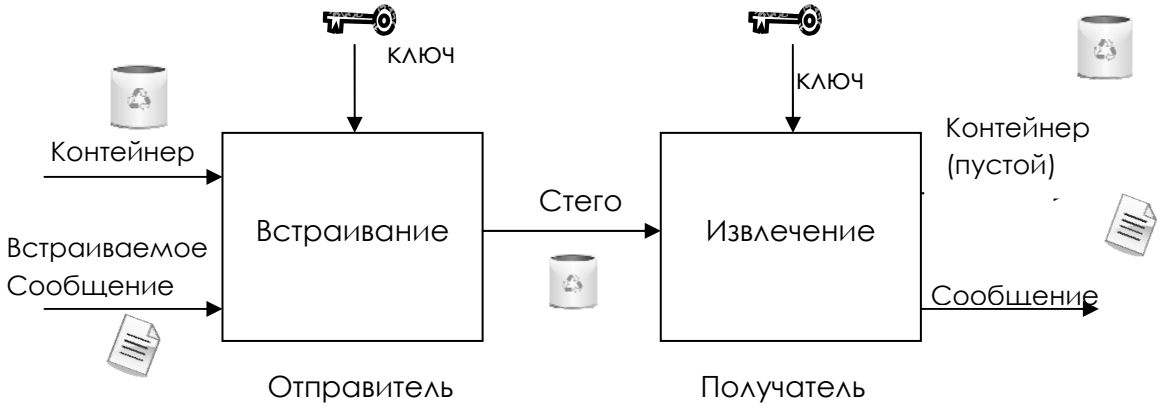



Рис. 14.1. Обобщенная модель стегосистемы

В качестве данных может использоваться любая информация: текст, сообщение, изображение и т.п.

В общем же случае целесообразно использовать слово "сообщение", так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

Контейнер – любая информация, предназначенная для сокрытия тайных сообщений.

Пустой контейнер – контейнер без встроенного сообщения; заполненный контейнер или стегоконтейнер, содержащий встроенную информацию.

Встроенное (скрытое) сообщение – сообщение, встраиваемое в контейнер.

Стеганографический канал или просто стегоканал – канал передачи стего.

Стегоключ или просто ключ – секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два вида:

- с секретным ключом;
- с открытым ключом.

В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, которые различаются таким образом, что с помощью вычислений невозможно вывести один ключ из

другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

Под цифровой стеганографией понимается сокрытие одной информации в другой. Причем сокрытие это должно реализоваться таким образом, чтобы, во-первых, не были утрачены свойства и некоторая ценность скрываемой информации, а во-вторых, неизбежная модификация информационного носителя не только не уничтожила смысловые функции, но и на определенном уровне абстракции даже не меняла их. Тем самым факт передачи одного сообщения внутри другого не выявляется традиционными методами.

В качестве носителя скрытой информации должен выступать объект (файл), допускающий искажения собственной информации, не нарушающие его функциональность. Внесенные искажения должны быть ниже уровня чувствительности средств распознавания.

В качестве носителя обычно используются файлы изображений или звуковые файлы. Такие файлы обладают большой избыточностью и, кроме того, обычно велики по размеру, обеспечивая достаточно места для сокрытия простого или форматированного текста. Скрываемое сообщение может быть простым набором чисел, изображением, простым или зашифрованным текстом.

Многие мультимедийные форматы имеют поля расширения, которые могут заполняться пользовательской информацией, а могут быть забиты нулями, в последнем случае их также можно использовать для хранения и передачи информации. Однако этот наивный способ не только не обеспечивает требуемого уровня секретности, но и не может прятать значительные объемы данных. Решение этих проблем нашлось в следующем подходе.

В графических файлах, аудио- и видеофайлах обычно содержится множество избыточной информации, которая совершенно не воспринимается органами чувств человека (следует, правда, заметить, что даже эта избыточная информация очень и очень далека от оригинала, поскольку, во-первых, данные всегда разбиваются на конечное число элементов, каждый из которых описывается конечным двоичным числом. Аналоговый же сигнал содержит потенциально бесконечное число сведений, которые обрубаются при оцифровке.) Поэтому при умеренной декрементации цифровых данных обычный человек в силу своего анатомического строения не может заметить разницы между исходной и модифицированной информацией.

Предположим, что в качестве носителя используется 24-битовое изображение размером 800x600 (графика среднего разрешения). Оно занимает около полутора мегабайта памяти (800x600x3 = 1440000 байт). Каждая цветовая комбинация тона (пикселя – точки) – это комбинация трех основных цветов: красного, зеленого и синего, которые занимают каждый по 1 байту (итого по 3 на пиксел). Если для хранения секретной информации использовать наименьший значащий бит (Least Significant Bits LSB) каждого байта, то получим по 3 бита на каждый пиксел. Емкость изображения носителя составит 800x600x3/8=180000 байт. При этом биты в каких-то точках будут совпадать с битами реального изображения, в других – нет, но, главное, что на глаз определить такие искажения практически невозможно.

Цифровая стеганография реализуется следующим образом: имеется какой-то цифровой файл – контейнер и сам файл-сообщение. Для обеспечения разрозненности и случайности значений зашифруем входное сообщение, так как шифровка обеспечивает большую степень защиты данных. Затем производится вставка сообщения в файл-контейнер. Затем

можно свободно передавать файл, но пароль для расшифровки должен быть заранее передан по независимому каналу получателю информации.

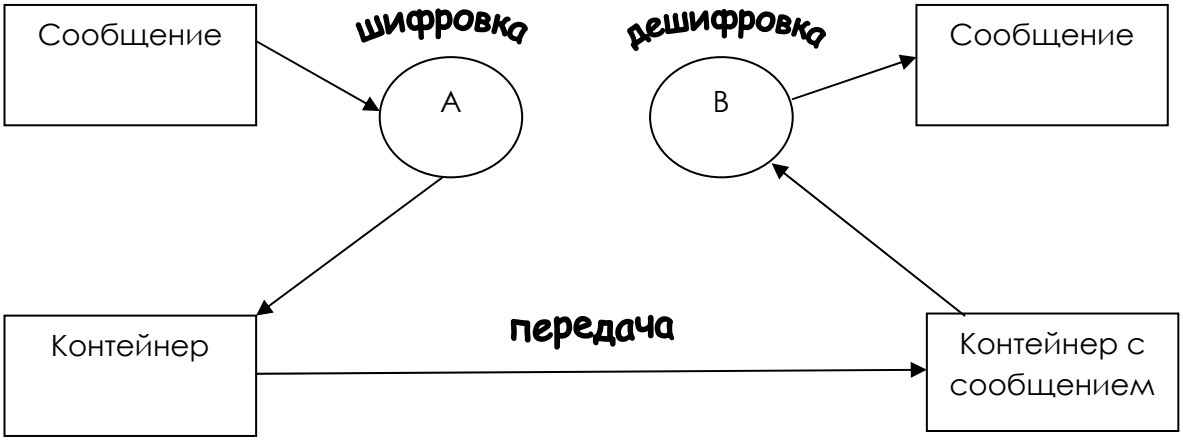



Рис. 14.2. Модель реализации цифровой стенографии

Самой главной задачей является обеспечить наибольшее сходство файла-контейнера с уже вложенным сообщением.

В младших битах изображений и других мультимедиа файлов имеются шумы – они распределены по всему файлу произвольным образом и, как правило, представляют собой случайные числовые значения.

Для обеспечения псевдослучайности при вставке файла в контейнер используют алгоритмы шифрования. Для большей надежности и схожести оригинала следует использовать изображения с шумами в младших разрядах – это изображения, полученные при помощи цифровой фотокамеры или со сканера. Такие изображения уже содержат внутри себя случайный шум, который дополнительно маскирует факт внедрения посторонней информации внутрь файла.

Кроме скрытой передачи сообщений, стеганография является одним из самых перспективных направлений, применяемых для аутентификации и маркировки авторской продукции. При этом часто в качестве внедряемой информации используются дата и место создания продукта, данные об

авторе, номер лицензии, серийный номер, дата истечения срока работы (удобно для распространения shareware-программ) и др. Эта информация обычно внедряется как в графические и аудиопроизведения, так и в защищаемые программные продукты. Все внесенные сведения могут рассматриваться как веские доказательства при рассмотрении вопросов об авторстве или для доказательства факта нелегального копирования и часто имеют решающее значение. Стеганография в сочетании с криптографией практически достигает 100% защищенности информации.

Введем важное понятие стегосистемы. Любая стегосистема должна отвечать следующим требованиям:

1. Свойства контейнера должны быть модифицированы, чтобы изменение невозможно было выявить при визуальном контроле. Это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стегосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего.

2. Стегосообщение должно быть устойчиво к искажениям, в том числе и злонамеренным. В процессе передачи изображение (звук или другой контейнер) может претерпевать различные трансформации: уменьшаться или увеличиваться, преобразовываться в другой формат и т.д. Кроме того, оно может быть сжато, в том числе и с использованием алгоритмов сжатия с потерей данных.

3. Для сохранения целостности встраиваемого сообщения необходимо использование кода с исправлением ошибки.

4. Для повышения надежности встраиваемое сообщение должно быть продублировано.

***Приложения***

В настоящее время можно выделить три тесно связанных между собой и имеющих одни корни направления приложения стеганографии: сокрытие данных (сообщений), цифровые водяные знаки и заголовки.

Сокрытие внедряемых данных, которые в большинстве случаев имеют большой объем, предъявляет серьезные требования к контейнеру: размер контейнера в несколько раз должен превышать размер встраиваемых данных.

Цифровые водяные знаки используются для защиты авторских или имущественных прав на цифровые изображения, фотографии или другие оцифрованные произведения искусства. Основными требованиями, которые предъявляются к таким встроенным данным, являются надежность и устойчивость к искажениям.

Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков.

Третье приложение, заголовки, используется в основном для маркирования изображений в больших электронных хранилищах (библиотеках) цифровых изображений, аудио - и видеофайлов.

В данном случае стеганографические методы используются не только для внедрения идентифицирующего заголовка, но и иных индивидуальных признаков файла.

Внедряемые заголовки имеют небольшой объем, а предъявляемые к ним требования минимальны: заголовки должны вносить незначительные искажения и быть устойчивы к основным геометрическим преобразованиям.

***Ограничения***

Каждое из перечисленных выше приложений требует определенного соотношения между устойчивостью встроенного сообщения к внешним воздействиям (в том числе и стегоанализу) и размером самого встраиваемого сообщения. Для большинства современных методов, используемых для сокрытия сообщения в цифровых контейнерах, имеет место следующая зависимость надежности системы от объема встраиваемых данных.


Рис. 14.3. Зависимость надежности системы от объема встраиваемых данных

Данная зависимость показывает, что при увеличении объема встраиваемых данных снижается надежность системы (при неизменности размера контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемых данных.

***Контейнеры***

Существенное влияние на надежность стегосистемы и возможность обнаружения факта передачи скрытого сообщения оказывает выбор контейнера. Например, опытный глаз цензора с художественным образованием легко обнаружит изменение цветовой гаммы при внедрении

сообщения в репродукцию «Мадонны» Рафаэля или «Черного квадрата» Малевича.

