ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

ФТД.В.01 Системы предотвращения утечек

Направление подготовки (специальность) 10.05.03 Информационная безопасность автоматизированных систем

Профиль образовательной программы Информационная безопасность автоматизированных систем критически важных объектов

Форма обучения очная

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1 (2 часа).

Тема: «Введение»

1.1.1 Вопросы лекции:

1. Цели и задачи курса «Системы предотвращения утечек».
2. Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации.
3. Основные понятия.

1.1.2 Краткое содержание вопросов:

1. Цели и задачи курса «Системы предотвращения утечек»

Цель освоения дисциплины:

Целями освоения дисциплины «Системы предотвращения утечек» являются изучение основных принципов, методов и средств защиты информации в процессе ее обработке, хранении и передачи с использованием компьютерных средств в информационных системах; теоретическое и практическое обучение студентов методам и средствам выявления и блокирования каналов утечки информации.

Задачи:

- изучение организационно-правовых вопросов создания (усовершенствования) и функционирования эффективной службы защиты информации на предприятиях различных форм собственности и видов деятельности,
- рассмотрение основных концепции создания информационной безопасности предприятия.
- рассмотрение каналов утечки информации, их классификации и механизмов возникновения,
- изучение систем предотвращения утечек.
- изучение методов и средств выявления и блокирования каналов утечки информации, новейших технологий и средств защиты информации
- освоение принципов организации контроля за эффективностью принятых мер защиты.

2. Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации.

Обучающийся в конце курса должен владеть:

-способностью проводить анализ защищенности автоматизированных систем

-способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

-способностью проводить анализ рисков информационной безопасности автоматизированной системы

- способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах

- способностью использовать нормативные правовые документы в своей профессиональной деятельности

- способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации

- способностью применять программные средства системного, прикладного и специального назначения

- способностью использовать инструментальные средства и системы программирования для решения профессиональных задач

- способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности

- способностью применять методы анализа изучаемых явлений, процессов и проектных решений

- способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов

- способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов

- способностью принимать участие в проведении экспериментально- исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности

- способностью осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

- способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

- способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю

В результате освоения дисциплины обучающийся должен:

знать:

- правовые основы обеспечения технической защиты информации;

- структуру государственной системы защиты информации от утечки по техническим каналам;

- каналы утечки информации и методы их оценки;

- принципы организации и обеспечение работ по защите информации;

-принципы работы с системами предотвращения утечек;

уметь:

- изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации;

- определять рациональные меры для выбора необходимых средств защиты информации и уметь их оценивать;

владеть навыками:

- расчета контролируемой зоны, в пределах которой могут происходить утечки информации.

3. Основные понятия.

Предотвращение утечек (англ. *Data Leak Prevention, DLP*) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Используются также следующие термины, обозначающие приблизительно то же самое:

- Data Loss Prevention (DLP);
- Data Leak Prevention (DLP);
- Data Leakage Protection (DLP);
- Information Protection and Control (IPC);
- Information Leak Prevention (ILP);
- Information Leak Protection (ILP);
- Information Leak Detection & Prevention (ILDP);
- Content Monitoring and Filtering (CMF);
- Extrusion Prevention System (EPS).

Из этой группы пока не выделился один термин, который можно было бы назвать основным или самым распространённым.

Задачи

Основной задачей DLP-систем, что очевидно, является предотвращение передачи конфиденциальной информации за пределы информационной системы. Такая передача (утечка) может быть намеренной или ненамеренной. Практика показывает, что большая часть ставших известными утечек (порядка 3/4) происходит не по злому умыслу, а из-за ошибок, невнимательности, безалаберности, небрежности работников [1]. Выявлять подобные утечки проще. Остальная часть связана со злым умыслом операторов и пользователей информационных систем. Понятно, что инсайдеры, как правило, стараются преодолеть средства DLP-систем. Исход этой борьбы зависит от многих факторов. Гарантировать успех здесь невозможно.

Кроме основной перед DLP-системой могут стоять и вторичные (побочные) задачи. Они таковы:

- архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;
- предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, эротики, излишних объёмов данных и т.п.);
- предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;
- предотвращение использования работниками казённых информационных ресурсов в личных целях;
- оптимизация загрузки каналов, экономия трафика;
- контроль присутствия работников на рабочем месте;
- отслеживание благонадёжности сотрудников, их политических взглядов, убеждений, сбор компромата.

1. 2 Лекция № 2 (2 часа).

Тема: «Правовые основы обеспечения защиты информации»

1.2.1 Вопросы лекции:

1. Государственная система защиты информации в Российской Федерации от утечки по техническим каналам.
2. Защита информации ограниченного доступа, обязанности и права субъектов.
3. Права и уровни доступа.

1.2.2 Краткое содержание вопросов:

1. Государственная система защиты информации в Российской Федерации от утечки по техническим каналам.

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Структура и основные функции государственной системы защиты информации от ее утечки по техническим каналам и организация работ по защите информации определены в "Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам", утвержденном Постановлением Правительства от 15 сентября 1993 г. № 912-51.
Этим Положением предусматривается, что мероприятия по защите информации, обрабатываемой техническими средствами, являются составной частью управленческой, научной и производственной деятельности учреждений и предприятий и осуществляются во взаимосвязи с другими мерами по обеспечению установленного федеральными законами "Об информации, информатизации и защите информации" и "О государственной тайне" комплекса мер по защите сведений, составляющих государственную и служебную тайну.
В то же время эти мероприятия являются составной частью работ по созданию и эксплуатации систем информатизации учреждений и предприятий, располагающих такой информацией, и должны осуществляться в установленном нормативными документами » порядке в виде системы защиты секретной информации.
Основные задачи государственной системы защиты информации:

- проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;
- исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных специальных программно-технических воздействий на информацию с целью ее разрушения, уничтожения, искажения или блокирования в процессе обработки, передачи и хранения;
- принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации;

- общая организация сил, создание средств защиты информации и средств контроля эффективности ее защиты;
- контроль за проведением работ по защите информации в органах государственного управления, объединениях, на предприятиях, в организациях и учреждениях (независимо от форм собственности).

В соответствии с Указом Президента Российской Федерации № 212 от 19.02.99 г., межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственную и служебную тайну, осуществляет коллегиальный орган - Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссии России).

Согласно Постановлению Правительства РФ от 12.09.93 г. №912-51 Гостехкомиссия России возглавляет Государственную систему защиты информации.

В соответствии с Законом Российской Федерации "О федеральных органах правительственной связи и информации", к основным функциям Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) в рассматриваемой области относится:

- осуществление координации деятельности по вопросам безопасности информационно-аналитических сетей, комплексов технических средств баз данных;
- осуществление координации деятельности в области разработки, производства и поставки шифровальных средств и оборудования специальной связи, по обеспечению криптографической и инженерно-технической безопасности шифрованной связи.

Федеральным законом от 03.04.95 г. N 40-ФЗ "Об органах Федеральной службы безопасности в Российской Федерации" к компетенции ФСБ в рассматриваемой области отнесены следующие вопросы:

- участие в разработке и реализации мер по защите сведений, составляющих государственную тайну;
- осуществление контроля за обеспечением сохранности сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности;
- осуществление мер, связанных с допуском граждан к сведениям, составляющим государственную тайну.

2. Защита информации ограниченного доступа, обязанности и права субъектов.

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

- конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;
- необходимый уровень безопасности информации, подлежащей защите;

- защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи информации).

Ключевым моментом политики государства в данной области является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их собственнику, владельцу, пользователю или иному лицу.

Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации включают:

- Законы Российской Федерации
- Указы Президента Российской Федерации и утверждаемые этими указами нормативные документы
- Постановления Правительства Российской Федерации и утверждаемые этими постановлениями нормативные документы (Положения, Перечни и т.п.)
- Государственные и отраслевые стандарты

- Положения, Порядки. Руководящие документы и другие нормативные и методические документы уполномоченных государственных органов (Гостехкомиссии России, ФАПСИ, ФСБ).

Федеральные законы и другие нормативные акты предусматривают:

- разделение информации на категории свободного и ограниченного доступа, причем информация ограниченного доступа подразделяется на:
- отнесенную к государственной тайне
- отнесенную к служебной тайне (информацию для служебного пользования), персональные данные (и другие виды тайн)
- и другую информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;
- *правовой режим защиты информации,* неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу, устанавливаемый:
- в отношении сведений, отнесенных к государственной тайне, -уполномоченными государственными органами на основании Закона Российской Федерации "О государственной тайне" (от 21.07.93 г. N 5485-1);
- в отношении конфиденциальной документированной информации -собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации "Об информации, информатизации и защите информации" (от 20.02.95 г. N 24-ФЗ);
- в отношении персональных данных - отдельным федеральным законом;
- *лицензирование деятельности* предприятий, учреждений и организаций в области защиты информации;
- *аттестование* автоматизированных информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);
- *сертификацию средств защиты* информации и средств контроля эффективности защиты, используемых в АС;
- возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;

- создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;
- определение прав и обязанностей субъектов в области защиты информации.

- Положение «О порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (ПКЗ-99) и другие

•«Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (Введена приказом ФАПСИ от 13 июня 2001 года N 152).

3. Права и уровни доступа.

Права доступа — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы (информации, её носителям, процессам и другим ресурсам) установленных правовыми документами или собственником, владельцем информации.

Права доступа определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения субъектам (например, пользователям системы) над объектами данных. Для этого требуется некая система для предоставления субъектам различных прав доступа к объектам. Это система разграничения доступа субъектов к объектам, которая рассматривается в качестве главного средства защиты от несанкционированного доступа к информации или порче самой системы.

Функции системы разграничения доступа

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твёрдых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Кроме того, вышеуказанный руководящий документ предусматривает наличие обеспечивающих средств для СРД, которые выполняют следующие функции:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;

- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учёт выходных печатных и графических форм и твёрдых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих её средств.

1. 3 Лекция № 3 (2 часа).

Тема: «Каналы утечки информации»

1.3.1 Вопросы лекции:

1. Особенности утечки информации.
2. Возможные каналы утечки информации.
3. Процесс внедрения DLP-систем

1.3.2 Краткое содержание вопросов:

1. Особенности утечки информации.

Особенности утечки информации

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Переносчиками информации могут быть любые ее носители.