По протяженности контейнеры можно подразделить на два типа: непрерывные (потоковые) и ограниченной (фиксированной) длины. Особенностью потокового контейнера является то, что невозможно определить его начало или конец. В непрерывном потоке данных самая большая трудность для получателя – определить, когда начинается скрытое сообщение. При наличии в потоковом контейнере сигналов синхронизации или границ пакета, скрытое сообщение начинается сразу после одного из них. В свою очередь, для отправителя возможны проблемы, если он не уверен в том, что поток контейнера будет достаточно долгим для размещения целого тайного сообщения. При использовании контейнеров фиксированной длины отправитель заранее знает размер файла и может выбрать скрывающие биты в подходящей псевдослучайной последовательности. На практике чаще всего используются контейнеры фиксированной длины, как это отмечалось выше, но такие контейнеры имеют ограниченный объем и иногда встраиваемое сообщение может не поместиться в файл-контейнер. Другой недостаток заключается в том, что расстояния между скрывающими битами равномерно распределены между наиболее коротким и наиболее длинным заданными расстояниями, в то время как истинный случайный шум будет иметь экспоненциальное распределение длин интервала. Конечно, можно породить псевдослучайные экспоненциально распределенные числа, но этот путь обычно слишком трудоемок. Однако на практике чаще всего используются именно контейнеры фиксированной длины, как наиболее распространенные и доступные.

Возможны следующие варианты контейнеров:

1. Контейнер генерируется самой стегосистемой. Примером может служить программа MandelSteg, в которой в качестве контейнера для

встраивания сообщения генерируется фрактал Мандельброта. Такой подход можно назвать конструирующей стеганографией.

2. Контейнер выбирается из некоторого множества контейнеров. В этом случае генерируется большое число альтернативных контейнеров, чтобы затем выбрать наиболее подходящие для сокрытия сообщения. Такой подход можно назвать селектирующей стеганографией. В данном случае при выборе оптимального контейнера из множества сгенерированных важнейшим требованием является естественность контейнера. Единственной же проблемой остается то, что даже оптимально организованный контейнер позволяет спрятать незначительное количество данных при очень большом объеме самого контейнера.

3. Контейнер поступает извне. В данном случае отсутствует возможность выбора контейнера и для сокрытия сообщения берется первый попавшийся контейнер, не всегда подходящий к встраиваемому сообщению. Назовем это безальтернативной стеганографией.

***Методы сокрытия информации***

В настоящее время наиболее распространенным, но наименее стойким является метод замены наименьших значащих битов или LSB-метод. Он заключается в использовании погрешности дискретизации, которая всегда существует в оцифрованных изображениях или аудио- и видеофайлах. Данная погрешность равна наименьшему значащему разряду числа, определяющему величину цветовой составляющей элемента изображения (пикселя). Поэтому модификация младших битов в большинстве случаев не вызывает значительной трансформации изображения и не обнаруживается визуально. Более подробно LSB-метод описан в статье В.Н. Кустова и А.А. Федчука «Методы встраивания скрытых сообщений» («Защита информации. Конфидент», № 3, 2000, стр. 34).

Другим популярным методом встраивания сообщений является использование особенностей форматов данных, применяющих сжатие с потерей данных (например, JPEG). Этот метод (в отличие от LSB) более стоек к геометрическим преобразованиям и обнаружению канала передачи, так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения. Более подробно этот метод описан в статье С.Ф. Быкова «Алгоритм сжатия JPEG с позиции компьютерной стеганографии» («Защита информации. Конфидент», № 3, 2000, стр. 26).

Для встраивания цифровых водяных знаков используются более сложные методы.

***Цифровые водяные знаки***

В современных системах формирования цифровых водяных знаков используется принцип встраивания метки, являющейся узкополосным сигналом, в широком диапазоне частот маркируемого изображения. Указанный метод реализуется при помощи двух различных алгоритмов и их возможных модификаций. В первом случае информация скрывается путем фазовой модуляции информационного сигнала (несущей) с псевдослучайной последовательностью чисел. Во втором - имеющийся диапазон частот делится на несколько каналов, и передача производится между этими каналами. Относительно исходного изображения метка является некоторым дополнительным шумом, но так как шум в сигнале присутствует всегда, его незначительное возрастание за счет внедрения метки не дает заметных на глаз искажений. Кроме того, метка рассеивается по всему исходному изображению, в результате чего становится более устойчивой к вырезанию.

В настоящее время компьютерная стеганография продолжает развиваться: формируется теоретическая база, ведется разработка новых,

более стойких методов встраивания сообщений. Среди основных причин наблюдающегося всплеска интереса к стеганографии можно выделить принятые в ряде стран ограничения на использование сильной криптографии, а также проблему защиты авторских прав на художественные произведения в цифровых глобальных сетях. Поэтому в ближайшее время можно ожидать новых публикаций и разработок в этой области.

## Тема 15. Технические средства и технологии защиты информационных систем безопасности от электромагнитного терроризма

Практика эксплуатации интегрированных систем безопасности (ИСБ) показывает, что, несмотря на присущую этим системам высокую эффективность эксплуатации, их высокое качество, каждая система защиты, ядром которой является персональный компьютер в силу его присутствия, становится уязвимой для электромагнитных каналов воздействия, иначе такого рода терроризм называют также силовым деструктивным воздействием (СДВ). Под СДВ понимают, например, резкий всплеск напряжения в сетях питания, коммуникаций или сигнализаций у ИСБ, что может привести к сбоям в работе оборудования, даже к его деградации, если амплитуда всплеска этого напряжения, длительность, энергия превысят порог безопасности.

Заметим, что СДВ могут иметь также и стихийный характер (наряду с преднамеренным).

В настоящее время под электромагнитным оружием понимают всякое техническое средство СДВ, которое способно дистанционно, без лишнего шума, поразить практически любую систему безопасности, в том числе ИСБ.

Для этого взломщику необходимо обеспечить соответствующую мощность электромагнитного импульса. Существенно повышает скрытность нападения тот факт, что анализ повреждения в уничтоженном оборудовании не позволяет однозначно идентифицировать причину повреждения, ибо причиной может быть как преднамеренное (взлом), так и непреднамеренное повреждение, типа индукции от удара молнии, что позволит злоумышленнику многократно применять методы СДВ.

Проведенный анализ показывает, что ПК или любое другое электронное оборудование, подвергаются СДВ по трем основным каналам воздействия: по сети питания, по проводным линиям, по эфиру с помощью мощных коротких электромагнитных импульсов. По принципу ввода энергии используются либо контактные, либо бесконтактные каналы СДВ.

Для проникновения энергии СДВ по сети питания имеются два основных канала: кондуктивный путь через вторичный источник питания (ВИП), наводки через паразитные емкостные и индуктивные связи, как внутренние, так и внешние (например, через сигнальные цепи и линии связи). Для проникновения СДВ по проводным линиям необходимо преодолеть предельную поглощающую способность компонентов, реализованных во входных цепях, – микросхем, транзисторов, диодов. Эти комплектующие деградируют уже при воздействии короткого импульса (10–1000 нс), так что для СДВ по проводным каналам требуется энергия на несколько порядков ниже, чем по сети питания, и СДВ по этим каналам может быть реализовано простыми техническими средствами («электромагнитное ружье» может воздействовать, например, как на охранную сигнализацию внешнего периметра, так и на блок процессора ПК).

Однако наиболее скрытым и наиболее эффективным является канал СДВ по эфиру с использованием мощного короткого электромагнитного импульса от компактных электромагнитных технических средств, размещаемых за пределами объекта атаки, хорошо замаскированных. В качестве такого средства может быть взят генератор с виртуальным катодом – виркатор или СВЧ-генератор, оснащенный специальной антенной с системой направленного свойства, или генератор со взрывным сжатием магнитного поля. Мощный импульс, тем не менее, может при атаке на объект воздействовать на все компоненты в пределах зоны электромагнитного воздействия и на все контуры, образованные

связями между компонентами оборудования, поэтому технические средства СДВ наносят глобальные поражения, оправдывая название «электромагнитной бомбы».

Ниже приводится подробный систематизированный перечень технических средств защиты (ТСЗ) от СДВ по цепям питания, по проводным линиям и от электромагнитного СДВ по эфиру.

*Рекомендации по защите систем безопасности*
*от силового деструктивного воздействия*

Проведенный анализ показывает, что в настоящее время основным каналом силового деструктивного воздействия продолжает оставаться сеть питания. Поэтому в таблице 15.1 приведены основные характеристики и особенности комплексных технических средств защиты (ТСЗ) от силового деструктивного воздействия по цепям питания, представленных на российском рынке.

Таблица 15.1. Основные характеристики комплексных ТСЗ от СДВ по цепям питания

| Показатели | Комплексные ТСЗ от СДВ по цепям питания | | | | |
|---|---|---|---|---|---|
| | без гальванической развязки | | | с гальванической развязкой | |
| | для защиты вводов в здание | для поэтажной защиты силовой сети, защиты помещений и потребителей | для защиты отдельных помещений и офисов с компенсацией провалов и всплесков напряжения | для защиты вводов в здание | для защиты отдельных помещений, офисов, мощных потребителей |
| 1 | 2 | 3 | 4 | 5 | 6 |
| Защита от помех с энергией кДж/ Ом | | 500 | 100 | | 500 |
| в том числе для ввода кабельного воздушного | 100<br>900 | | | 100<br>900 | |

*Окончание табл. 15.1*

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| Реализация | Супер-фильтры СПФ-65-4/5 СПФ-130-4/5 | Супер-фильтры СПФ-15/30/40-4/5 | Помехозащи-щенные устройства электропитания УЭП 5/10/15-3 Кондиционеры КН 500, корректоры напряжения КНТ 15/30/40/65/130 | Трансформаторные подстанции ТПП 25/50/100; трансфильтры ТФТ25/50/10 | Трансфильты трехфазные ТФТ 5/10 (4-проводный вход, 5-проводный выход) |
| Основные компоненты | Силовые Конденсаторы с демпфирующими цепями | Модуль выравнивания потенциалов линий | Корректор напряжения | Помехоподавляющий изолирующий трансформатор | Помехоподавляющий изолирующий трансформатор |
| Особенности | Суперфильтры выпускаются в 4- или 5- проводном исполнении | Производится модификация суперфильтра сузлами для защиты от СДВ | Имеется модификация для сетей с большой асимметрией напряжения по фазам питающей сети | Возможно применение упрощенной схемы заземления | Модификация ТФ 500 используется для защиты от НСД, ТФ 1000 – для защиты реакторов АЭС |

Указанные в таблице отечественные ТСЗ от СДВ в настоящее время выпускаются ЗАО «ЭМСОТЕХ» и рядом предприятий ВПК. Из импортных ТСЗ, представленных на российском рынке, можно отметить продукцию зарубежных фирм «APC», «Tripplite», «Upsonic», «Sola», «Best», «Elteco», «Victron» и др.