Утечка информации по сравнению с утечкой (хищением) материальных объектов имеет ряд особенностей, которые надо учитывать при организации защиты информации:

- утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику);

- **при утечке информации происходит ее тиражирование**, которое не изменяет характеристики носителя информации (не уменьшается количество листов документа, не сокращается число пикселей изображения, не меняются размеры, цвет и другие демаркирующие признаки продукции и т. д.);

- **цена информации** при ее утечке **уменьшается** за счет тиражирования;

- факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям, когда меры по обеспечению ее безопасности могут оказаться неэффективными.

Первая особенность имеет **существенное значение для безопасности информации,** так как сами по себе факты утери документа или разглашения сведений за пределы контролируемой зоны и другие действия далеко не всегда приводят к утечке информации.

В общем случае можно говоритьоб**утечке информации как факте нарушения ее безопасности** только в том случае**, если она попадает к злоумышленнику** независимо от того, знает или не знает об этом владелец информации. Если по какой-то причине на этом пути передачи информации происходит разрыв в цепочке, то информация исчезает вместе с ее носителем, а утечки информации не происходит.

Следовательно,**под утечкой следует понимать не процесс распространения носителя информации за пределы определенной области пространства** вообще**, а частный случай**распространения**, когда информация попадает к злоумышленнику**. Выход же носителя за пределы заданной области создает предпосылки для утечки информации и повышает угрозу ее безопасности.

Если **получатель информации санкционирован**, то речь идет не об утечке, а о **передаче информации** по так называемому **функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.**

Часто **хищение** и **утечку** информации рассматривают как **автономные процессы.**

Под **хищением понимают умышленное присвоение чужой собственности без разрешения ее законного владельца.**

Аналогичная ситуация с **утечкой** информации.

Физический путь переноса информации от ее источника к несанкционированному получателю называется **каналом утечки.**

2. Возможные каналы утечки информации.

Технические каналы утечки информации

Акустический канал

Акустический канал утечки информации реализуется в следующем:

подслушивание разговоров на открытой местности и в помещениях, находясь рядом или используя направленные микрофоны (бывают параболические, трубчатые или плоские). Направленность 2-5 градусов, средняя дальность действия наиболее распространенных – трубчатых составляет около 100 метров. При хороших климатических условиях на открытой местности параболический направленный микрофон может работать на расстояние до 1 км;

- негласная запись разговоров на диктофон или магнитофон (в т.ч. цифровые диктофоны, активизирующиеся голосом);
- подслушивание разговоров с использованием выносных микрофонов (дальность действия радиомикрофонов 50-200 метров без ретрансляторов).

Микрофоны, используемые в радиозакладках, могут быть встроенными или выносными и имеют два типа: акустические (чувствительные в основном к действию звуковых колебаний воздуха и предназначенные для перехвата речевых сообщений) и вибрационные (преобразующие в электрические сигналы колебания, возникающие в разнообразных жестких конструкциях).

Акустоэлектрический канал

Акустоэлектрический канал утечки информации, особенностями которого являются:

- удобство применения (электросеть есть везде);
- отсутствие проблем с питанием у микрофона;
- возможность съема информации с питающей сети не подключаясь к ней (используя электромагнитное излучение сети электропитания). Прием информации от таких "жучков" осуществляется специальными приемниками, подключаемыми к силовой сети в радиусе до 300 метров от "жучка" по длине проводки или до силового трансформатора, обслуживающего здание или комплекс зданий;
- возможные помехи на бытовых приборах при использовании электросети для передачи информации, а также плохое качество передаваемого сигнала при большом количестве работы бытовых приборов.

Предотвращение:

- трансформаторная развязка является препятствием для дальнейшей передачи информации по сети электропитания;

Телефонный канал

Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен:

- гальванический съем телефонных переговоров (путем контактного подключения подслушивающих устройств в любом месте абонентской телефонной сети). Определяется путем ухудшения слышимости и появления помех, а также с помощью специальной аппаратуры;
- телефонно-локационный способ (путем высокочастотного навязывания). По телефонной линии подается высокочастотный тональный сигнал, который воздействует на нелинейные элементы телефонного аппарата (диоды, транзисторы, микросхемы) на которые также воздействует акустический сигнал. В результате в телефонной линии формируется высокочастотный модулированный сигнал. Обнаружить подслушивание возможно по наличию высокочастотного сигнала в телефонной линии. Однако дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает ста метров. Возможное противодействие: подавление в телефонной линии высокочастотного сигнала;
- индуктивный и емкостной способ негласного съема телефонных переговоров (бесконтактное подключение).

Индуктивный способ — за счет электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии. В качестве приемного устройства съема информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии.

Ёмкостной способ — за счет формирования на обкладках конденсатора электростатического поля, изменяющегося в соответствии с изменением уровня телефонных переговоров. В качестве приемника съема телефонных

переговоров используется емкостной датчик, выполненный в виде двух пластин, плотно прилегающих к проводам телефонной линии.

Подслушивание разговоров в помещении с использованием телефонных аппаратов возможно следующими способами:

- низкочастотный и высокочастотный способ съема акустических сигналов и телефонных переговоров. Данный способ основан на подключении к телефонной линии подслушивающих устройств, которые преобразованные микрофоном звуковые сигналы передают по телефонной линии на высокой или низкой частоте. Позволяют прослушивать разговор как при поднятой, так и при опущенной телефонной трубке. Защита осуществляется путем отсекания в телефонной линии высокочастотной и низкочастотной составляющей;
- использование телефонных дистанционных подслушивающих устройств. Данный способ основывается на установке дистанционного подслушивающего устройства в элементы абонентской телефонной сети путем параллельного подключения его к телефонной линии и дистанционным включением. Дистанционное телефонное подслушивающее устройство имеет два деконспирирующих свойства: в момент подслушивания телефонный аппарат абонента отключен от телефонной линии, а также при положенной телефонной трубке и включенном подслушивающем устройстве напряжение питания телефонной линии составляет менее 20 Вольт, в то время как она должна составлять 60.

Оптический канал

В оптическом канале получение информации возможно путем:

- визуального наблюдения,
- фото-видеосъемки,
- использования видимого и инфракрасного диапазонов для передачи информации от скрыто установленных микрофонов и других датчиков.

В качестве среды распространения в оптическом канале утечки информации выступают:

- безвоздушное пространство;
- атмосфера;
- оптические световоды.

Безвоздушное пространство, являющееся средой распространения утечки информации, возникает при наблюдении за наземными объектами с космических аппаратов. К свойствам среды распространения, влияющих на длину канала утечки, относятся:

- характеристики прозрачности среды распространения;
- спектральные характеристики света.

3. Процесс внедрения DLP-систем

Внедрять системы DLP довольно просто, однако настроить их так, чтобы они начали приносить ощутимые выгоды, не так легко. На данный момент при внедрении систем мониторинга и контроля информационных потоков (мой вариант описания термина DLP) чаще всего используют один из следующих подходов:

1. ***Классический***. При таком подходе в компании уже определена критичная информация и требования по ее обработке, а система DLP только контролирует их выполнение.
2. ***Аналитический***. При этом в компании есть общее представление о том, что необходимо контролировать распространение критичной инофрмации (обычно конфиденциальной информации), однако поимание потоков информации и необъодимых требований к ним еще не определены. Тогда система DLP выступает в роде инструментария, собирающего необходимые данные, анализ которых позволит четко сформулировать требования по обработке информации, а затем уже и дополнительно, более точно, настроить и саму систему.

Кратко приведу примеры шагов по внедрению DLP, характерных для каждого из подходов..

Классический подход по внедрению DLP:

1. ***Определить основные бизнес процессы и проанализировать их***. На выходе внеобходимо получить документ "*Перечень конфиденциальной информации*" (иногда это может быть более расширенный перечень, что-то типа рабочего документа "*Перечень контролируемой информации*", т.к. например вы хотите контролировать и пресекать в электронной переписке использование ненормативной лексики) и рабочий документ "Перечень владельцев информации". Понимание того, кто является владельцем той или иной информации, необходимо для того, чтобы в последствии определить требования по ее обработке.
2. ***Определить основные носители информации и способы передачи.*** Необходимо понять, на каких носителях может присутствовать контролируемая иноформация в рамках ИТ-инфраструктуры организации. При этом хорошей практикой является разработка таких рабочих докуменов как "*Перечень носителей информации*" и "*Перечень возможных каналов утечки информации*".
3. ***Определить требования по использованию информации и сервисов***. Часто бывает, что такие требования формулируются в отдельных политиках, например, в документах "Политка использования электронной почты", "Политика использования сети Интернет" и другие. Однако удобнее разработать единую "*Политику допустимого использования ресурсов*". В ней имееь смысл указывать требования по следующим блокам: работа с электроной почтой и сетью Интернет, использование съемных носителей; использование рабочих станций и ноутбуков, обработка информации на персональных устройствах (кпк, смартфоны, планшеты и пр.), использование копировально-множительной техники и сетевых хранилищ данных, общение в социальных сетях и блогах, использование сервисов мгновенных сообщений, обработка информации, закрепленнной на твердых носителях (бумага).
4. ***Ознакомить сотрудников с требованиями по использованию информации и сервисов, определенными на предыдущем шаге.***
5. ***Спроектировать систему DLP***. С точки зрения технического проектирования, я рекомендую разрабатывать как минимум "*Техническое задание*" и "*Программу и методику испытаний*". также дополнительно пригодятся и такие документы как "*Корпоративный стандарт по настройке политик DLP*", в котором вы должны детально указать то, как система будет фильтравать информацию и реагировать на события и

инциденты, и "*Положение по распределению ролей по управлению и обслуживанию DLP*", в котором Вы зафиксируете роли и границы ответственности за управление DLP.

6. ***Внедрить и настроить систему DLP, запустить в опытную эксплуатацию.***Первоначально это лучше всего сделать в режиме мониторинга.
7. ***Провести обучение персонала, ответственного за управление и обслуживание DLP***. На данном этапе Вам желатьльно разработать *Комплект ролевых иснструкций по DLP* (управление и обеспечение).
8. ***Проанализировать итоги и результаты опытной эксплуатации, внести правки (при необходимости), запустить в промышленную эксплуатацию.***
9. ***Внести правки (при отсутствии, разработать) в процедуру управления инцидентами (или аналоги).***
10. ***Регулярно проводить анализ инцидентов и совершенствовать политику настройки DLP .***

Аналитический подход по внедрению DLP:

1. ***Спроектировать систему DLP***. На данном этапе будет достаточно простого "*Технического задания*" и "*Программы и методики испытаний*".