Таблица 15.2. Основные рекомендации по защите систем безопасности от СДВ

| N п\п | Рекомендации по защите систем безопасности от СДВ | Примечание |
|---|---|---|
| Общие организационно - технические мероприятия | | |
| 1 | Провести анализ схем электроснабжения внутренних и внешних коммуникационных каналов объекта, а также линий аварийно - пожарной сигнализации для выявления возможных путей СДВ | К анализу привлекаются квалифицированные электрики и связисты |
| 2 | Произвести разделение объекта на зоны защиты и рубежи обороны:<br>1-й рубеж – защита по периметру объекта;<br>2-й рубеж – защита поэтажная;<br>3–й рубеж – индивидуальная защита | Для небольших объектов (офисов) 1-й рубеж может отсутствовать, а 2-й рубеж сократиться до защиты отдельного помещения |
| 3 | После проведения монтажа системы безопасности провести тестирование на реальные воздействия | Для тестирования используются специальные имитаторы СДВ |
| 4 | Разработать соответствующие документы ограничительного характера, направленные на ограничение возможности использования ТС СДВ | Например, запретить использование розеток выделенной сети для пылесосов и другого оборудования, в которые могут быть встроены ТС СДВ |
| Защита систем безопасности от СДВ по сети питания | | |
| 5 | На все фидеры, выходящие за пределы контролируемой службой безопасности (СБ) зоны, установить групповые устройства защиты (ГУЗ) от СДВ | ГУЗ установить в зонах, подконтрольных СБ |
| 6 | На сеть электропитания серверов, систем охраны и сигнализации объекта установить защиту | В зависимости от решаемых задач объем индивидуальной защиты может быть существенно расширен |
| 7 | Щитки питания, распределительные щиты, розетки, клеммы, заземления и т.п. необходимо размещать в помещениях, контролируемых СБ | Не рекомендуется установка розеток в слабо контролируемых помещениях (буфет, склад, гардероб и т.п.) |
| 8 | Используя анализатор неоднородности линии снять контрольный «портрет» электросети | Контрольный «портрет» снимается после завершения монтажа сети |
| 9 | Для выявления несанкционированного подключения к сети надо контролировать «текущий портрет» для сравнения с контрольным портретом | Этот метод контроля особенно эффективен для обнаружения ТСС ДВ последовательного типа |

*Продолжение табл. 15.2*

| N п\п | Рекомендации по защите систем безопасности от СДВ | Примечание |
|---|---|---|
| 10 | Текущее обслуживание и ремонт электрооборудования должны проводиться под контролем сотрудников СБ | |
| 11 | Доступ к щитам и другим элементам электрооборудования должен быть ограничен | Ограничение определяется соответствующими документами и мероприятиями |
| 12 | Все электрооборудование, в том числе и бытового назначения, должно тщательно поверяться | Особое внимание обратить на UPS, микроволновые печи, пылесосы, кондиционеры, аппараты для сварки |
| 13 | Организовать круглосуточный мониторинг сети электропитания с одновременной записью в журнале всех сбоев и повреждений оборудования, фиксацией времени сбоев и характера дефектов. Путем анализа результатов возможно своевременное обнаружение факта НСД | В качестве регистраторов можно использовать широкий спектр приборов от простых счетчиков импульсов до комплексов с ПК |
| 14 | При закупке электрооборудования систем безопасности необходимо обращать внимание на степень его защиты от импульсных помех. Обычное оборудование должно иметь класс устойчивости не ниже А, ответственное – не ниже В | По стандарт IEEE 587-1980 помеха класса А:0.5 мкс/6кВ/200 А/1,6 Дж класса В 0,5 мкс/6 кВ/500 а/4 Дж |
| Защита системы безопасности от СДВ по проводным линиям | | |
| 15 | На все проводные линии связи и аварийно-охранно-пожарной сигнализации, которые выходят за пределы зоны контроля СБ, установить устройства защиты от СДВ | Места для установки шкафов с УЗ выбираются в зонах, подконтрольных СБ |
| 16 | Для выявления несанкционированного подключения к проводным линиям с помощью анализатора неоднородности снять контрольный «портрет» сети. Систематическое сравнение текущего и контрольного «портретов» сети обеспечивает обнаружение НСД | Контрольный «портрет» снимается только после полного завершения монтажа сети проводных линий |
| 17 | Ремонтные работы и текущее обслуживание оборудования, линий связи и цепей сигнализации системы безопасности необходимо производить под контролем СБ | |
| 18 | Доступ к линиям связи и сигнализации, датчикам, кросспанелям, мини-АТС и другим элементам системы безопасности должен быть ограничен | Ограничение обеспечивается соответствующими документами и техническими средствами |

*Окончание табл. 15.2*

| N п\п | Рекомендации по защите систем безопасности от СДВ | Примечание |
|---|---|---|
| 19 | Нежелательно размещение оборудования сети (маршрутизаторов, АТС, кросса и т.п.) на внешних стенах объекта | В этом случае велика вероятность успешного СДВ из неконтролируемой зоны |
| 20 | Желательно не применять общепринятую топологию прокладки проводных линий связи и сигнализации вдоль стены параллельно друг другу, так как она является идеальной для атаки на объект с помощью ТС СДВ с бесконтактным емкостным инжектором. Целесообразно использовать многопарные кабели связи с «вигами парами» | В противном случае с помощью плоского накладного электрода и ТС СДВ оборудование может быть выведено из строя злоумышленником за 10...30 с |
| 21 | При закупке оборудования систем безопасности необходимо учитывать степень его защиты от импульсных помех. Минимальная степень защищенности должна соответствовать ГОСТ Р 50716-95 при степени жесткости испытаний 3−4 | Для более подробной информации см. журнал «Конфидент. Защита информации» (1998 N2) |
| Защита систем безопасности от электромагнитного СДВ по эфиру | | |
| 22 | Основным методом защиты от СДВ является экранирование на всех рубежах как аппаратуры, так и помещений. При невозможности экранирования всего помещения необходимо прокладывать линии связи и сигнализации в металлических трубах или по широкой заземленной полосе металла, а также использовать специальные защитные материалы | В качестве экранирующего материала можно использовать металл, ткань, защитную краску, пленку, специальные материалы |
| 23 | Многорубежная защита от СДВ по эфиру организуется аналогично защите по сети питания и по проводным линиям | |
| 25 | В защищенных помещениях особое внимание обратить на защиту по сети питания, используя в первую очередь разрядники и экранированный кабель питания | Обратить внимание, что традиционные фильтры питания от помех здесь не спасают от СДВ |

Таким образом, СДВ, реализуемое по проводным и беспроводным каналам, а также по сетям питания, в настоящее время является серьезным оружием против систем защиты объектов, в частности интегрированных систем безопасности и защищенных помещений. Это оружие оправдывает свое название «электромагнитной бомбы» и по эффективности воздействия является более грозным, чем программное разрушающее оружие для компьютерных сетей. Аналитические исследования показывают, что новые технологии делают технические средства силового деструктивного воздействия все более перспективными для применения и требуют к себе большего внимания в первую очередь со стороны служб безопасности и разработчиков систем защиты.

## Тема 16. Вредоносные вирусные программы. Современные технические средства борьбы с компьютерными вирусами

### *Использование компьютерных вирусов для организации каналов утечки и несанкционированного доступа к информации*

Необходимо отметить, что компьютерные вирусы (КВ), или, как более правильно, программные вирусы (ПВ), являются в настоящее время наиболее эффективным средством доставки и внедрения различных разведывательных программ.

Под программным вирусом понимается автономно функционирующая программа, обладающая способностью к самовключению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях (ИВС) и отдельных ЭВМ. Программные вирусы представляют собой весьма эффективное средство реализации практически всех угроз безопасности ИВС.

Предшественниками ПВ принято считать так называемые «троянские программы», тела которых содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям. Наиболее распространенной разновидностью «троянских программ» являются широко известные программы массового применения (редакторы, игры, трансляторы и т.п.), в которые встроены так называемые логические бомбы, срабатывающие по наступлении некоторого события. В свою очередь, разновидностью логической бомбы является «бомба с часовым механизмом», запускаемая в определенные моменты времени. Следует отметить, что «троянские программы» не являются саморазмножающимися и распространяются по ИВС самими

программистами, в частности посредством общедоступных банков данных и программ (BBS).

Заражение программы (исполняемого файла применительно к наиболее распространенной операционной системе PC-подобных ПЭВМ MS DOS), как правило, выполняется таким образом, чтобы вирус получил управление раньше самой программы.

«Первичное заражение» происходит в процессе поступления инфицированных программ из памяти одной машины в память другой, причем в качестве средства перемещения этих программ могут использоваться как магнитные носители (дискеты), так и каналы ИВС (например, в упоминавшихся BBS). Вирусы, использующие для размножения каналы ИВС, принято называть сетевыми.

Цикл жизни вируса обычно включает следующие периоды: внедрение, инкубационный, репликация (саморазмножение) и проявление. В течение инкубационного периода вирус пассивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например необратимую коррекцию информации на магнитных носителях (жестких либо гибких).

Физическая структура вируса достаточно проста. Он состоит из головы и, возможно, хвоста. Под головой вируса понимается его компонент, получающий управление первым. Хвост – это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называют несегментированными, тогда как вирусы, содержащие голову и хвост, – сегментированными.

По характеру размещения в памяти ПЭВМ с операционной системой MS DOS принято делить вирусы на файловые нерезидентные, файловые резидентные, бутовые, гибридные и пакетные.

Файловый нерезидентный вирус целиком размещается в исполняемом файле, в связи с чем он активизируется только в случае

активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе. При этом выбор очередного файла для заражения осуществляется вирусом посредством поиска по каталогу.

Файловый резидентный вирус отличается от нерезидентного тем, что заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память (ОП) ПЭВМ. С чисто технологической точки зрения ОП можно считать файлом, к которому применимы все описанные выше способы имплантации. Однако резидентный вирус отличается от нерезидентного как логической структурой, так и общим алгоритмом функционирования. В связи с существенно более универсальной по сравнению с нерезидентными вирусами общей схемой функционирования резидентные вирусы могут реализовывать самые разные способы инфицирования. Наиболее распространенными способами являются инфицирование запускаемых программ, а также файлов при их открытии или чтении.

Одной из разновидностей резидентных вирусов являются так называемые бутовые вирусы. Отличительной особенностью последних является инфицирование загрузочного (бут-сектора) магнитного носителя (гибкого или жесткого диска). При этом инфицированными могут быть как загружаемые, так и незагружаемые дискеты.

Механизм инфицирования, реализуемый бутовыми вирусами, таков: при загрузке MS DOS с инфицированного диска вирус в силу своего положения на нем (независимо от того, с дискеты или винчестера производится загрузка) получает управление и копирует себя в ОП. Затем он модифицирует вектор прерываний таким образом, чтобы прерывания по обращению к диску обрабатывались собственным обработчиком прерываний вируса, и запускает загрузчик ОС. Благодаря перехвату прерываний бутовые вирусы могут реализовать столь же широкий набор

способов инфицирования и целевых функций, сколь и файловые резидентные вирусы.

Близость механизмов функционирования бутовых и файловых резидентных вирусов сделала возможным и естественным появление файлово-бутовых, или гибридных, вирусов, инфицирующих как файлы, так и бут-секторы. Особенностью пакетного вируса является размещение его головы в пакетном файле. При этом голова представляет собой строку или программу на языке управления заданиями ОС.

Сетевые вирусы, называемые также автономными репликативными программами или, для краткости, репликаторами, используют для размножения средства сетевых операционных систем ИВС.

Классическим примером реализации процесса размножения с использованием только стандартных средств электронной почты является широко известный репликатор Морриса, выведший из строя ИВС Интернета.

Эффекты, вызываемые вирусами в процессе реализации ими целевых функций, принято делить на следующие целевые группы:

- искажение информации в файлах либо в таблице размещения файлов (FAT), которое может привести к разрушению файловой системы MS DOS в целом; имитация сбоев аппаратных средств;

- инициирование ошибок в программах пользователей или ОС и т.п.

Наиболее распространенным средством нейтрализации вирусов являются программные антивирусы. Антивирусы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на следующие группы: детекторы, фаги, вакцины, прививки, ревизоры, мониторы.

Детекторы обеспечивают выявление вирусов посредством просмотра исполняемых файлов и поиска так называемых сигнатур − устойчивых

последовательностей байтов, имеющихся в телах известных вирусов. Наличие сигнатуры в каком-либо файле свидетельствует о его заражении соответствующим вирусом. Антивирус, обеспечивающий возможность поиска различных сигнатур, называют полидетектором. Фаги выполняют функции, свойственные детекторам, но, кроме того, «излечивают» инфицированные программы посредством «выкусывания» («пожирания») вирусов из их тел. По аналогии с полидетекторами, фаги, ориентированные на нейтрализацию различных вирусов, именуют полифагами.