2. ***Определить и настроить минимальные политики DLP.*** Нашей задачей является не мониторинг и блокирование любых активностей, а именно сбор аналитической информации о том, какими каналами и средствами пользуются для передачи той или иной корпоративной информации.

3. ***Провести обучение персонала, ответственного за управление и обслуживание DLP.*** Тут можно использовать стандартные "вендорские" инструкции.

4. ***Внедрить и настроить систему DLP, запустить в опытную эксплуатацию*** (в режиме мониторинга).

5. ***Проанализировать итоги и результаты опытной эксплуатации.*** Задача - выявить и проанализировать основные информационные потоки.

6. ***Внести правки (разработать) основные документы, регламентирующие мониторинг и контроль информации, ознакомить с ними сотрудников.***Документы "*Перечень конфиденциальной информации*" и "*Политика допустимого использования*".

7. ***Внести правки в настройки DLP, определить процедуру управления и обслуживания DLP, запустить в промышленную эксплуатацию***. Разработать документы "*Корпоративный стандарт по настройке политик DLP*", "*Положение по распределению ролей по управлению и обслуживанию DLP*", "*Комплект ролевых инструкций по DLP*".

8. ***Внести правки (при отсутствии, разработать) в процедуру управления инцидентами (или аналоги).***

9. ***Регулярно проводить анализ инцидентов и совершенствовать политику настройки DLP.***

Подходы отличаются, но и тот и другой вполне подходят для внедрения систем DLP. Надеюсь, что представленная выше информация сможет навести Вас на новые удачные мысли по защите информации от утечек.

1. 4 Лекция № 4 (2 часа).

Тема: «Предотвращение утечек конфиденциальной информации»

1.4.1 Вопросы лекции:

1. Каналы утечки информации при эксплуатации ЭВМ.
2. Анализ передаваемой информации.
3. Методы защиты информации.

1.4.2 Краткое содержание вопросов:

1. Каналы утечки информации при эксплуатации ЭВМ.

Виды и природа каналов утечки информации при эксплуатации ЭВМ

В завершение рассмотрения технических каналов утечки информации следует особо остановится на таком актуальном вопросе, как каналы утечки информации, образующиеся при эксплуатации персональных электронно-вычислительных машин (ПЭВМ), или персональных компьютеров (ПК). Действительно, с точки зрения защиты информации эти технические устройства яв-ляются прекрасным примером для изучения практически всех каналов утечки информа-ции — начиная от радиоканала и заканчивая материально-вещественным. Учитывая роль, которую играют ПЭВМ в современном обществе вообще, а также тенденцию к по-всеместному использованию ПЭВМ для обработки информации с ограниченным досту-пом в частности, совершенно необходимо детальнее рассмотреть принципы образования каналов утечки информации при эксплуатации ПЭВМ.

Как известно, современные ПЭВМ могут работать как независимо друг от друга, так и взаимодействуя с другими ЭВМ по компьютерным сетям, причем последние могут быть не только локальными, но и глобальными.

С учетом этого фактора, полный перечень тех участков, в которых могут находиться подлежащие защите данные, может иметь следующий вид:

- непосредственно в оперативной или постоянной памяти ПЭВМ;
- на съемных магнитных, магнитооптических, лазерных и других носителях;
- на внешних устройствах хранения информации коллективного доступа (RAID-массивы, файловые серверы и т.п.);
- на экранах устройств отображения (дисплеи, мониторы, консоли);
- в памяти устройств ввода/вывода (принтеры, графопостроители, сканеры);
- в памяти управляющих устройств и линиях связи, образующих каналы сопряжения компьютерных сетей.

Каналы утечки информации образуются как при работе ЭВМ, так и в режиме ожида-ния. Источниками таких каналов являются:

- электромагнитные поля;
- наводимые токи и напряжения в проводных системах (питания, заземления и соединительных);

- переизлучение обрабатываемой информации на частотах паразитной генерации элементов и устройств технических средств (ТС) ЭВМ;
- переизлучение обрабатываемой информации на частотах контрольно-измерительной аппаратуры (КИА).

Помимо этих каналов, обусловленных природой процессов, протекающих в ПЭВМ и их техническими особенностями, в поставляемых на рынок ПЭВМ могут умышленно создаваться дополнительные каналы утечки информации. Для образования таких кана-лов может использоваться:

- размещение в ПЭВМ закладок на речь или обрабатываемую информацию (замаскированные под какие-либо электронные блоки);
- установка в ПЭВМ радиомаячков;
- умышленное применение таких конструктивно-схемных решений, которые приводят к увеличению электромагнитных излучений в определенной части спектра;
- установка закладок, обеспечивающих уничтожение ПЭВМ извне (схемные решения);
- установка элементной базы, выходящей из строя.

Кроме того, классификацию возможных каналов утечки информации в первом приближении можно провести на основании принципов, в соответствии с которыми обрабатывается информация, получаемая по возможному каналу утечки. Предполагается три типа обработки: человеком, аппаратурой, программой. В соответствии с каждым типом обработки всевозможные каналы утечки также разбиваются на три группы. Применительно к ПЭВМ группу каналов, в которых основным видом обработки является обработка человеком, составляют следующие возможные каналы утечки:

- хищение материальных носителей информации (магнитных дисков, лент, карт);
- чтение информации с экрана посторонним лицом;
- чтение информации из оставленных без присмотра бумажных распечаток.

В группе каналов, в которых основным видом обработки является обработка аппаратурой, можно выделить следующие возможные каналы утечки:

- подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

В группе каналов, в которых основным видом обработки является программная обработка, можно выделить следующие возможные каналы утечки:

- несанкционированный доступ программы к информации;
- расшифровка программой зашифрованной информации;
- копирование программой информации с носителей;
- блокирование или отключение программных средств защиты.

При этом техническому контролю должны подвергаться следующие потенциальные каналы утечки информации:

- побочные электромагнитные излучения в диапазоне частот от 10 Гц до 100 МГц;
- наводки сигналов в цепях электропитания, заземления и в линиях связи;

- опасные сигналы, образующиеся за счет электроакустических преобразований, которые могут происходить в специальной аппаратуре контроля информации. Эти сигналы должны контролироваться в диапазоне частот от 300 Гц до 3,4 кГц;
- каналы утечки информации, образующиеся в результате воздействия высокочастотных электромагнитных полей на различные провода, которые находятся в помеще-нии и могут, таким образом, стать приемной антенной. В этом случае проверка проводится в диапазоне частот от 20 кГц до 100 МГц.

Наиболее опасным каналом утечки является дисплей, так как с точки зрения защиты информации он является самым слабым звеном в вычислительной системе. Это обусловлено принципами работы видеоадаптера, состоящего из специализированных схем для генерирования электрических сигналов управления оборудования, которое обеспечивает генерацию изображения.

Схемы адаптера формируют сигналы, определяющее информацию, которая отобра-жается на экране. Для этого во всех видеосистемах имеется видеобуфер. Он представля-ет собой область оперативной памяти, которая предназначена только для хранения тек-ста или графической информации, выводимой на экран. Основная функция видеосисте-мы заключается в преобразовании данных из видеобуфера в управляющие сигналы дисплея, с помощью которых на его экране формируется изображение. Эти сигналы и стараются перехватить.

2. Анализ передаваемой информации.

Предлагается изучить степень защищенности передаваемой по туннельному соединению информации с использованием анализатора сетевого трафика.

ВЫПОЛНИТЬ!

1. На втором рабочем месте запустить произвольный web-сервер.

2. Запустить анализатор трафика и настроить его на перехват пакетов, передаваемых виртуальным сетевым адаптером VMnet1.

3. Отправить из ОС виртуальной машины несколько ECHO-запросов в адрес сервера двумя способами: сначала напрямую через сеть VMnet1 (адрес сервера 192.168.200.1), а затем через туннельное соединение (адрес сервера необходимо выяснить при помощи диалогового окна состояния соединения). Обратите внимание, что пакеты, посылаемые через туннельное соединение, не опознаются как ICMP-пакеты. Поскольку шифрование передаваемой информации и программное сжатие отключены, то содержимое исходного IP-пакета сохраняется в первоначальном виде. Изменения в передаваемой информации заключаются только в том, что к исходному пакету добавляется заголовок протокола PPTP, который затем снимается при выходе пакета из туннеля.

4. Перевести IP-адреса источников и приемников ECHO-запросов (всего 4 различных адреса) в шестнадцатеричную систему исчисления. Найти эти адреса в перехваченных пакетах. Убедиться, что при туннелировании IP адреса остаются неизменными и могут быть восстановлены в случае пере- хвата трафика. Привести пакеты ECHO-запросов, отправленных напрямую и через туннель, и выделить в них соответствующие IP-адреса.

5. Запустить на виртуальной машине Internet Explorer и подключиться к запущенному в локальной сети web-серверу. При помощи анализатора трафика посмотреть пакеты, передаваемые через интерфейс VMnet1. Найти HTTP-запросы, отправляемые на 80 (50h) порт web-сервера, а также ответы сервера, отправляемые с 80 порта. Текст HTTP-запроса начинается со слова GET, следующего за ним пробела и далее URL запрашиваемого ресурса. Сравнить эти пакеты с пакетами, передаваемыми по локальной сети. В чем выражено отличие этих пакетов?

6. Разорвать виртуальное соединение.

7. Включить шифрование передаваемой информации, для этого в свойствах соединения в ОС виртуальной машины установить следующий параметр:

Безопасность. Шифрование данных.

Установить виртуальное соединение. Отправить из ОС виртуальной машины несколько ECHO-запросов через туннельное соединение. Просмотреть перехваченный трафик, есть ли возможность установить, пакеты какого содержания передавались? Зашифрованы ли поля заголовков? Какая информация может быть перехвачена злоумышленником в случае его подключения к линии связи?

3.Методы защиты информации.

Современные методы защиты информации Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю.

Сегодня используется шесть основных способов защиты :

Препятствие;

Маскировка;

Регламентация;

Управление;

Принуждение;

Побуждение.

Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз. Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Маскировка — способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Управление — способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.

Регламентация — важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение — методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

1.5 Лекция № 5 (2 часа).

Тема: «Основы организации и обеспечения работ по технической защите информации»

1.5.1 Вопросы лекции:

1. Подходы к созданию комплексной защиты информации в организации.
2. Основные критерии оценки защиты информации от утечки.
3. Методы борьбы с утечками информации.