В отличие от детекторов и фагов, вакцины по своему принципу действия напоминают сами вирусы. Вакцина имплантируется в защищаемую программу и запоминает ряд количественных и структурных характеристик последней. Если вакцинированная программа не была к моменту вакцинации инфицированной, то при первом же после заражения запуске произойдет следующее. Активизация вирусоносителя приведет к получению управления вирусом, который, выполнив свои целевые функции, передаст управление вакцинированной программе. В последней, в свою очередь, сначала управление получит вакцина, которая выполнит проверку соответствия запомненных ею характеристик аналогичным характеристикам, полученным в текущий момент. Если указанные наборы характеристик не совпадают, то делается вывод об изменении текста вакцинированной программы вирусом. Характеристиками, используемыми вакцинами, могут быть длина программы, ее контрольная сумма и т.п.

Принцип действия прививок основан на учете того обстоятельства, что любой вирус, как правило, помечает инфицируемые программы каким-либо признаком, чтобы не выполнять их повторное заражение. Прививка, не внося никаких других изменений в текст защищаемой программы, помечает ее тем же признаком, что и вирус, который, таким образом, после

активизации и проверки наличия указанного признака считает ее инфицированной и «оставляет в покое».

Ревизоры обеспечивают слежение за состоянием файловой системы, используя для этого подход, аналогичный реализованному в вакцинах. Программа-ревизор в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра файлов. Если при этом обнаруживается, что согласно имеющейся системной информации файл с момента предшествующего просмотра не обновлялся пользователем, а сравниваемые наборы характеристик не совпадают, то файл считается инфицированным.

Монитор представляет собой резидентную программу, обеспечивающую перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающую у пользователей подтверждение на выполнение операций, следующих за прерыванием. В случае запрета или отсутствия подтверждения монитор блокирует выполнение пользовательской программы.

Антивирусы рассмотренных типов существенно повышают вирусозащищенность отдельных ПЭВМ и ИВС в целом, однако в связи со свойственными им ограничениями, естественно, не являются панацеей. Так, для разработки детекторов, фагов и прививок нужно иметь тексты вирусов, что возможно только для выявленных вирусов. Вакцины обладают потенциальной способностью защиты программ не только от известных, но и от новых вирусов, однако обнаруживают факт заражения только в тех случаях, если сами были имплантированы в защищаемую программу раньше вируса. Результативность применения ревизоров зависит от частоты их запуска, которая не может быть выше 1−2 раз в день

в связи со значительными затратами времени на просмотр файлов (порядка 30...60 мин применительно к жесткому! диску емкостью 80 Мбайт). Мониторы контролируют процесс функционирования пользовательских программ постоянно, однако характеризуются чрезмерной интенсивностью ложных срабатываний, которые развивают у оператора «рефлекс подтверждения» и тем самым по существу минимизируют эффект от такого контроля. Следует также учитывать, что принципы действия и тексты любых антивирусов доступны разработчикам ПВ, что позволяет им создавать более изощренные вирусы, способные успешно обходить все известные защиты.

В таблице 16.1 приведены общие характеристики компьютерных вирусов, потенциально опасных с точки зрения несанкционированного доступа к информации.

Таблица 16.1. Характеристики компьютерных вирусов

| Класс вируса | Виды вируса | Характер воздействия |
|---|---|---|
| Не повреждающие файловую структуру | Размножающиеся в ОЗУ | Имитация неисправности процессора, НМД, принтера, портов, дисплея, клавиатуры. |
| | | Формирование на терминале текстовых и графических сообщений |
| | Раздражающие оператора | Синтез речи, формирование мелодии и звуковых спецэффектов |
| | Сетевые | Переключение режимов настройки клавиатуры, дисплея, принтера, портов |
| Повреждающие файловую структуру | Повреждающие пользовательские программы и данные. | Разрушение исходных текстов программ, библиотек компиляторов, искажение баз данных, текстовых документов, графических изображений и электронных таблиц |
| | Разрушающие системную информацию (в том числе криптовирусы) | Разрушение логической системы диска, искажение структуры заполнения носителя, форматирование носителей, повреждение файлов ОС |
| Действующие на аппаратуру и оператора | Выводящие из строя аппаратуру | Выжигание люминофора, повреждение микросхем, магнитных дисков, принтера |
| | Действующие на оператора | Воздействие на психику оператора и т.п. |

Как видно из таблицы 16.1, наибольший вред с точки зрения утечки информации могут нанести криптовирусы, поскольку они в состоянии пробить брешь даже в таком мощном средстве обороны, как криптозащита. Например, в момент проставления электронной подписи криптовирусы могут перехватить секретные ключи и скопировать их в заданное место.

Как правило, против таких криптовирусов можно использовать только одну защиту – загрузку с чистой дискеты и использование чистого (фирменного) программного продукта.

На российском рынке в настоящее время присутствуют программные средства обнаружения и обезвреживания компьютерных вирусов, представленные в таблице 16.2.

Таблица 16.2. Современные антивирусные программные средства

| Средство защиты | Назначение | Программы | Принцип действия |
|---|---|---|---|
| Детектор | Обнаружение зараженных вирусом файлов | ViruScan, NetScan, Aidstest | Поиск участка кода, принадлежащего известному вирусу |
| Фильтр | Перехват «подозрительных» обращений к ОС и сообщение о них пользователю | FluShot Plus, Anti4Us, Floserum, Disk Monitor, Vshield | Контроль действий, характерных для поведения вируса |
| Доктор (фаг) | «Лечение» зараженных программ или дисков | Clear-Up, M-Disk, Aidstest Dr. Web | Уничтожение тела вируса |
| Ревизор | Постоянная ревизия целостности (неизменности) файлов | Validate | Запоминание сведений о состоянии программ и системных областей дисков, сравнение их состояния с исходным |
| Доктор-ревизор | Обнаружение и «лечение» зараженных файлов | Dr. Web и др. | Обнаружение изменений в файлах и дисках и возврат их в исходное состояние |

Анализ современных антивирусных программ показывает, что в последнее время наметилась явно выраженная тенденция к интеграции различных видов программ в единое программное средство с функциями детектора-ревизора-доктора, что делает это средство удобным для пользователя. Однако приходится констатировать, что в настоящее время абсолютной защиты от неизвестных вирусов не существует, поэтому антивирусные программы постоянно обновляются, как правило, не реже одного раза в месяц. Надежно защитить компьютер от вирусов может только сам пользователь. В первую очередь необходимо правильно организовать работу и избегать бесконтрольной переписи программ с других компьютеров. Далее, особую бдительность необходимо проявлять при работе с выходом в компьютерную сеть, где вероятность внедрения компьютерных вирусов резко возрастает. Учитывая то, что в основе большинства вредоносных программ присутствуют программные вирусы, последние всегда должны быть в поле зрения пользователя.

## СПИСОК ЛИТЕРАТУРЫ

***Основная литература***

1. Торокин А.А. Инженерно − техническая защита информации. − М.: Гелиос АРВ, 2005.

2. Титаренко Г.А., Брага В.В., Вдовенко Л.А. и др. (под ред. Г. Титаренко). Информационные технологии управления. Учебник для вузов. − М.: ЮНИТИ-ДАНА, 2005.

3. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение. − М.: Солон-Пресс, 2004.

4. Гринберг А.С., Горбачев Н.Н., Теплякова А.А. Защита информационных ресурсов государственного управления. Учебник для вузов. –М.: ЮНИТИ, 2003.

5. Гринберг А.С., Горбачев Н.Н., Бондаренко А.С. Информационные технологии управления. Учебник для вузов. − М.: ЮНИТИ, 2004.

6. Барсуков В.С. Безопасность: технологии, средства, услуги. − М.: КУДИЦ–ОБРАЗ, 2001.

7. Советов Б.Я., Яковлев С.А. Моделирование систем. Учебник для вузов. − М.: Высшая школа,1985.

***Дополнительная литература***

1. Артащенков Ю.М., Ковалев М.С., Котов Н.Н., Тюрин Е.П. Применение технических средств в борьбе с терроризмом − М.: НИЦ «Охрана» ГУВО МВД России,2000.

2. Теория и практика обеспечения информационной безопасности. Под ред. Зегжды П.Д. – М.: Изд-во Агентства «Яхтсмен», 1998.

3. Липаев В.В. Программно-техническая безопасность информационных систем. – М.: МИФИ, 1997.

4. Андрианов В.И., Соколов А.В. «Шпионские штучки – 2» или как сберечь свои секреты. – СПб.: Полигон, 1997.

5. Руководящий документ. Защита от НСД информации. Термины и определения. – М.: Гостехкомиссия России, 1992.

6. Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993.

7. Голенкевич Т.А. Прикладная теория надежность. – М.: Высшая школа, 1985.

# ОПИСАНИЕ КУРСА И ПРОГРАММА

## Цели и задачи курса

Согласно Федеральному закону «Об информации, информатизации и защите информации» защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб её собственнику, владельцу, пользователю и иному лицу.

В наше время стремительного развития новых информационных технологий, всеобщей компьютеризации, постоянно обостряющейся конкуренции различных товаропроизводителей, все более изощренными становятся методы взлома систем информационной безопасности, технические и интеллектуальные методы и средства несанкционированного доступа к информации различной физической природы, различной степени конфиденциальности и секретности, циркулирующей в информационных системах от локального до стратегического уровня.

В связи с этим, основной, главной целью курса «Современные технические методы и средства защиты информации» является выработка навыков у учащихся по формированию у них системного подхода к проблеме анализа и синтеза технических средств защиты информации от несанкционированного доступа. В результате освоения данного курса учащийся должен уметь оперативно и быстро выявить и классифицировать всевозможные каналы утечки информации, циркулирующей в информационной системе (ИС), исполняющей чаще всего функцию управления (ИУС) каким-либо объектом, подверженного угрозе безопасности информации.

Напомним, что под информационной системой мы понимаем взаимосвязанную совокупность средств, методов, персонала,

используемую для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Однако, современная концепция безопасности, действующая в рамках эффективного управления любой современной организацией, оперирует в подавляющем большинстве случаев, с автоматизированными информационными системами, т.е. с такими комплексами, каждый из которых включает в себя компьютерное и коммуникационное оборудование, программное обеспечение, диагностики средства, информационные ресурсы, а так же системный персонал.

К числу побочных целей данного курса, в рамках выше изложенного системного подхода к проблеме синтеза, методов и средств защиты информации от несанкционированного доступа, могут быть отнесены следующие вопросы:

1) Умение квалифицировано и оперативно произвести анализ и общепринятую классификацию видов умышленных угроз для безопасности информации;

2) Умение квалифицированно и оперативно выбирать или синтезировать системы информационной безопасности (СИБ), адекватно реагирующие на возможные в данной ситуации виды умышленных угроз безопасности информации;

3) Умение квалифицированно и оперативно выбирать или синтезировать нужный в конкретной ситуации по обеспечению информационной безопасности технические средства защиты;

4) Умение квалифицированно и оперативно оценит надёжность применимой в данной ситуации системы информационной безопасности.

Напомним, что под безопасностью информационной системы мы понимаем защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс её функционирования, от попыток хищения (несанкционированного получения) информации, модификации

или физического разрушения её компонентов, высокий уровень противостояния данной информационной системы различным возмущающим воздействиям.