1.5.2 Краткое содержание вопросов:

1. Подходы к созданию комплексной защиты информации в организации.

Принципы построения комплексной системы защиты информации

При построении любой системы необходимо определить принципы, в соответствии с которыми она будет построена. Комплексной системы защиты информации (КСЗИ) — сложная система, функционирующая, как правило, в условиях неопределенности, требующая значительных материальных затрат. Поэтому определение основных принципов КСЗИ позволит определить основные подходы к ее построению:

- принцип законности заключается в соответствии принимаемых мер законодательству РФ о защите информации, а в случае отсутствия соответствующих законов — другим государственным нормативным документам по защите. В соответствии с принципом полноты защищаемой информации защите подлежит не только информация, составляющая государственную, коммерческую или служебную тайну, но и та часть несекретной информации, утрата которой может нанести ущерб ее собственнику либо владельцу. Реализация этого принципа позволяет обеспечить и охрану интеллектуальной собственности.
- принцип обоснованности защиты информации заключается в установлении путем экспертной оценки целесообразности засекречивания и защиты той или другой информации, вероятных экономических и других последствий такой защиты исходя из баланса жизненно важных интересов государства, общества и граждан. Это, в свою очередь, позволяет расходовать средства на защиту только той информации, утрата или утечка которой может нанести действительный ущерб ее владельцу.
- принцип создания специализированных подразделений по защите информации заключается в том, что такие подразделения являются непременным условием организации комплексной защиты, поскольку только специализированные службы способны должным образом разрабатывать и внедрять защитные мероприятия и осуществлять контроль за их выполнением.
- принцип участия в защите информации всех соприкасающихся с нею лиц исходит из того, что защита информации является служебной обязанностью каждого лица, имеющего по роду выполняемой работы отношение к защищаемой информации, и такое участие дает возможность повысить качество защиты.

- принцип персональной ответственности за защиту информации требует, чтобы каждое лицо персонально отвечало за сохранность и неразглашение вверенной ему защищаемой информации, а за утрату или распространение такой информации оно несет уголовную, административную или иную ответственность.
- принцип наличия и использования всех необходимых сил и средств заключается в том, что КСЗИ требует, во-первых, участия в ней руководства предприятия и специальной службы защиты информации; во-вторых, использования различных организационных форм и методов защиты; в-третьих, наличия необходимых материально-технических ресурсов, включая технические средства защиты.
- принцип превентивности предполагает заблаговременное принятие мер по защите информации. Из этого принципа вытекает, в частности, необходимость разработки защищенных информационных технологий.

Среди рассмотренных принципов едва ли можно выделить более или менее важные. А при построении комплексной системы защиты информации (КСЗИ) важно использовать их в совокупности.

2. Основные критерии оценки защиты информации от утечки.

Защиту информации оценивают и контролируют в условиях сложной помеховой обстановки, так как контролируемые параметры, как правило, ниже уровня непреднамеренных (фоновых) либо маскирующих (организованных) помех. Результаты измерений должны отвечать требованиям помехозащищенности, а также требованиям достоверности (верности) и степени соответствия нижнего порогового уровня защищенности, оцениваемого по параметрам сигналов при отношении сигнал/шум меньше единицы.

Нормативно-методические документы должны устанавливать воспроизводимость измерений (отображающаяся близость друг к другу результатов измерений, выполненных в различных условиях, в различное время, в различных местах, различными методами и средствами).

Воспроизводимость измерений должна быть высокой и соответствовать необходимой точности. Сложность помеховой обстановки, разнородность элементов и связей, высокая степень неопределенности сложной системы обусловливает временную задержку представления результатов оценки параметров, определяющих защиту информации. Методики измерений совершенствуются для уменьшения временной задержки.

3. Методы борьбы с утечками информации.

Методы

Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента. Первый способ позволяет избежать ложных срабатываний (ошибок первого рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д. Пропуски конфиденциальной информации (ошибки второго рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются.

Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности. Однако первоначально внешние угрозы считались более опасными. В последние годы на внутренние угрозы стали обращать больше внимания, и популярность DLP-систем возросла. Необходимость их использования стала упоминаться в стандартах и нормативных документах (например, раздел "12.5.4 Утечка информации" в стандарте ГОСТ ISO/IEC 17799-2005). Специализированные технические средства для защиты от внутренних угроз стали массово выпускаться только после 2000 года.

В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста. Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Обычно они стоят на прокси-серверах, серверах электронной почты, а также в виде отдельных серверов. Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т.п. Хостовые компоненты также стараются отслеживать изменение сетевых настроек, инсталляцию программ для туннелирования, стеганографии и другие возможные методы для обхода контроля. DLP-система должна иметь компоненты обоих указанных типов плюс модуль для централизованного управления

1. 6 Лекция № 6 (2 часа).

Тема: «Организация и осуществление работ по выявлению каналов утечки информации»

1.6.1 Вопросы лекции:

1. Компоненты системы предотвращения утечек.
2. Процесс внедрения DLP-систем.
3. Перспективы предотвращения утечки информации.

1.6.2 Краткое содержание вопросов:

1. Компоненты системы предотвращения утечек.

Системы защиты от утечек конфиденциальной информации (Data Loss Prevention - DLP) предназначены для отслеживания и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети. Помимо предотвращения утечек информации DLP система может выполнять функции по отслеживанию действий пользователей, записи и анализу их коммуникаций через e-mail, социальные сети, чаты и т.д. Основная задача систем DLP – обеспечение выполнения принятой в организации политики конфиденциальности (защита информации от утечки).

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый или репутационный ущерб, а также для организаций, которые настороженно относятся к лояльности своих сотрудников. Решения класса DLP по предотвращению утечек информации обеспечивают защиту такой конфиденциальной информации, как условия тендеров, заказы на услуги и решения, номера пластиковых карт, сведения о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и т.д.

Основные функции DLP-систем

- контроль передачи информации через Интернет с использованием E-Mail, HTTP, HTTPS, FTP, Skype, ICQ и других приложений и протоколов;
- контроль сохранения информации на внешние носители - CD, DVD, flash, мобильные телефоны и т.п.;
- защита информации от утечки путем контроля вывода данных на печать;
- блокирование попыток пересылки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий, использование карантинной папки;
- поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам;
- предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.

Обычно система класса DLP включает следующие компоненты:

- центр управления и мониторинга;
- агенты на рабочих станциях пользователей;

- сетевой шлюз DLP, устанавливаемый на Интернет-периметр.

2. Процесс внедрения DLP-систем.

На выбор технологической платформы влияют разнообразные факторы, далеко не всегда технического характера. Например, корпоративные стандарты. Если корпоративным стандартом являются продукты определенного вендора и в компании уже установлено соответствующее ПО, то внедрять, скорее всего, будут решение этого производителя. Аналогичная ситуация складывается и с выбором аппаратной платформы. В компании может быть принят целый ряд принципиальных решений – назовем их политическими, – которые сужают круг потенциальных платформ. Например, в качестве возможных вариантов рассматриваются исключительно отечественные или, наоборот, зарубежные вендоры. На выбор технологической платформы также влияют индивидуальные предпочтения, каждый выбирает по себе – обучать или регистрировать. Что имеется ввиду? По нашим наблюдениям, потребителей DLP-решений в России можно условно разделить на две группы. К первой относятся те, кто стремится, в первую очередь, обучать сотрудников выполнению существующих политик ИБ. Ко второй группе – те, кто предпочитает копить факты/доказательства для последующего разбора. Представителям первой группы логично предлагать решения, обладающие широким набором инструментов по обучению сотрудников (например, востребованы диалоговые окна с возможностью отказаться от действия, последствием которого будет являться нарушение политики ИБ). Для представителей второй группы больше подходят системы с широкими возможностями по хранению и поиску данных по архиву (лидером в этом сегменте DLP является комплекс «Дозор-Джет»). Безусловно, необходимо учитывать, реализованы ли в предлагаемой DLP-системе такие технологии и функции, как цифровые отпечатки, выявление идентификаторов, языковая поддержка, автоматическое определение кодировок сообщений и т. д. В начале статьи уже говорилось о том, что довольно часто компании необходимо оперативно внедрить DLP-решение для устранения выявленной уязвимости в системе ИБ. Именно по этой причине отсутствует возможность провести комплексное обследование бизнес-процессов и разработать политику DLP-системы на первом этапе внедрения. Для этих условий оптимально подходит комплекс «Дозор-Джет» – решение, которое, с одной стороны, поставляется с набором предустановленных правил фиксации инцидентов, с другой стороны, архивирует значительную часть обрабатываемых данных. Наличие архива позволяет ретроспективно исследовать

сохраненные данные и на их основе кастомизировать предустановленную политику фиксации .

3. Перспективы предотвращения утечки информации.

В связи с бурным развитием информационных технологий и технических средств система защиты информации предприятия становится уязвимой и как следствие предприятию может быть нанесен экономический ущерб.

Задача оптимизации комплексной системы защиты информации (КСЗИ) на предприятии становится перспективной и чрезвычайно актуальной. Решение задачи оптимизации КСЗИ на предприятии сводится к:

- минимизации затрат на построение КСЗИ,
- увеличению уровня защищенности, обеспечиваемого КСЗИ,
- выбора оптимального решения по построению КСЗИ на предприятии.

Условия, которые бы позволяли исключить (значительно снизить) возможность утечки информации на предприятиях различных форм собственности можно представить схемой функционирования комплексной системы защиты информации (КСЗИ) на предприятии (рис.1).

Модели, методы и средства защиты информации, используемые на предприятиях, различны и чаще всего выбираются по правилу:

$$<Z \rightarrow min, U_z \geq U_{dz}> \text{ или } <U_z \rightarrow max,\ Z \leq Z_d>, \quad (1)$$

где Z – затраты на разработку, реализацию, внедрение и администрирование КСЗИ на предприятии, U_z – уровень защиты, обеспечиваемый КСЗИ, Z_d – приемлемая стоимость КСЗИ на предприятии, U_{dz} – приемлемый уровень качества КСЗИ. Задачи (1) могут быть решены методами многокритериальной оптимизации, однако ограничены в практическом применении.

Для решения задачи оптимизации КСЗИ на предприятии предлагается использовать метод последовательных уступок [6], в котором выделяется ряд частных показателей качества защищенности, имеющих превосходство над остальными показателями, переводимыми в разряд ограничений.

Рассмотрим минимизацию затрат на построение КСЗИ.

Пусть $a_{ij} = 1$, если i -ое средство информационной безопасности выбрано для защиты j -го информационного ресурса предприятия, и $a_{ij} = 0$, если i -ое средство информационной безопасности не используется для защиты от угроз.

Требуется минимизировать затраты вида

$$Z = \sum_{i=1}^{n}\sum_{j=1}^{m} Z_{ij}a_{ij} + \sum_{i=1}^{n} Z_i k_i \rightarrow \min$$

(2)

при соблюдении граничных условий:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} s_j m_{ij} a_{ij} \geq U_{dz}\ ,\ \sum_{i=1}^{n} a_{ij} = 1, \forall j \in J\ ,$$

$$\sum_{j=1}^{m} s_{ij} = 1, a_{ij} \in \{0;1\}\ ,\ k_{ij} \in \{0;1\}\ ,$$

(3)

, где Z_{ij} – затраты на защиту j -го информационного ресурса i -м средством, i = 1, n, j = 1, m, Zi – затраты для совокупности информационных ресурсов i -м средством, I = $\{i_1, i_2, ..., i_n\}$ – множество средств КСЗИ на предприятии, $J = \{ j_1, j_2, ..., j_m\}$ – множество защищаемых информационных ресурсов, m_{ij} – оценка качества защиты i -м средством j -го информационного ресурса, s_j – коэффициент j -го информационного ресурса в интегрированной оценке качества КСЗИ, k_iпеременная бинарного типа, k_i Î{0;1}, k_i = 1 , если i -е средство КСЗИ может быть использовано, k_i = 0 – в противном случае.

Рассмотрим увеличение уровня защищенности, обеспечиваемого КСЗИ. Требуется максимизировать уровень U_z:

$$U_z = \sum_{i=1}^{n}\sum_{j=1}^{m} s_j m_{ij} a_{ij} \rightarrow \max$$

(4)

при соблюдении следующих граничных условий:

$$Z = \sum_{i=1}^{n}\sum_{j=1}^{m} Z_{ij}a_{ij} + \sum_{i=1}^{n} Z_i k_i \leq Z_d\ ,\ \sum_{i=1}^{n} a_{ij} = 1, \forall j \in J\ ,\ k_i \in \{0;1\}\ ,\ a_{ij} \in \{0;1\}$$

(5)

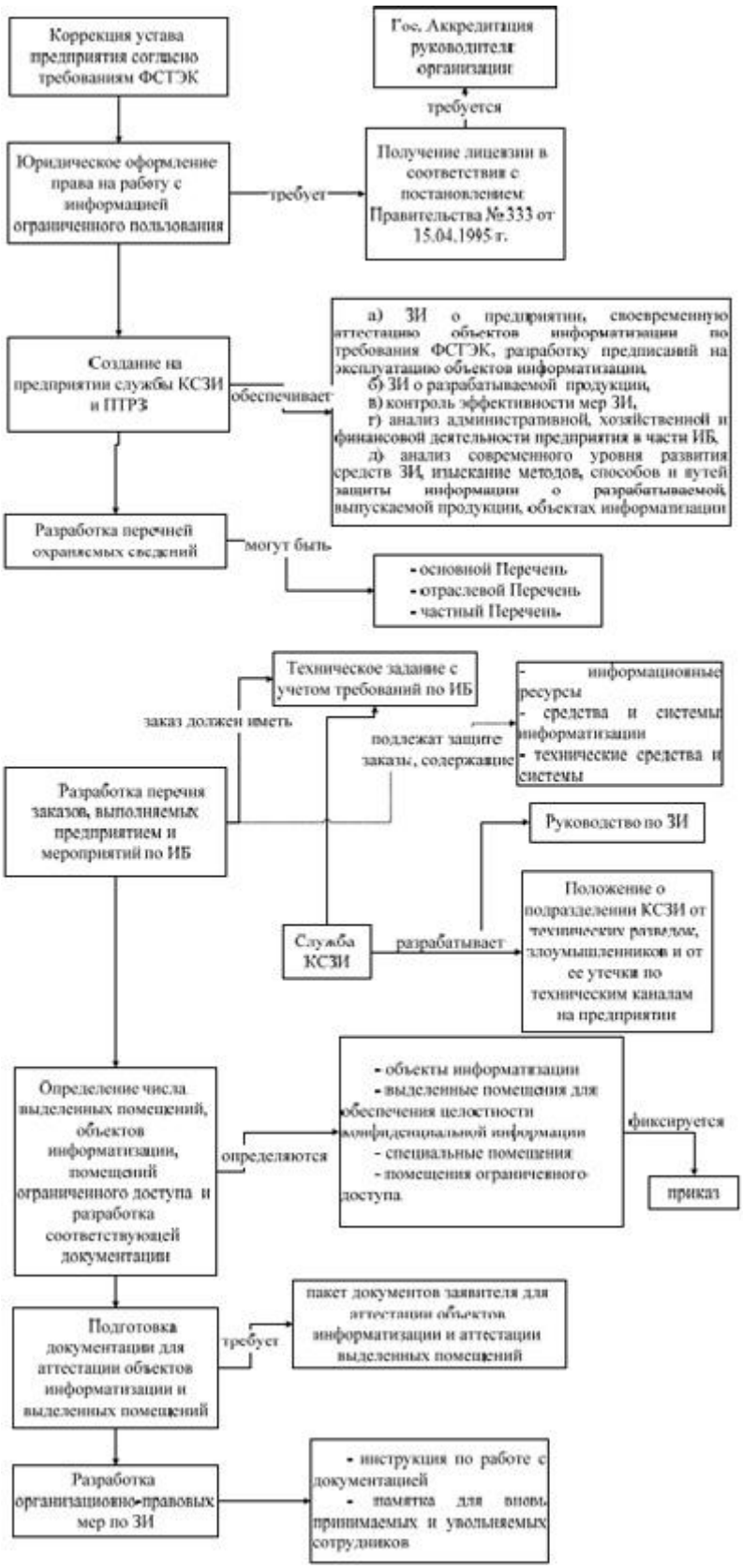


Рис.1. Обобщенная схема функционирования службы КСЗИ

При построении интегрированной оценки уровня U_z защищенности информации, обеспечиваемый КСЗИ на предприятии, предложен следующий расчет коэффициентов защищенности отдельных бизнес-процессов $K_{bi} = \{k_{b1}, k_{b2},..., k_{bs}\}$ предприятия [2]:

$$K_{b_i} = 1 - \frac{\sum_{i=1}^{s} n_i \sum_{i \in P_i} \omega_{iw} y_i (1 - \Delta_w)}{\sum_{i=1}^{s} n_i \sum_{i \in P_i} \omega_{wi} y_i}$$

(6)

где P_i – количество наиболее вероятных информационных угроз для i -ой бизнес-операции на предприятии, Δ_w – коэффициент защищенности от w -й угрозы, ω_{wi} – интенсивность потока атак w -го вида угроз на i –ю бизнес-операцию ($w \in P_i$), для $w \notin P_i$,$w_{wi} = 0$, y_i – время выполнения i -й бизнес-операции, O – количество бизнес-операций в бизнес-процессе предприятия, n_i – вероятность выполнения бизнес-операции i в совокупности бизнес-процессов предприятия, $O = \{o_j \mid j = 1,p\}$,$O_j \subset k_{bi}$.

Рассмотрим выбор оптимального решения по построению КСЗИ на предприятии [3, 4]. Выбор оптимального решения по построению КСЗИ на предприятии основан на анализе многопараметрического критерия, зависящего от ряда частных показателей качества работы КСЗИ. В соответствии с (1) основанием для вывода об абсолютном превосходстве одних показателей над другими служит степень различия отдельных показателей по важности, при которой сравнение оценок вариантов построения системы КСЗИ осуществляется только по самому важному показателю без учета остальных, затем только по второму показателю и т.д.

Особое место в современной системе защиты информации на предприятии имеют информационные ресурсы. Под информационными ресурсами понимаются документы и массивы документов в информационных системах предприятия [7].

Информационные ресурсы предприятия подвержены различного рода угрозам. Для снижения угроз, уязвимостей, рисков на предприятии необходим контроль и эффективное управление информационными ресурсами. Эффективное управление подразумевает принятие решений при оптимизации комплексной системы защиты информации на предприятии (рис. 2).

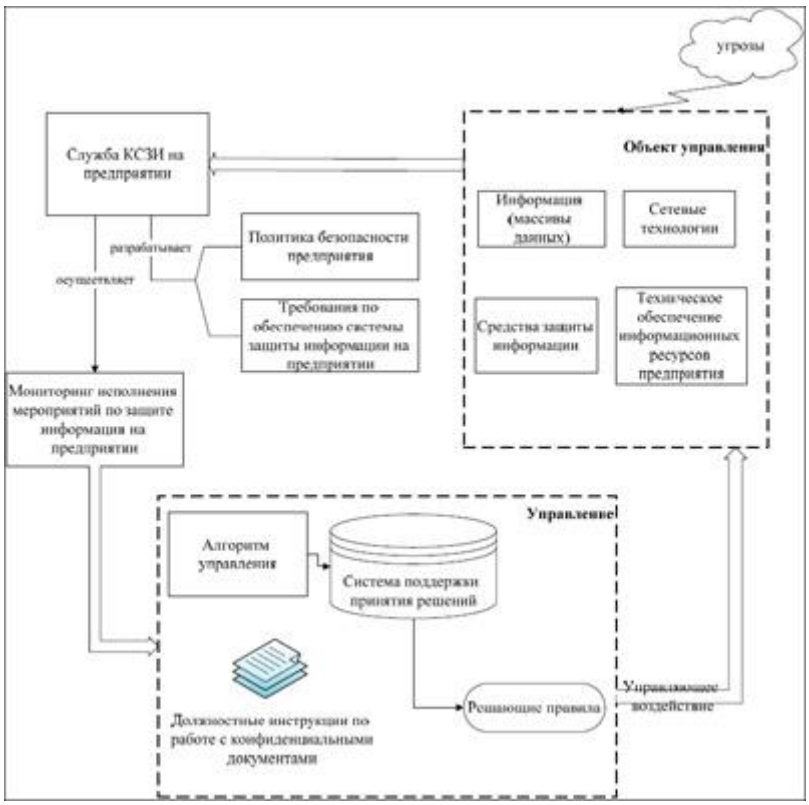


Рис.2. Структурная схема управления при оптимизации КСЗИ на предприятии

Вопросы распределения, использования и защиты информационных ресурсов предприятия возложены на службу КСЗИ, которая формирует стратегию потребностей в информационных ресурсах, оценивает текущее состояние системы защиты информации и эффективность использования информационных ресурсов.