Приведем стандартный перечень видов умышленных угроз безопасности информации:

- пассивные и активные угрозы;
- внутренние и внешние угрозы;
- утечка конфиденциальной информации;
- компрометация информации.
-несанкционированное использование информационных ресурсов;
-ошибочное использование информационных ресурсов;
- несанкционированный обмен информацией между абонентами;
-отказ от информации;
-нарушение информационного обслуживания;
-незаконное использование привилегий;

Заметим, что кроме пассивных, активных, внешних и внутренних угроз, настоящих достаточно общий характер, все остальные приведенные угрозы, в основном характерны для безопасности нормального функционирования используемых конкретных информационных систем, например, информационно-вычислительных систем, различных автоматизированных систем управления, систем управления, использующих искусственный интеллект и т.д.

Отметим, что под выше упомянутыми средствами мы понимаем специальные приборы, оборудование, сооружения, создающие препятствия несанкционированному доступу к информационным данным. Это могут быть различные средства физического препятствия, сигнальные системы, средства визуального наблюдения, магнитные карты, биологические идентификаторы и т.д. Но, например, криптографические

средства защиты информации, можно рассматривать и как технические средства защиты информации, и как аппаратно-программное.

Изложенные выше главные и побочные цели курса, порождают целый ряд задач, с необходимостью решений которых сталкиваются специалисты защиты информации (мы приведем их далеко не полный перечень).

Заметим, что понятие «информационная безопасность» является понятием чрезвычайно широким, всеобъемлющим, глобальным, и поэтому нет смысла попытаться выделить одну глобальную, главную задачу, ибо она будет носить чересчур общий характер, поэтому приведем перечень задач курса, наиболее интересных с нашей точки зрения. Ввиду большого масштаба всей проблемы, этот список не может быть полным.

1.освоение основных теоретических и практических навыков для организации процедуры моделирования макросистем и микросистем, используемых в информационных технологиях управления системами информационной безопасности.

2.уметь квалифицировано и оперативно осуществить процесс синтеза модели, применяемой информационной системой на основе классического и системного подхода.

3.уметь квалифицировано и оперативно составлять структурные схемы технических устройств, используемых в данной ситуации и представляющих собой потенциальные объекты взлома.

4.на основании структурных схем применяемых технических устройств выполнить расчеты надежности каждого технического устройства и расчет вероятности взлома применяемой информационной системы. Найти пути уменьшения вероятности взлома системы, в частности путем модификации структурных схем отдельных технологических устройств и модификации структурной схемы всей методы информационной системы данной задачи.

Курс «Современные технические методы и средства защиты информации» находит свое действенное применение в такой широкой области знаний, как информационная безопасность, защита информации.

Этот курс предназначен для реализации по магистерским программам «Обеспечение информационной» безопасности автоматизированных «систем», «Разработка и применение нанотехнологий на базе проектирования и управления системы качества промышленных предприятий».

Данный курс, может рассматриваться как обязательный для направления «автоматизация и управление», для всех остальных он может рассматриваться как курс по выбору.

## Инновационность курса

Инновационность курса касается таких элементов его содержания, как организация процедуры моделирования макросистем и микросистем, используемых в информационной безопасности. Моделирование должно производиться на базе системного подхода и с использованием известных в теории моделирования систем методик моделирования случайных величин, векторов а также с использованием методик типовых математических схем сложных систем: A-схем, D-схем, F-схем, P-схем, Q-схем, с успехом используемых в теории автоматизированных систем управления,

Но наибольшая степень инновационности, на наш взгляд, содержится в расчетах вероятности взлома системы, основывающихся на известных методах расчета надежности систем, использующих логические функции системы на базе структурной схемы системы.

При выполнении расчетов вероятности взлома системы, естественно, заранее должны известны вероятности взлома всех отдельных элементов

системы, или, по крайней мере, вероятности взлома комплексов системы, объединяющих её группы элементов.

Кроме того, в курсе достаточно подробно рассматриваются методы интегральной защиты информации, основанные на концепции интегральной безопасности, предполагающей обязательную непрерывность процесса обеспечения безопасности объекта, как во времени, так и по всему циклу технологической деятельности предприятия. Интегральная безопасность учитывает все возможные виды угроз, - блокирует одновременно все возможные каналы утечки.

Уделено внимание и достаточно новой технологии защиты информации и компьютерной сценографии, её основным положениям, техническим и программно-аппаратным методиками, использующих цифровые системы обработки звуковых сигналов, включающие фильтры низких частот, цифроаналоговые и аналогоцифровые преобразователи, цифровые процессоры радио-электронной аппаратуры

## Структура курса

Программа курса рассчитана на 104 часа (3 кредита), из которых лекционных занятий -40 часов, практических занятий-40часов, самостоятельной работы-24 часа - три контрольные работы, выполняемые в аудитории или дома в ограниченный срок времени.

ЛЕКЦИОННЫЕ ТЕМЫ.

1 лекция-2 часа

ТЕМА №1.Основные понятия теории защиты информации в измерительных системах и информационных технологиях управления объектом.

(4 часа)

ТЕМА №2.Виды умышленных угроз безопасности информации.

(2 часа)

ТЕМА №3.Методы и технические средства построения технических систем информационной безопасности, их структура.

(4часа)

ТЕМА №4.Криптографические методы защиты информации.

(2часа)

ТЕМА №5.Анализ и особенности каналов утечки и несанкционированного доступа к информации в технических информационных системах.

(2 часа)

ТЕМА №6.Аппаратная реализация современных технических методов несанкционированного доступа к информации.

(2 часа)

ТЕМА №7.Современные технические средства обнаружения угроз.

(2 часа)

ТЕМА №8.Современные технические средства обеспечения безопасности к каналах информационно-вычислительных систем, телекоммуникаций и ЭВМ.

(2 часа)

ТЕМА №9.Современные технологические средства защиты информации от несанкционированного доступа в сетях ЭВМ.

(4 часа)

ТЕМА №10.Основнык понятия моделирования больших систем. Математическое моделирование больших систем на основе математических систем: A-схем, D-схем, F-схем, P-схем, Q-схем.

(2 часа)

ТЕМА №11.Основные понятия теории надежности систем. Метод расчета надежности систем на базе построения логической функции системы.

(2 часа)

ТЕМА №12.Метод расчета вероятности взлома системы на основе логической функции системы.

(4 часа)

ТЕМА №13.Концепция интегральной защиты информации.

(2 часа)

ТЕМА №14.Компютерная стенография как перспективное, современное, техническое и программное средство защиты информации, от несанкционированного доступа.

(2 часа)

ТЕМА №15.Технические средства и технологии, информационных систем безопасности от электромагнитного терроризма.

(2 часа)

ТЕМА №16.Вредоносные вирусные программы. Современные технические средства борьбы с компьютерными вирусами.

(2 часа)

ТЕМА №17.Содержание метода временных диаграмм, его графическое представление. Исследование причин универсальности этого метода в задачах моделирования работы сложенных многоканальных систем управления безопасностью объектов.

(2 часа)

## ПЛАН СЕМИНАРСКИХ ЗАНЯТИЙ.

Семинар по теме№1 (2 часа)

Анализ основных технических средств для несанкционированного добывания информации.

Семинар по теме№2 (2 часа)

Сравнительные характеристики пассивных средств получения информации.

Сравнительные характеристики активных средств получения информации.

Семинар по теме№3 (2 часа)

Изучение основных положений концепции безопасности автоматизированных систем обработки информации.

Семинар по теме№4 (2 часа)

Симметрические криптосистемы: подстановки, перестановки, гаммирование, блочные шифры. Системы с открытым ключом. Алгоритм RSA.

Семинар по теме№5 (2 часа)

Сравнительные технические характеристики пассивных и активных средств незаконного получения информации. Методы защиты.

Семинар по теме№6 (2 часа)

Современные угрозы информации в информационно-вычислительных системах и телекоммуникационных каналах связи.

Семинар по теме№7 (2 часа)

Основы концепции интегральной безопасности объекта.

Семинар по теме№8 (2 часа)

Сравнительный анализ технических характеристик сканеров и нелинейных радиолокаторов при их применении для решения задач обнаружения радиопередатчиков в ближней зоне этих передатчиков.

Семинар по теме№9 (2 часа)

Анализ факторов, существенно влияющих на безопасность распределенных систем и анализ угроз для сетей ЭВМ.

Семинар по теме№10 (2 часа)

Разработка моделирующего алгоритма для системы безопасности, представленный в виде многоканальной Q-схемы.

Семинар по теме№10 (2 часа)

Процедура формализации систем («охраняемых объектов») с использованием А-схемы.

Построение моделирующих алгоритмов.

Семинар по теме№10 (2 часа)

Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого D- схемой.

Семинар по теме№10 (2 часа)

Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого F- схемой.

Семинар по теме№10 (2 часа)

Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого P- схемой.

Семинар по теме№11 (2 часа)

Основы логических расчетов надежности автоматизированных систем безопасности. Структурная схема объекта (системы). Принципы составления логической функции работоспособности объекта (системы).

Семинар по теме№11 (2 часа)

Приведение логической функции работоспособности системы безопасности к элементарному виду.

Семинар по теме№12 (2 часа)

Алгоритм расчета вероятности взлома системы безопасности, основанный на логической функции работоспособности системы.

Семинар по теме№13(2 часа)

Методы приведения логической функции системы безопасности к элементарному виду для задачи несанкционированного доступа в систему безопасности.

Семинар по теме№15 (2 часа)

Основные каналы силового деструктивного воздействия; технические средства, реализующие и защищающие от электромагнитного терроризма.

СИСТЕМА КОНТРОЛЯ ЗАНЯТИЙ

## Контрольные вопросы для проверки качества знаний

1.Понятие системы. Определение системы информационной системы управления, возможности этой системы.

2.Информационная технология, классификация информационных технологий.

3.Процесс управления системами, основные понятия.

4.Информационные системы в корпоративных системах.

5.Понятие информационного обеспечения, его структура.

6.Модель «клиент-сервер». Трехуровневая модель «клиент-сервер».

7.Новейшие информационные технологии в управленческой деятельности.

8.Безопасность информационной системы, угроза безопасности информации, определения.

9.Классификация умышленных угроз безопасности информации.

10.Понятие оценки безопасности информационной системы.

11.Структура систем информационной безопасности.

12.Понятие об этапах разработки систем защиты.

13.Электромагнитные каналы утечки информации, их особенности, причины возникновения.

14. Электромагнитные каналы утечки информации, и их причины возникновения.

15.Параметрические каналы, утечки информации.

16.Акустические каналы утечки.

17.Классификация угроз компьютерной безопасности.

18.Классификация технических средств обнаружения угроз безопасности.

19.Современние сканеры как техническое средство защиты системы от взлома Их основные технические характеристики.

20.Зщита от взлома системы с помощью нелинейных локаторов, их основные характеристики. Основные области применения.

21.Примеры детекторов паразитных излучений, незаконной аудио и видео аппаратуры.

22.Металлоискатели, их функции и возможности.

23.Определение надежности системы.

24.Логический метод расчета вероятности несанкционированного доступа в систему; основные компоненты системы.

25.Метод расчета надежности системы безопасности не основе логической функции работоспособности.

26.Понятие о современных методах и средствах обеспечения безопасности в каналах информационно-вычислительных систем, телекоммуникаций.

27.Типовые меры обеспечения безопасности ПЭВМ.

28.Технические средства обеспечения безопасности ПЭВМ.

29.Современный подход к обеспечению защиты информации в сетях ЭВМ, основные понятия.

30.Понятие о криптографических методах защиты информации.

31.Понятие о методологических основах создании современных систем информационной безопасности.

32.Основные принципы концепции интегральной защиты информации, её преимущества.

33.Понятие о современных методах компьютерной стеганографии как о средстве защиты информации.