На предприятии защита информационных ресурсов сводится к оптимизации методов защиты информации, технических средств и его состава. Управление информационными ресурсами связано с информационной мощностью предприятия [1]. Информационная мощность предприятия – синергетическая характеристика, описывающая степень эффективности использования существующих информационных активов для увеличения конкурентоспособности предприятия с достижением максимума при:

- полном использовании функционала и возможностей информационных систем,
- организации информационных бизнес-решений, адекватных решаемым предприятием задачам [1].

1. 7 Лекция № 7 (2 часа).

Тема: «Типовые средства защиты информации и особенности их эксплуатации»

1.7.1 Вопросы лекции:

1. Общая характеристика средств защиты информации от утечки по техническим каналам.
2. Обзор средств активной защиты: акустика, виброакустика, слаботочные линии, сотовые телефоны, диктофоны, постановщики помех.
3. Современные фавориты в области защиты от утечек.

1.7.2 Краткое содержание вопросов:

1. Общая характеристика средств защиты информации от утечки по техническим каналам.

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают **способ получения с помощью ТСР разведывательной информации** об объекте. Причем под **разведывательной информацией** обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими, и т.д. То есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах.

В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. Например воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт (земля) и т.п.

Технические средства разведки служат для приема и измерения параметров сигналов. В данном пособии рассматриваются портативные средства разведки, используемые для перехвата информации, обрабатываемой в технических средствах, акустической (речевой) информации, а также средства скрытого виденаблюдения и съемки.

2. Обзор средств активной защиты: акустика, виброакустика, слаботочные линии, сотовые телефоны, диктофоны, постановщики помех.

Задачей технических средств защиты информации является либо ликвидация каналов утечки информации, либо снижение качества получаемой злоумышленником информации. Основным показателем качества речевой информации считается разборчивость – слоговая, словесная, фразовая и др. Чаще всего используют слоговую разборчивость, измеряемую в процентах. Принято считать, что качество акустической информации достаточное, если обеспечивается около 40 % слоговой разборчивости. Если разобрать разговор практически невозможно (даже с использованием современных технических средств повышения разборчивости речи в шумах), то слоговая разборчивость соответствует около 1–2 %.

Предупреждение утечки информации по акустическим каналам сводится к пассивным и активным способам защиты. Соответственно, все приспособления защиты информации можно смело разделить на два больших класса – пассивные и активные. Пассивные – измеряют, определяют, локализуют каналы утечки, ничего не внося при этом во внешнюю среду. Активные – «зашумляют», «выжигают», «раскачивают» и уничтожают всевозможные спецсредства негласного получения информации.

Пассивное техническое средство защиты – устройство, обеспечивающее скрытие объекта защиты от технических способов разведки путем поглощения, отражения или рассеивания его излучений. К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного способа – максимально ослабить акустический сигнал от источника звука, например, за счет отделки стен звукопоглощающими материалами.

По результатам анализа архитектурно-строительной документации формируется комплекс необходимых мер по пассивной защите тех или иных участков. Перегородки и стены по возможности должны быть слоистыми, материалы слоев – подобраны с резко отличающимися акустическими характеристиками (например, бетон—поролон). Для уменьшения мембранного переноса желательно, чтобы они были массивными. Кроме того, разумнее устанавливать двойные двери с воздушной прослойкой между ними и уплотняющими прокладками по периметру косяка. Для защиты окон от утечки информации их лучше делать с двойным остеклением, применяя звукопоглощающий материал и увеличивая расстояние между стеклами для повышения звукоизоляции, использовать шторы или жалюзи. Желательно оборудовать стекла излучающими вибродатчиками. Различные отверстия во время ведения конфиденциальных разговоров следует перекрывать звукоизолирующими заслонками.

Другим пассивным способом пресечения утечки информации является правильное устройство заземления технических средств передачи информации. Шина заземления и заземляющего контура не должна иметь петель, и ее рекомендуется выполнять в виде ветвящегося дерева. Магистрали заземления вне здания следует прокладывать на глубине около 1,5 м, а внутри здания – по стенам или специальным каналам (для возможности регулярного осмотра). В случае подключения к магистрали заземления нескольких технических средств соединять их с магистралью нужно параллельно. При устройстве заземления нельзя применять естественные заземлители (металлические конструкции зданий, имеющие соединение с землей, проложенные в земле металлические трубы, металлические оболочки подземных кабелей и т. д.).

Так как обычно разнообразные технические приборы подключены к общей сети, то в ней возникают различные наводки. Для защиты техники от внешних сетевых помех и защиты от наводок, создаваемых самой аппаратурой, необходимо использовать сетевые фильтры. Конструкция фильтра должна обеспечивать существенное снижение вероятности возникновения внутри корпуса побочной связи между входом и выходом из-за магнитных, электрических либо электромагнитных полей. При этом однофазная система распределения электроэнергии должна оснащаться трансформатором с заземленной средней точкой, трехфазная – высоковольтным понижающим трансформатором.

Экранирование помещений позволяет устранить наводки от технических средств передачи информации (переговорных комнат, серверных и т. п.). Лучшими являются экраны из листовой стали. Но применение сетки значительно упрощает вопросы вентиляции, освещения и стоимости экрана. Чтобы ослабить уровни излучения технических средств

передачи информации примерно в 20 раз, можно рекомендовать экран, изготовленный из одинарной медной сетки с ячейкой около 2,5 мм либо из тонколистовой оцинкованной стали толщиной 0,51 мм и более. Листы экранов должны быть между собой электрически прочно соединены по всему периметру. Двери помещений также необходимо экранировать, с обеспечением надежного электроконтакта с дверной рамой по всему периметру не реже, чем через 10–15 мм. При наличии в помещении окон их затягивают одним или двумя слоями медной сетки с ячейкой не более 2 мм. Слои должны иметь хороший электроконтакт со стенками помещения.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

К активным техническим средствам защиты относятся также различные имитаторы, средства постановки аэрозольных и дымовых завес, устройства электромагнитного и акустического зашумления и другие средства постановки активных помех. Активный способ предупреждения утечки информации по акустическим каналам сводится к созданию в «опасной» среде сильного помехового сигнала, который сложно отфильтровать от полезного.

Современная техника подслушивания дошла до такого уровня, что становится очень сложно обнаружить приборы считывания и прослушивания. Самыми распространенными методами выявления закладочных устройств являются: визуальный осмотр; метод нелинейной локации; металлодетектирование; рентгеновское просвечивание.

Проводить специальные меры по обнаружению каналов утечки информации и дорого, и долго. Поэтому в качестве средств защиты информации часто выгоднее использовать устройства защиты телефонных переговоров, генераторы пространственного зашумления, генераторы акустического и виброакустического зашумления, сетевые фильтры. Для предотвращения несанкционированной записи переговоров используют устройства подавления диктофонов.

Подавители диктофонов (также эффективно воздействующие и на микрофоны) применяют для защиты информации с помощью акустических и электромагнитных помех. Они могут воздействовать на сам носитель информации, на микрофоны в акустическом диапазоне, на электронные цепи звукозаписывающего устройства. Существуют стационарные и носимые варианты исполнения различных подавителей.

В условиях шума и помех порог слышимости для приема слабого звука возрастает. Такое повышение порога слышимости называют акустической маскировкой. Для формирования виброакустических помех применяются специальные генераторы на основе электровакуумных, газоразрядных и полупроводниковых радиоэлементов.

На практике наиболее широкое применение нашли *генераторы шумовых колебаний*. Шумогенераторы *первого типа* применяются для подавления непосредственно микрофонов как у радиопередающих устройств, так и у диктофонов, т. е. такой прибор банально вырабатывает некий речеподобный сигнал, передаваемый в акустические колонки и вполне эффективно маскирующий человеческую речь. Кроме того, такие устройства применяются для борьбы с лазерными микрофонами и стетоскопическим прослушиванием. Надо отметить, что акустические шумогенераторы – едва ли не

единственное средство для борьбы с проводными микрофонами. При организации акустической маскировки следует помнить, что акустический шум создает дополнительный дискомфорт для сотрудников, для участников переговоров (обычная мощность генератора шума составляет 75–90 дБ), однако в этом случае удобство должно быть принесено в жертву безопасности.

Известно, что «белый» или «розовый» шум, используемый в качестве акустической маскировки, по своей структуре имеет отличия от речевого сигнала. На знании и использовании этих отличий как раз и базируются алгоритмы шумоочистки речевых сигналов, широко используемые специалистами технической разведки. Поэтому наряду с такими шумовыми помехами в целях активной акустической маскировки сегодня применяют более эффективные генераторы «речеподобных» помех, хаотических последовательностей импульсов и т. д. Роль устройств, преобразующих электрические колебания в акустические колебания речевого диапазона частот, обычно выполняют малогабаритные широкополосные акустические колонки. Они обычно устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки.

«Розовый» шум – сложный сигнал, уровень спектральной плотности которого убывает с повышением частоты с постоянной крутизной, равной 3–6 дБ на октаву во всем диапазоне частот. «Белым» называется шум, спектральный состав которого однороден по всему диапазону излучаемых частот. То есть такой сигнал является сложным, как и речь человека, и в нем нельзя выделить какие-то преобладающие спектральные составляющие. «Речеподобные» помехи формируются путем микширования в различных сочетаниях отрезков речевых сигналов и музыкальных фрагментов, а также шумовых помех, или из фрагментов самого скрываемого речевого сигнала при многократном наложении с различными уровнями (наиболее эффективный способ).

Системы *ультразвукового подавления* излучают мощные неслышимые человеческим ухом ультразвуковые колебания (около 20 кГц). Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты диктофона и к значительным искажениям записываемых (передаваемых) сигналов. Но опыт использования этих систем показал их несостоятельность. Интенсивность ультразвукового сигнала оказывалась выше всех допустимых медицинских норм воздействия на человека. При снижении интенсивности ультразвука невозможно надежно подавить подслушивающую аппаратуру.