34.Сравнительный анализ, сравнительные характеристики современных методов защиты информации, основанных на компьютерной стеганографии. Перспективы компьютерной стеганографии.

35.Технические средства защиты информационных систем от электромагнитного терроризма.

36.Основные каналы силового деструктивного воздействия электромагнитных полей на интегрированную систему безопасности.

37.Оптические технологии защиты документов(голограммы, основные типы и особенности современных голограмм.).

38.Понятие о технологиях защиты информации с помощью электронных ключей. Основной компонент системы защиты HARDLOCK.

# ОБЩИЕ ПРАВИЛА ВЫПОЛНЕНИЯ КОНТРОЛЬНЫХ РАБОТ

Предлагаемые ниже контрольные работы, равно как и контрольные вопросы для проверки качества знаний, относятся к системе контроля знаний, получаемых слушателями данного курса.

Предлагаемые контрольные вопросы, в количестве 38 вопросов, бесспорно, требуют времени на подготовку и письменной формы ответа в подавляющем числе (за исключением, может быть вопросов: №1, №2, №9, №10, №22, №30, №33, №38)

В силу этого, полный перечень вопросов, может быть использован самим студентом для проверки его уровня знаний в любое время. Но с другой стороны, преподаватель может прибегать к этому списку вопросов, как во время экзамена (или зачета), давая небольшое время на подготовку ответа письменно, так и в течении семестра, в любое время, устраивая блиц-опрос в устной форме, при, этом, естественно, от студента требуется лишь корректный ответ по сути задаваемого вопроса.

Что касается контрольных работ 1-3, то они оцениваются 100-бальной системой, принятой в РУДН.

Все контрольные работы, примерно на 70% состоят из материала (в виде вопросов или расчетных задач), трудности гораздо выше средней (в особенности это замечание касается вопросов с номерами 5,6 в работе 1, №№1,3,5 для работы 2, №№2,4,5,6, в работе 3).

Ответы на эти вопросы требуют глубокого знания курса и выполнения письменных (трудоемких) математических расчетов (не стандартных).

Поэтому, как вариант может рассматриваться возможность выполнения контрольных работ №2 и №3 дома, вне аудиторной обстановки. При этом срок сдачи этих работ должен быть не больше 2-х

или 3-х дней после вручения и фиксации срока выдачи этих работ, на усмотрение преподавателя.

Необходимо отметить, что трудоемкость работ возрастает с их нумерацией, и поэтому результаты итоговой аттестации могут, (на усмотрение преподавателя) выставляться по результатам работ №2 и №3.

## ПРИМЕРНАЯ ШКАЛА ОЦЕНИВАНИЯ

Если итоговая оценка курса производиться на основании результатов экзамена, то выставления оценок стандартна, производится по 100-бальной системе, и результирующая экзаменационная оценка определяется целиком преподавателем курса. Однако в том случае, если итоговая аттестация проводится в форме зачета, то «зачет» может быть поставлен на основании результатов выполнения всех трех контрольных работ, с привлеченным, если это необходимо, перечня контрольных вопросов(1-38)

А)-«отлично» (96-100)-ставиться за 100%-ое, качественное выполнение всех работ полностью.

«отлично» (91-95)-ставиться если в выполнении задач №1, №2, №5; в работе №2 правильно выполнены задачи №1, №5; в работе №3 правильно выполнены задачи №2, №4, №5, №6;

Б)-«хорошо» (76-90)-если в каждой работе правильно выполнены хотя бы одна из задач повышенной трудности (см. выше пункт А) и полностью получены правильные ответы на все остальные вопросы.

В)-«удовлетворительно» (35-75) и неудовлетворительно (меньше 35) должны быть полностью отнесены компетенции и принципиальности преподавателя , принимающего экзамен (зачет).

В случае, если общая сумма по трем контрольным не превосходит 115 баллов (т. е. меньше 115-ти), студент должен ответить на какие-либо вопросы (см. выше, №№1-38).

Если ответы студента удовлетворят преподавателя, студент аттестуется положительно, в противном случае, он не аттестуется преподавателем, и назначается повторная переэкзаменовка.

## СОДЕРЖАНИЕ КОНТРОЛЬНЫХ РАБОТ

Контрольная работа №1 (8 часов)

1. Изобразить графически с помощью блок-схем, процесс синтеза моделей системы информационной безопасности на основе классического и системного подходов.

Произвести подробную интерпретацию двух моделей, охарактеризовав смысловую нагрузку каждой из компонент двух моделей.

Дать определения понятий подсистемы и системы.

2. Дать определение информационной системы управления и системы информационной безопасности. Привести конкретные примеры систем.

Дать определение организационной и функциональной структур системы. Нарисовать блок-схемы организационной и функциональной структур конкретной системы (организация или система управления безопасностью объекта и т.д.)

3. Дать определение информационной технологии, изобразить в виде блок-схемы классификацию информационных технологий и информационных технологий в области средств защиты информации.

4. Привести классификацию умышленных угроз на примере конкретного объекта. Выбор объекта произволен.

5. Дать определение системы криптографической защиты информации, подчеркнуть отличие криптографических методов от других методов защиты информации.

Криптографический алгоритм, шифрующий ключ.

Характеристики классических алгоритмов с закрытыми ключами и алгоритмов с открытыми ключами.

Понятие об алгоритме шифрования на основе российского стандарта ГОСТ 28147-89, его области применимости.

6. Провести примерную оценку информационной безопасности предприятия, организации, фирмы, на которой Вы работаете.

Контрольная работа №2 (8 часов)

1. Изобразить с помощью графа Q-схему, соответствующую одноканальной системе массового обслуживания, имеющей 5 мест массового обслуживания в “очереди”. Перечислить все возможные состояния такой системы.

Произвести интерпретацию данной Q-схемы как модели информационной безопасности системы (объекта), имеющей 6 состояний.

Произвести интерпретацию каждого из шести состояний посредством терминологии задач “несанкционированного доступа”, например:

“0” – состояние: отсутствует проникновение в систему, система функционирует нормально.

“1” – состояние: произошел несанкционированный доступ в систему по электромагнитному каналу утечки.

“2” – состояние: функционируют какие-либо два канала утечки, например электромагнитный и оптико-электронный и т.д., на усмотрение квалификации учащегося.

2. Основные понятия “воздушного” технического канала утечки информации. Привести пример конкретного объекта, для которого “воздушный” канал утечки является актуальным, приоритетным.

3. Понятие интегральной безопасности. Перечислить основные технические средства обеспечения интегральной безопасности по таким видам её обеспечения, как безопасность информации, безопасность объектов и безопасность личности.

4. Современные аппаратные и программно-аппаратные средства контроля уровня безопасности компьютерных сетей.

5. Рассчитать надежность системы безопасности информации конкретного объекта на основании заданной структурной схемы объекта путем составления логической функции и приведения её к элементарному и бесповторному виду.

6. Сканеры, их устройство, принцип действия, область применимости, частотный диапазон, чувствительность.

Радиомониторинг с помощью сканеров как эффективное техническое средство защиты информации от незаконного проникновения с помощью “жучков” – радио, видео и телефонных закладок.

Контрольная работа №3 (8 часов)

1. Криптографические системы с открытым ключом. Блок-схема, преимущества, принцип работы. Требования, предъявляемые к этим системам, предназначенность этих систем. Алгоритм RSA.

2. Изобразить с помощью блок-схемы алгоритм, моделирующий функционирование системы информационной безопасности, моделируемую при помощи Q-схемы с одним каналом обслуживания и тремя местами в очереди. Интерпретировать каждое из 4-х состояний

системы в терминологии задач “несанкционированного доступа”, например:

“0” – состояние: отсутствует проникновение в систему, система функционирует нормально.

“1” – состояние: произошел доступ в систему по одному из каналов утечки, например, параметрическому.

“2” – состояние: ликвидирован параметрический канал утечки, но возник электрический канал утечки и т.д., на усмотрение квалификации учащегося.

3. Определение надежности системы. Основные количественные показатели – вероятность безотказной работы системы вероятность отказа системы. Дать интерпретацию этих показателей в рамках теории информационной безопасности, когда рассматриваются системы безопасности информации.

4. Понятия Q-схемы и D-схемы как типовых математических моделей в рамках теории защиты информации, принципиальное различие между этими схемами. Привести примеры систем информационной безопасности, адекватно описываемых этими схемами.

5. Произвести расчет надежности информационной системы безопасности, заданной своей структурной схемой.

6. Рассчитать вероятность “взлома” системы информационной безопасности, заданной своей структурной схемой, методом построения с логической функции для этой структурной схемы. Считать заданными вероятности отказа (взлома) каждого из блоков структурной схемы.

## АННОТИРОВАНИЕ СОДЕРЖАНИЕ КУРСА

Краткое содержание лекционного курса.

Лекция №1 (2 часа)

Система, определение, интерпретация применительно к целям и задачам курса. Информационные системы управления, определения, возможность. Классификация по уровню управления; классификация по области функционирования; по степени автоматизации. Понятие информационной технологии, классификация информационных технологий по ряду признаков.

Лекция №2 (2 часа)

Системы обеспечения информационной безопасности как синтез технических и аппаратно-программных средств обеспечения информационной безопасности. Понятие безопасности информационной системы, понятие угрозы безопасности информации. Описание наиболее важных областей применимости систем защиты информации. Организационная и функциональная структуры автоматизированной системы защиты информации Вашего предприятия (фирма, банк, производственное объединение и т.д.).

Лекция №3 (2 часа)

Подробно рассматриваются угрозы безопасности информации, такие, как, например, пассивные и активные угрозы, внутренние и внешние. Промышленный шпионаж, утечка конфиденциальной информации, многочисленные пути несанкционированного доступа, требующие высокого уровня технической оснащенности, примитивные

пути несанкционированного доступа, перечень основных видов компьютерных вирусов (вредоносных программ) и другие способы взлома.

Лекция №4 (2 часа)

Безопасность системы как степень её защищенности от внутренних и внешних угроз. Различные подходы к оценке безопасности. Оценка уровней безопасности в США и России, сходства системы защиты, принцип непрерывного развития системы, разделение и минимизация полномочий по доступу к информации организации, контроль и регистрация попыток взлома, строгий контроль за обеспечением надежности системы защиты информации.

Лекция №5 (2 часа)

Основные технические признаки системы информационной безопасности высокого уровня. Подход к структуре системы информационной безопасности, основанный на структурировании специальных подсистем. Блок-схема современного метода обеспечения безопасности информации. Подробное описание современных технических и программных средств защиты информации.

Лекция №6 (2 часа)

Сущность, назначение, специфика криптографических методов защиты информации. Понятие об основных методах преобразования. Шифрующие ключи. Характеристики симметричных и асимметричных криптографических систем. Подстановки. Подстановка Цезаря.

Лекция №7 (2 часа)

Анализ каналов утечки информации на основе системного подхода, разнообразие их видов из-за разнообразия основных технических средств и

вспомогательных технических, перечень этих средств. Электромагнитные, электрические и параметрические технические каналы утечки, их характерные особенности, причины возникновения, физическая природа.

Лекция №8 (2 часа)

Аппаратная реализация современных методов несанкционированного доступа к информации. Краткая характеристика разновидностей радиомикрофонов (“закладки”), электронных “ушей”, средств перехвата телефонный связи, средств скрытых наблюдений, средств контроля компьютеров и сетей средств приема, записи, управления (приемники для радиопрокладок, устройства накопления и записи, радиотрансляторы и другие многочисленные радиоэлектронные средства).

Лекция №9 (2 часа)

Классификация технических средств обнаружения угроз безопасности на основе интегральной концепции безопасности. Компьютерные полиграфы.

Лекция №10 (2 часа)

Основная концепция информационной безопасности, основные положения концепции. Основные методы и средства обеспечения безопасности в каналах информационно-вычислительных систем, телекоммуникаций ЭВМ. Характеристики, основное содержание следующих методов: маркировка; препятствие; управление доступом; регламентация; побуждение; принуждение. Средства механизмов защиты: аппаратные, физические, программные, организационные, морально-этические, законодательные.

Лекция №11 (2 часа)

Компьютерные преступления и человеческий фактор. Слабая защищенность от несанкционированного доступа локальных сетей связи, причины уязвимости локальных сетей. Технические средства защиты. Функция системы защиты NBS, её устройство, достоинства. Системы передачи данных на базе инфракрасного излучения. Программы управления защитой данных. Современный подход к обеспечению сетевой защиты информации. Основные факторы оказывающие существенное влияние на безопасность распределенных систем. Средства создания индивидуальной защиты каждого узла сети ПЭВМ.

Лекция №12 (2 часа)

Системный подход к моделированию систем. Классификация видов моделирования систем. Математические схемы моделирования систем: непрерывно-детерминированные модели (D-схемы); дискретно-детерминированные модели (F-схемы); дискретно-стохастические модели (P-схемы); непрерывно-стохастические модели (Q-схемы); обобщенные модели (A-схемы). Использование этих математических схем для моделирования информационно-вычислительных систем, систем управления информационной безопасностью.

Лекция №13 (2 часа)

Основные количественные показатели теории надежности. Интенсивность отказов, средняя наработка на отказ. Понятие структурной схемы системы (объекта). Логическая функция работоспособности исследуемой системы. Приведение логической функции к элементарному бесповторному виду с помощью основных логических функций. Расчет вероятности безотказной работы исследуемой системы.

Лекция №14 (2 часа)

Расчет надежности типовых структурных схем: параллельное соединение нескольких элементов; последовательное соединение; логический мост; треугольник. Составление структурных схем для систем управления безопасностью объекта.

Лекция №15 (2 часа)

Расчет вероятности незаконного проникновения в систему (”взлом” системы) на основании оценок вероятностей проникновения в систему по соответствующим, характерным для данной системы каналом утечки. Составление логической функции работоспособности для систем информационной безопасности, заданных своими структурными схемами. Расчет вероятности проникновения в систему с помощью составленной логической функции.

Лекция №16 (2 часа)

Основные понятия, концепции интегральной защиты информации, разработка системы управления информационной безопасностью объекта на основании анализа каналов утечки информации, характерных для конкретной системы защиты информации с использованием концепций интегральной защиты.

Лекция №17 (2 часа)

Основные понятия компьютерной стеганографии, основные принципы компьютерной стеганографии, её области применения. Современные технические аппаратно-программные методы, применяемые в компьютерной стеганографии. Сравнительные технико-программные характеристики современных стеганографических методов. Оценка уровня

скрытности мультимедийных стенографических каналов хранения и передачи информации.

Лекция №18 (2 часа)

Электромагнитные каналы утечки информации. Характерные побочные излучения, возможные причины их возникновения. Основные каналы взлома системы безопасности – сеть питания, проводные линии, через эфир, - путём применения мощных коротких электромагнитных импульсов. Электромагнитное ружье. Электромагнитная пушка. Классификация технических средств защиты систем безопасности для защиты от электромагнитных технических средств силового воздействия по цепям питания, проводным линиям и по эфиру.

Лекция №19 (2 часа)

Вредоносные программы, классификация вредоносных программ, причины трудностей в борьбе с вредоносными программами. Наиболее распространенные “виды вредоносных” программ: “логические бомбы”, “троянский конь”, “вирус”, “червь”, “захватчик Паролей”, “компроментация информации”. Технические средства борьбы с ними: организационные мероприятия, направленные на создание узкого замкнутого круга лиц, имеющий прямой доступ к прикладным программам; антивирусы – детекторы, фаги, вакцины, прививки, ревизоры, мониторы.

Лекция №20 (2 часа)

Метод временных диаграмм. Его применение в одноканальных и многоканальных системах массового обслуживания, как универсального метода моделирования процесса функционирования системы массового обслуживания. Математическая природа его универсальности. Применение метода временных диаграмм в задачах расчета вероятности

взлома системы безопасности объекта, его интерпретация в задачах несанкционированного доступа.

Общая трудоемкость лекционного курса в часах составляет 40 часов.

**Краткое содержание семинарских занятий.**

Семинар №1 (2 часа)

Перечень основных источников электромагнитного излучения при работе с компьютером, формирующими физические сигналы, создающие каналы утечки информации: материнские платы компьютеров, блоки питания, принтеры, накопители, плоттеры, аппаратура связи; дисплей – как источник электромагнитного излучения высокой частоты.

Семинар №2 (2 часа)

Номенклатура современных технических средств несанкционированного добывания информации: радиомикрофоны (закладки), электронные “уши”, средства перехвата телефонной связи, средства скрытого наблюдения и поиска, средства контроля компьютеров и сетей, приемники для радиопрокладок, радиотрансляторы, устройства дистанционного управления.

Семинар №3 (2 часа)

Основные компоненты общей модели системы обеспечения безопасности автоматизированных систем обработки информации. Поиск уязвимых компонент. Перечень уязвимых компонент аппаратные средства вычислительной техники, программные средства (операционные системы, драйверы, интерфейсное и сетевое программное обеспечение),

информационное обеспечение (базы данных, файлы), системы связи (локальные вычислительные сети, кабельные сети).

Семинар №4 (2 часа)

Отечественный стандарт криптографической защиты (ГОСТ 28147-89). Электронная подпись.

Семинар №5 (2 часа)

Места установок пассивных и активных средств незаконного получения информации, дальность действия средств, стоимость, вероятность применения, качества перехвата и обнаружения. Методы защиты от пассивных и активных средств взлома системы: шифрование (кодирование), фильтрация, экранировка помещений.

Семинар №6 (2 часа)

Классификация угроз безопасности в информационно-вычислительных и телекоммуникационных сетях: по способам воздействия на сеть, по целям угрозы, по видам ошибок, допущенных при создании сетей по способам атаки по используемым средствам, по-принципу и характеру воздействия.

Семинар №7 (2 часа)

Анализ факторов угроз на конкретном объекте (по выбору) и синтез концепции интегральной безопасности данного объекта. Физическая защита (технические средства, линии связи, персонал) и логическая защита (операционные системы, прикладные программы, массив данных) – основные направления противодействия утечке в рамках концепции информационной безопасности.

Семинар №8 (2 часа)

Сканеры, нелинейные радиолокаторы. Устройство принцип действия, области применимости преимущества и недостатки. Краткая характеристика комплекса OSCOR-5000.

Семинар №9 (2 часа)

Технология клиент-сервер, область применения, преимущества. Основные факторы, затрудняющие применение этой технологии в распределенных системах.

Семинар №10 (2 часа)

Система информационной безопасности как многоканальная, многофазная Q-схема. Модель системы информационной безопасности реализуется в виде моделирующего алгоритма, предоставляемого блок-схемой, часть блоков которой имитирует “поток заявок” – случайное число взломов системы, другая часть блоков имитирует многофазность системы, т.е. выбор различных способов защиты от угроз, оставшаяся часть блоков соответствует возможным процессам взаимодействия внутри системы между её каналам и обмену информации между каналами.

Семинар №11 (2 часа)

Алгоритм, моделирующий функционирование системы информационной безопасности, которая может быть предоставлена в виде структурной трехблочной схемы, блоки которой предоставляют определённые части этой системы с определенными функциями.

Семинар №12 (2 часа)

А-схема как агрегатный подход общего характера к моделированию процесса функционирования системы информационной безопасности.

Преимущества агрегативного подхода при моделировании систем безопасности. Система безопасности объекта как сложная система состоящая из конечного числа взаимодействующих подсистем.

Семинар №13 (2 часа)

Непрерывно-детерминированный подход к процессу функционирования системы безопасности объекта, сущность непрерывно-детерминированного подхода (на основе D-схем). Описание объекта (системы информационной безопасности) обыкновенным дифференциальным уравнением, или системой дифференциальных уравнений. Начальное условие соответствует начальному состоянию системы безопасности объекта.

Семинар №14 (2 часа)

Математическая модель системы в виде F-схемы, отличительные черты F-схем. Избирательность систем безопасности, которые в состоянии быть представленными адекватными им в определенных смыслах F-схемами. Блок-схема моделирующего алгоритма.

Семинар №15 (2 часа)

Разновидности систем, которые моделируются P-схемами. Характерные черты P-схем. Реальные ситуации, адекватные системам безопасности, моделирующихся с помощью P-схем. Блок-схема моделирующего алгоритма.

Семинар №16 (2 часа)

Логические постулаты теории надежности. Структурная схема системы, построение логической функции по элементу. Применение постулата для приведения логической функции к элементарному виду.

Семинар №17 (2 часа)

Структурная схема информационной системы безопасности. Представление её логической функции. Расчет вероятности взлома системы с помощью приведения логической функции системы к бесповоротному виду.

Семинар №18 (2 часа)

Составление блок-схемы алгоритма, моделирующего нормальный процесс функционирования системы безопасности процессом дискретных проникновений случайного характера.

Семинар №19 (2 часа)

Классификация каналов деструктивно-силового воздействия с помощью магнитных полей на систему информационной безопасности конкретной структуры. Различные виды экранирования системы информационной безопасности, противодействующие электромагнитному терроризму.

Семинар №20 (2 часа)

Графическая иллюстрация применения метода временных диаграмм для расчета параметров и эффективности работы многоканальной системы массового обслуживания. Интерпретация работы Q-схем в рамках задачи расчета вероятности взлома системы безопасности  с тем же числом каналов. Число каналов, число мест в очереди и интенсивность входного и выходного потоков заданы заранее.

Общая трудоемкость семинарских занятий составляет 40 часов.

# ТЕМЫ КУРСОВЫХ РАБОТ

1. Каналы утечки в общем случае и каналы утечки на вашем предприятии. Перечень, анализ преимуществ и недостатков каждого из каналов, анализ средств защиты, перспективы развития существующих и образования новых видов каналов утечки.

2. Анализ видов и основных технических характеристик электромагнитных методов взлома систем информационной безопасности, методы защиты от этих методов, прогресс и перспективы развития среди методов нападения и методов защиты.

3. Классификация умышленных угроз безопасности для функционирующей информационной системы. Анализ технических характеристик и технических возможностей каждого из методов, их перспективность применения.

4. Классификация угроз несанкционированного проникновения в телекоммуникационные каналы связи. Приоритетные способы взлома, использующие уязвимые места системы каналов связи.

5. Сканеры, нелинейные радиолокаторы и некоторые другие средства обнаружения радиопередатчиков (“электронных ушей”) в ближней зоне этих подслушивающих устройств. Новые технические идеи в методах “взлома” и методов “защиты”.

6. Анализ, классификация факторов, как отрицательно влияющих на безопасность распределенных систем, так и повышающих эту безопасность. Проанализировать верхний предел прочности некоторой конкретной системы безопасности, например, на Вашем предприятии.

7. Системы массового обслуживания. Q-схемы - основные понятия, классификация. Применение Q-схем в качестве математических моделей в схемах систем информационной безопасности. Интерпретация стандартных понятий Q-схем (“канал обслуживания”, “очередь”,

“приоритетность”, “среднее время обслуживания”, “отказы” и др.) в качестве основных понятий моделей системы безопасности.

8. Составить блок-схему (структурную схему) системы информационной безопасности Вашего предприятия. Классифицировать по степени опасности каналы взлома системы. Предложить технические средства борьбы с ними.