Акустический и виброакустический генераторы вырабатывают шум (речеподобный, «белый» или «розовый») в полосе звуковых сигналов, регулируют уровень шумовой помехи и управляют акустическими излучателями для постановки сплошной шумовой акустической помехи. Вибрационный излучатель служит для постановки сплошной шумовой вибропомехи на ограждающие конструкции и строительные коммуникации помещения. Расширение границ частотного диапазона помеховых сигналов позволяет снизить требования к уровню помехи и снизить словесную разборчивость речи.

На практике одну и ту же поверхность приходится зашумлять несколькими виброизлучателями, работающими от разных, некоррелированных друг с другом источников помеховых сигналов, что явно не способствует снижению уровня шумов в помещении. Это связано с возможностью использования метода компенсации помех при подслушивании помещения. Данный способ заключается в установке нескольких микрофонов и двух– или трехканальном съеме смеси скрываемого сигнала с помехой в пространственно разнесенных точках с последующим вычитанием помех.

Электромагнитный генератор (генератор *второго типа)* наводит радиопомехи непосредственно на микрофонные усилители и входные цепи диктофона. Данная аппаратура одинаково эффективна против кинематических и цифровых диктофонов. Как правило, для этих целей применяют генераторы радиопомех с относительно узкой полосой излучения, чтобы снизить воздействие на обычную радиоэлектронную аппаратуру (они практически не оказывают воздействия на работу сотовых телефонов стандарта GSM, при условии, что связь по телефону была установлена до включения подавителя). Электромагнитную помеху генератор излучают направленно, обычно это конус 60–70°. А для расширения зоны подавления устанавливают вторую антенну генератора или даже четыре антенны.

Следует знать, что при неудачном расположении подавителей могут возникать ложные срабатывания охранной и пожарной сигнализации. Приборы с мощностью больше 5–6 Вт не проходят по медицинским нормам воздействия на человека.

3. Современные фавориты в области защиты от утечек.

Изолированная автоматизированная система для работы с конфиденциальной информацией

Сущность одного из первых способов, который начал применяться для защиты от утечки конфиденциальной информации, состоит в создании выделенной автономной АС, состоящей из средств вычислительной техники, необходимых для работы с конфиденциальной информацией (рис. 2). При этом такая АС полностью изолируется от любых внешних систем, что даёт возможность исключить возможную утечку информации по сети.

Рис. 2. Выделенная изолированная АС, предназначенная для обработки конфиденциальной информации

АС этого типа оснащаются системами контроля доступа, а также системами видеонаблюдения. Доступ в помещения, в которых находится АС, осуществляется по специальным пропускам, при этом обычно производится личный досмотр сотрудников с целью контроля электронных и бумажных носителей информации. Для блокирования возможности утечки информации путём её копирования на внешние носители, из компьютеров АС, как правило, удаляются все устройства, при помощи которых можно записать информацию на такие носители. Кроме того, опечатываются все системные

блоки и порты компьютеров для исключения возможности несанкционированного подключения новых устройств. При необходимости передать информацию за пределы выделенного помещения данная процедура проводится одним или несколькими сотрудниками по строго оговоренному регламенту при помощи соответствующего оборудования. В этом случае для работы с открытой информацией, а также для доступа к Интернет-ресурсам используется отдельная система, которая физически никак не связана с АС, обрабатывающей конфиденциальную информацию.

Как правило, описанный подход применяется в государственных структурах для защиты секретной информации. Он позволяет обеспечить защиту от всех вышеперечисленных каналов утечки конфиденциальной информации. Однако на практике во многих коммерческих организациях большинство сотрудников должно одновременно иметь доступ к конфиденциальной и открытой информации, а также работать с Интернет-ресурсами. В такой ситуации создание изолированной среды обработки конфиденциальной информации потребовало бы создание двух эквивалентных АС, одна из которых предназначалась только для обработки конфиденциальной информации, а другая – для работы с открытыми данными и ресурсами Интернет. Такой подход, как правило, невозможно реализовать из-за его очевидной избыточности и высокой стоимости.

Системы активного мониторинга рабочих станций пользователей

Системы активного мониторинга [4] представляют собой специализированные программные комплексы, предназначенные для выявления несанкционированных действий пользователей, связанных, в частности, с попыткой передачи конфиденциальной информации за пределы контролируемой территории предприятия. Системы мониторинга состоят из следующих компонентов (рис. 3):

- модули-датчики, устанавливаемые на рабочие станции пользователей и обеспечивающие сбор информации о событиях, регистрируемых на этих станциях;
- модуль анализа данных, собранных датчиками, с целью выявления несанкционированных действий пользователей, связанных с утечкой конфиденциальной информации;
- модуль реагирования на выявленные несанкционированные действия пользователей;
- модуль хранения результатов работы системы;
- модуль централизованного управления компонентами системы мониторинга.

Датчики систем мониторинга устанавливаются на те рабочие станции, на которых пользователи работают с конфиденциальной информацией. На основе настроек, заданных администратором безопасности, датчики системы позволяют контролировать доступ приложений пользователей к конфиденциальной информации, а также накладывать ограничения на те действия, которые пользователь может выполнить с этой информацией. Так, например, системы активного мониторинга позволяют запретить запись конфиденциальной информации на внешние носители, заблокировать передачу информации на внешние сетевые адреса, а также вывод данных на печать.

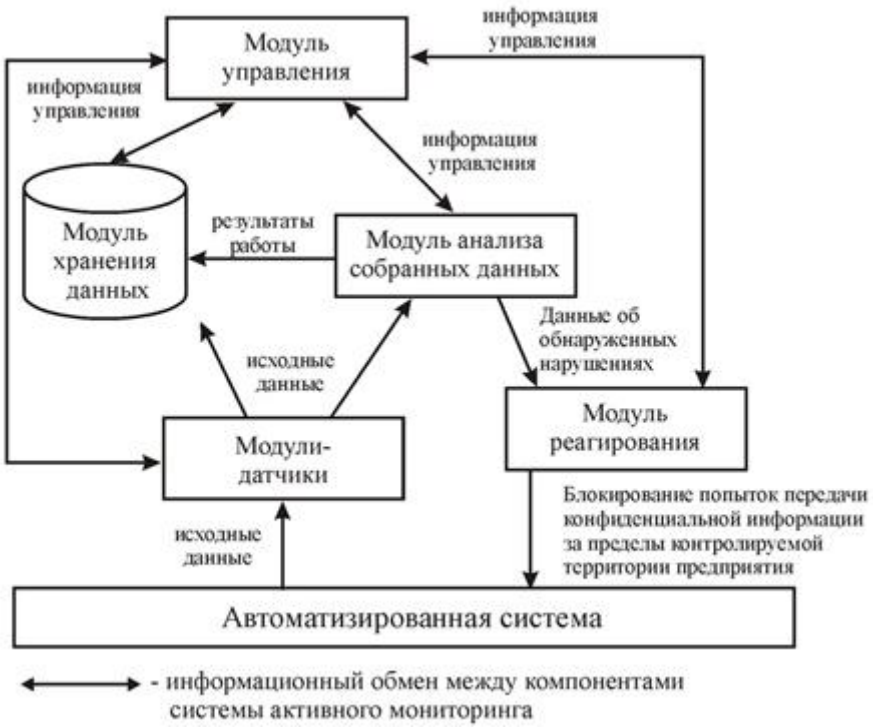


Рис. 3. Типовая архитектура систем активного мониторинга рабочих станций пользователей

Примерами коммерческих программных продуктов, которые могут быть отнесены к классу систем активного мониторинга, являются - система управления политикой безопасности «Урядник» (www.rnt.ru), система разграничения доступа «DeviceLock» (www.devicelock.ru) и система мониторинга «InfoWatch» (www.infowatch.ru).

Преимуществом использования систем мониторинга является возможность создания виртуальной изолированной среды обработки конфиденциальной информации без физического выделения отдельной АС для работы с данными ограниченного доступа. Кроме того, системы этого типа позволяют программно ограничить вывод информации на внешние носители, что избавляет от необходимости физического удаления из компьютеров устройств записи информации, а также опечатывания портов и системных блоков. Однако, применение систем активного мониторинга влечёт за собой установку дополнительного ПО на каждую рабочую станцию, что потенциально может привести к увеличению сложности администрирования АС, а также к возможным конфликтам в работе программ системы.

Выделенный сегмент терминального доступа к конфиденциальной информации

Ещё один способ защиты от утечки конфиденциальной информации заключается в организации доступа к конфиденциальной информации АС через промежуточные терминальные серверы. При такой схеме доступа пользователь сначала подключается к терминальному серверу, на котором установлены все приложения, необходимые для работы с конфиденциальной информацией. После этого пользователь в терминальной сессии запускает эти приложения и начинает работать с ними так, как будто они установлены на его рабочей станции (рис. 4).

Рис. 4. Схема установки терминального сервера доступа к конфиденциальным данным

В процессе работы в терминальной сессии пользователю отсылается только графическое изображение рабочей области экрана, в то время как вся конфиденциальная информация, с которой он работает, сохраняется лишь на терминальном сервере. Один такой терминальный сервер, в зависимости от аппаратной и программной конфигурации, может одновременно обслуживать сотни пользователей. Примерами терминальных серверов являются продукты Microsoft Terminal Services (www.microsoft.com) и Citrix MetaFrame (www.citrix.com).

Практическое использование технического решения на основе терминального сервера позволяет обеспечить защиту от несанкционированного копирования конфиденциальной информации на внешние носители за счёт того, что вся информация хранится не на рабочих станциях, а на терминальном сервере. Аналогичным образом обеспечивается защита и от несанкционированного вывода документов на печать. Распечатать документ пользователь может только при помощи принтера, установленного в сегменте терминального доступа. При этом все документы, выводимые на этот принтер, могут регистрироваться в установленном порядке.

Использование терминального сервера позволяет также обеспечить защиту от несанкционированной передачи конфиденциальной информации по сети на внешние серверы вне пределов контролируемой территории предприятия. Достигается это путём фильтрации всех пакетов данных, направленных вовне сегмента терминального доступа, за исключением тех пакетов, которые обеспечивают передачу графического изображения рабочей области экрана на станции пользователей. Такая фильтрация может быть реализована при помощи межсетевого экрана, установленного в точке сопряжения сегмента терминального доступа с остальной частью АС. В этом случае все попытки установить соединения с терминального сервера на узлы сети Интернет будут заблокированы. При этом сама рабочая станция может иметь беспрепятственный доступ к Интернет-ресурсам. Для обмена информацией между пользователями, работающими в терминальных сессиях, может использоваться выделенный файловый сервер, расположенный в терминальном сегменте доступа.