9. Специфика применения криптографических методов. Симметричные и ассиметричные криптографические системы. Понятие о математических методах шифрования. Зашифровать методом …. простейшее сообщение (из нескольких слов).

10. Анализ, классификация основных современных методов дешифрования. Пример использования любого из методов дешифровки.

11. Анализ, специфика, технические характеристики параметрических каналов утечки на Вашем предприятии.

12. Компьютерная стенография. История возникновения, анализ основных аппаратно-программных методов.

13. Непрерывно-детерминированный подход к моделированию систем управления (D-схемы). Сконструировать систему управления охраны информационной безопасности Вашего предприятия, составить структурную схему и соответствущую логическую функцию. Рассчитать вероятность “взлома” (отказа) сконструированной системы.

14. Агрегативный подход к моделированию систем управления (А – схемы моделирования). Преимущества агрегативного подхода. Блок-схема системы управления безопасностью (на основе А-схемы) на вашем предприятии. Расчет вероятности взлома этой системы.

15. Подход к моделированию системы управления безопасностью на основе F-схемы. Особенности применения F-схемы для моделирования систем управления, отличительные черты F-схемы как математической схемы моделирования конечного автомата. Разработка блок-схемы

алгоритма моделирования системы управления безопасностью Вашего предприятия.

16. Подход к моделированию системы управления на основе Р-схемы, избирательность данного подхода по отношению к объектам моделирования. Разработка алгоритма, моделирующего систему управлению безопасностью на Вашем предприятии с применением Р-схемы.

17. В рамках моделирования системы управления на основе Р-схемы разработать структурную схему системы управления безопасностью на примере Вашего предприятия. Получить логическую функцию работоспособности, на основании полученной функции рассчитать вероятность взлома системы управления хотя бы по одному из каналов несанкционированного доступа. Расчет производить в рамках системы управления на Вашем предприятии.

18. Графическое представление процесса функционирования с помощью метода временных диаграмм многоканальной системы массового обслуживания (число каналов задаётся в работе) с заданным числом мест в очереди (задаётся в работе). Интенсивности входного и выходного потока так же задаются заранее. Времена обслуживания “заявок” в каждом канале являются случайными величинами, распределенные по равномерному закону.

19. Рассчитать надежность системы безопасности информации объекта, заданного его структурной схемой в условиях случайности моментов времени взлома и случайности выбора одного из трех каналов утечки: электромагнитного, электрического и параметрического.

20. Взлом системы информационной безопасности при помощи вредоносных программ. Классификация вредоносных программ, наиболее типичные виды “вредоносных программ”: “троянский конь”, “логические бомбы”, “вирус”, “червь”, “захватчик паролей”, “компроментация

информации”. Описание способов борьбы с этими программами, технических, аппаратно-программных и организационных. Анализ антивирусных программ: фаги, детекторы, вакцины, прививки, ревизоры, мониторы. Сравнительные характеристики антивирусных методов, перспективы их развития.

## ТЕМЫ РЕФЕРАТОВ

1. Понятие информационного ресурса, информации и информатизации. Информационные ресурсы, необходимые для управления системой управления безопасностью (в широком смысле) организации, их источники.

2. Автоматизированные информационные системы. Информационно-вычислительные системы, информационно-справочные и другие виды систем как подсистемы автоматизированных информационных систем. Описать их задачи (на примере Вашего предприятия).

3. Представление сложной системы в виде организационной и функциональной структур как кибернетический, системный подход к анализу системы, её подсистем и решаемых внутри системы подсистем задач вследствие основной и побочных целей системы и её многочисленных связей с внешней, окружающей систему средой.

4. Электронный документооборот. Его функции в государственных организациях. Системы записи электронного документооборота в рамках самой системы электронного документооборота. Примеры потоков документооборота. Примеры потоков документооборота, траектории их движения на Вашем предприятии.

5. Пакетные и диалоговые режимы процессов обработки данных на Вашем предприятии, их основные цели, преимущества и недостатки.

6. Интернет-технологии в работе системы управления. Концепция “электронного правительства”. Классификация Web-служб. Информационные порталы, мультипорталы, интегрированные порталы, порталы знаний. Их цели, задачи.

7. Сервисно-ориентированные технологии. Их применение на вашем Предприятии в рамках SOA-концепции.

8. Объектно-ориентированные технологии, объектно-ориентированные базы данных, объектно-ориентированные системы управления базами данных. Причины возникновения , цели, преимущества. Языки запросов.

9. Системы искусственного интеллекта и интеллектуальные информационные технологии (нейросети, генетические алгоритмы, нечеткая логика). Основные понятия. Цели создания систем искусственного интеллекта.

10. Применение интеллектуальных информационных технологии в задачах безопасности на предприятии.

11. Нейросети, обучение нейросетей. Перспективы применения нейросетей в задачах охраны безопасности (как внешней, так и внутренней) на Вашем предприятии ( в частности)

12. Создание экспертной системы на основе интеллектуальной системы охраны безопасности предприятия, ей основные подсистемы.

13. Компьютерная стенография – как современная информационная технология защиты информации. История развития от “вчера” до “сегодня”.

14. Обзор технических средств обеспечения личной безопасности (последние несколько лет).

15. Электромагнитные каналы утечки, их побочные излучения. Природа электромагнитных каналов утечки. Увеличение их числа и разновидностей одновременно с ростом объема и увеличением степени автоматизации системы защиты информации.

16. Физическая природа электрических каналов утечки в системе. Защита системы от “взломов”. Природа их тесной связи с многочисленными линиями и сетями связи.

17. Воздействие электромагнитных полей на человека (обслуживающий персонал). Возрастание в связи с этим отрицательной роли человеческого фактора в проблеме “охраны” объекта от несанкционированных проникновений. Необходимые оргмероприятия, уменьшающие эту отрицательную роль.

18. Принципы работы многоканальной системы массового обслуживания; метод временных диаграмм. Исследование принципиальной возможности использования методов теории массового обслуживания в ситуациях с непрерывно развивающимся во времени случайным потоком дискретных моментов “взлома” в схемах интегральной безопасности сложной распределённой системы.

19. Система тревожной сигнализации “ОСПАС-2”: нижний и верхний уровень обеспечения безопасности; задачи комплекса программно-аппаратных средств, состав технических средств комплекса “ОСПАС-2” (приёмные радиомодули, типы антенн, антенных фильтров и т.д.)

20. Проксимити-технология в системах безопасности; Устройства идентификации, сравнительные характеристики считывателей; интеграция – тенденция дальнейшего развития проксимити-технологии.

## ТЕМЫ ЭССЕ

1. Информация в современном обществе; информационный бум: это, в итоге “зло или добро” для отдельного индивидуума? В асимптотике развития социума какая из пословиц окажется правильнее: “век живи, век учись” или “много будешь знать, быстро состаришься”.

# КАЛЕНДАРНО-ТЕМАТИЧЕСКИЙ ПЛАН ДИСЦИПЛИНЫ

| № темы | Название темы по программе курса | Лекции часы кредит | Семи-нары часы кредит | Само-стоятельная работа часы кредит |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 1 | Основные понятия теории защиты информации в измерительных системах и информационных технологиях управления объектом. | 4 | | |
| 2 | Виды умышленных угроз безопасности информации. | 2 | 4 | |
| 3 | Методы и технические средства построения технических систем информационной безопасности, их структура. | 4 | 2 | |
| 4 | Криптографические методы защиты информации. | 2 | 2 | |
| 5 | Анализ и особенности каналов утечки и несанкционированного доступа к информации в технических информационных системах. | 2 | 2 | |
| 6 | Аппаратная реализация современных технических методов несанкциони-рованного доступа к информации. | 2 | 2 | |
| 7 | Современные технические средства обнаружения угроз. | 2 | 2 | |
| 8 | Современные технические средства обеспечения безопасности к каналах информационно-вычислительных систем, телекоммуникаций и ВМ. | 2 | 2 | |
| 9 | Современные технологические сред-ства защиты информации от несанк-ционированного доступа в сетях ЭВМ. | 2 | 2 | |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| | Контрольная работа №1 | | | 8 |
| 10 | Основные понятия моделирования больших систем, математическое моделирование больших систем на основе математических систем: A-схем, D-схем, F-схем, P-схем, Q-схем. | 2 | 12 | |
| 11 | Основные понятия теории надежности систем. Метод расчета надежности систем на базе построения логической функции системы. | 4 | 4 | |
| 12 | Метод расчета вероятности взлома системы на основе логической функции системы. | 2 | 2 | |
| | Контрольная работа №2 | | | 8 |
| 13 | Концепция интегральной защиты информации. | 2 | | |
| 14 | Компьютерная стенография как перспективное, современное, техническое и программное средство защиты информации, от несанкционированного доступа. | 2 | | |
| 15 | Технические средства и технологии, информационных систем безопасности от электромагнитного терроризма. | 2 | 2 | |
| 16 | Вредоносные вирусные программы. Современные технические средства борьбы с компьютерными вирусами. | 2 | | |
| 17 | Содержание метода временных диаграмм, его графическое представление. Исследование причин универсальности этого метода в задачах моделирования работы сложенных многоканальных систем управления безопасностью объектов. | 2 | 2 | |
| | Контрольная работа №3 | | | 8 |

# СПИСОК ЛИТЕРАТУРЫ

**Обязательная**

1. Барсуков. В.С. безопасность: технологии, средства, услуги. М., “КУДИЩ-ОБРАЗ”, 2001. Стр.(7-14) – тема 5, стр.(14-18) – тема 6, стр.(22-27) – тема 16, стр.(28-35) – тема 8, стр.(77-87) – тема 4, стр.(67-72) – тема 9, стр.(88-93) – тема 13, стр.(263-278) – тема 15, стр.(174-180) – тема 14, стр.(246-260) – тема 6, тема 7. Советов Б.Я. Яковлев С.А. Моделирование систем. Учебник для вузов. М. Высшая школа, 1989 стр.(105-151) – тема 10, стр.(160-183) – тема 17.

2. Титаренко Г.А., Брага В.В., Вдовенко Л.А. и др.(под ред. Титаренко Г.А.) Информационные технологии управления. Учебник для вузов. М.,“ЮНИТИ” 2005 стр.(8-16) – тема 1, стр.(84-88) – тема 1, стр.(192-221) тема 2, тема 3, тема 16, тема 6, тема 8.

3. Гринберг А.С., Горбачев Н.Н, Теплякова А.А Защита информационных ресурсов государственного управления. Учебник для вузов. М.”ЮНИТИ”, 2003. Стр.(5-20) – тема 1, Стр.(35-45) – тема 3, Стр.(50-53) – тема 16.

4. Гринберг А.С., Горбачев Н.Н, Бондаренко А.С. Информационные технологии управления. Учебник для вузов. М.”ЮНИТИ”, 2004. Стр.(3-17) – тема 1, Стр.(43-51) – тема 5, Стр.(7-21) – тема 13.

5.Уханов Л.Т. Управление безопасностью информации в автоматизированных системах М. “МИФИ”, 1996. Стр.(5-80) – тема 2, тема 3, тема 8, тема 11.

**Дополнительная**

1. Теория и практика обеспечения информационной безопасности (Под ред. П.Д. Зегжды.-М: Изд-во Агенства “Яхтсмен”, 1998.

2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов от информации – СПБ, “Лань”, 1996

3. Руководящий документ. Защита от НСД к информации. Термины и определения. – М., Госкомиссия России, 1992.

4. Руководящий документ. Защита от НСД к информации. – М., Госкомиссия России, 1992.

5. Мартик С. Механизмы защиты в сетях ЭВМ. –М., “Мир”, 1993.