Средства контентного анализа исходящих пакетов данных

Средства контентного анализа обеспечивают возможность обработки сетевого трафика, отправляемого за пределы контролируемой территории с целью выявления возможной утечки конфиденциальной информации. Используются они, как правило, для анализа исходящего почтового и web-трафика, отправляемого в сеть Интернет. Примерами средств контентного анализа этого типа являются системы «Дозор-Джет» (www.jetinfo.ru), «Mail Sweeper» (www.infosec.ru) и «InfoWatch Web Monitor» (www.infowatch.com). Такие средства защиты устанавливаются в разрыв канала связи между сетью Интернет и

АС предприятия, таким образом, чтобы через них проходили все исходящие пакеты данных (рис. 5).

Рис. 5. Схема установки средств контентного анализа в АС

В процессе анализа исходящих сообщений последние разбиваются на служебные поля, которые обрабатываются по критериям, заданным администратором безопасности. Так, например, средства контентного анализа позволяют блокировать пакеты данных, которые содержат такие ключевые слова, как – «секретно», «конфиденциально» и др. Эти средства также предоставляют возможность фильтровать сообщения, которые направляются на внешние адреса, не входящие в систему корпоративного электронного документооборота.

Преимуществом систем защиты данного типа является возможность мониторинга и накладывания ограничений, как на входящий, так и исходящий поток трафика. Однако, эти системы не позволяют гарантировать стопроцентное выявление сообщений, содержащих конфиденциальную информацию. В частности, если нарушитель перед отправкой сообщения зашифрует его или замаскирует под видом графического или музыкального файла при помощи методов стеганографии, то средства контентного анализа в этом случае окажутся практически бессильными.

Средства криптографической защиты конфиденциальной информации

Для защиты от утечки информации могут использоваться и криптографические средства, обеспечивающие шифрование конфиденциальных данных, хранящихся на жёстких дисках или других носителях. При этом ключ, необходимый для декодирования зашифрованной информации, должен храниться отдельно от данных. Как правило, он располагается на внешнем отчуждаемом носителе, таком как дискета, ключ Touch Memory или USB-носитель. В случае, если нарушителю и удастся украсть носитель с конфиденциальной информацией, он не сможет её расшифровать, не имея соответствующего ключа.

Рассмотренный вариант криптографической защиты не позволяет заблокировать другие каналы утечки конфиденциальной информации, особенно если они совершаются пользователем после того, как он получил доступ к данным. С учётом этого недостатка компанией Microsoft была разработана технология управления правами доступа RMS (Windows Rights Management Services) [2] на основе операционной системы Windows Server 2003. Согласно этой технологии вся конфиденциальная информация хранится и передаётся в зашифрованном виде, а её дешифрование возможно только на тех компьютерах и теми пользователями, которые имеют на это права. Вместе с конфиденциальными данными также передаётся специальный XML-файл, содержащий категории пользователей, которым разрешён доступ к информации, а также список тех действий, которые эти пользователи могут выполнять. Так, например, при помощи такого XML-файла, можно запретить пользователю копировать конфиденциальную информацию на внешние носители или выводить её на печать. В этом случае, даже если пользователь скопирует информацию на внешний носитель, она останется в зашифрованном виде и он не сможет получить к ней доступ на другом компьютере. Кроме того, собственник информации может определить временной период, в течение которого пользователь сможет иметь доступ к информации. По истечении этого периода доступ пользователя

автоматически блокируется. Управление криптографическими ключами, при помощи которых возможна расшифровка конфиденциальных данных, осуществляется RMS-серверами, установленными в АС.

Необходимо отметить, что для использования технологии RMS на рабочих станциях АС должно быть установлено клиентское ПО с интегрированной поддержкой этой технологии. Так, например, компания Microsoft встроила функции RMS в собственные клиентские программные продукты – Microsoft Office 2003 и Internet Explorer. Технология RMS является открытой и может быть интегрирована в любые программные продукты на основе набора инструментальных средств разработки RMS SDK.

Ниже приводится обобщённый алгоритм использования технология RMS для формирования конфиденциальной информации пользователем «А» и последующего получения к ней доступа пользователем «Б» (рис. 6):

- На первом этапе пользователь «А» загружает с RMS-сервера открытый ключ, который в последствии будет использоваться для шифрования конфиденциальной информации.
- Далее пользователь «А» формирует документ с конфиденциальной информацией при помощи одного из приложений, поддерживающих функции RMS (например, при помощи Microsoft Word 2003). После этого пользователь составляет список субъектов, имеющих права доступа к документу, а также операции, которые они могут выполнять. Эта служебная информация записывается приложением в XML-файл, составленный на основе расширенного языка разметки прав доступа – eXtensible rights Markup Language (XrML).
- На третьем этапе приложение пользователя «А» зашифровывает документ с конфиденциальной информацией при помощи случайным образом сгенерированного симметричного сеансового ключа, который в свою очередь зашифровывается на основе открытого ключа RMS-сервера. С учётом свойств асимметричной криптографии расшифровать этот документ сможет только RMS-сервер, поскольку только он располагает соответствующим секретным ключом. Зашифрованный сеансовый ключ также добавляется к XML-файлу, связанному с документом.
- Пользователь отправляет получателю «Б» зашифрованный документ вместе с XML-файлом, содержащим служебную информацию.
- После получения документа пользователь «Б» открывает его при помощи приложения с функциями RMS.
- Поскольку адресат «Б» не обладает ключом, необходимым для его расшифровки, приложение отправляет запрос к RMS-серверу, в который включается XML-файл и сертификат открытого ключа пользователя «Б».
- Получив запрос, RMS-сервер проверяет права доступа пользователя «Б» к документу в соответствии с информацией, содержащейся в XML-файле. Если пользователю доступ разрешён, то тогда RMS-сервер извлекает из XML-файла зашифрованный сеансовый ключ, дешифрует его на основе своего секретного ключа и заново зашифровывает ключ на основе открытого ключа пользователя «Б». Использование открытого ключа пользователя позволяет гарантировать, что только он сможет расшифровать ключ.
- На восьмом этапе RMS-сервер отправляет пользователю «Б» новый XML-файл, содержащий зашифрованный сеансовый ключ, полученный на предыдущем шаге.
- На последнем этапе приложение пользователя «Б» расшифровывает сеансовый ключ на основе своего закрытого ключа и использует его для открытия документа с конфиденциальной информацией. При этом приложение ограничивает возможные действия пользователя только теми операциями, которые перечислены в XML-файле, сформированном пользователем «А».

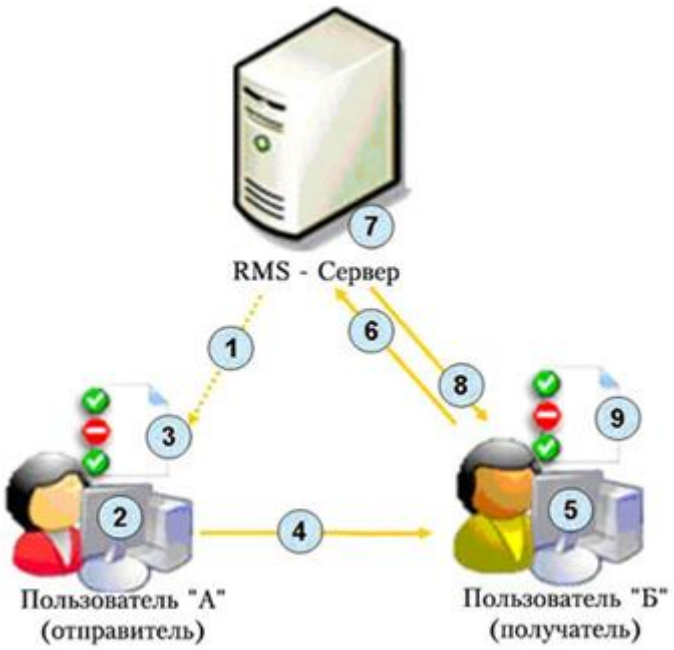


Рис. 6. Схема взаимодействия узлов на основе технологии RMS

В настоящее время технология RMS является одним из наиболее перспективных способов защиты конфиденциальной информации. В качестве недостатка этой технологии необходимо отметить тот факт, что она может быть реализована лишь в рамках платформы Microsoft Windows и только на основе тех приложений, в которых используются функции RMS SDK.

1. 8 Лекция № 8 (2 часа).

Тема: «Средства оценки защищенности информации от утечки по техническим каналам»

1.8.1 Вопросы лекции:

1. Модель канала утечки.
2. Методы достижения условия защищённости.
3. Обзор систем контроля защищенности.

1.8.2 Краткое содержание вопросов:

1. Модель канала утечки.

Предметом защиты информации являются источники информационных физических полей рассеивания, процессы излучения этих полей, их распространения, наводок, локализации, маскирования и извлечения, модели каналов утечки информации (КУИ), методы, алгоритмы, средства оценки (измерения) параметров и характеристик каналов утечки информации, меры защиты информации, информационные параметры и параметры селекций, а также характеристики маскирующих шумов. Разрушение канала утечки речевой информации заключается в снижении ее разборчивости до нормативного значения. Это достигается поддержанием уровня маскирующих шумов. Решение о защите информации принимается на основании простых гипотез H0 и H1. Гипотеза H0 принимается при невозможности восстановления речевой информации. Недоступные наблюдению выходные параметры Yn={y1n, y2n, …, ymn} для каждого канала утечки информации 10 Y1,Y2,…,Yn принадлежат области гипотезы H0, разделенной от альтернативной области гипотезы H1 границей, установленной пороговым значением разборчивости речи. Ее объективность оценивается при слабых сигналах в шумах высокого уровня оперативным и достоверным контролем с высокой точностью. Сущность защиты речевой информации заключается в увеличении в каналах утечки информации маскирующих шумов до уровня пороговой разборчивости речи. При пороговой разборчивости элементы речевого сигнала становятся логически не связанными. Маскирование звука – повышение порога слышимости уха для слабого (маскируемого) звука более сильным (маскирующим) звуком до полного заглушения. В информационной системе требуется измерять параметры и характеристики слабых сигналов в шумах с высокой точностью при большом количестве различных измеряемых физических величин. Средства измерений должны удовлетворять широкому диапазону измерений, повышенной чувствительности и быстродействию представления полученных результатов. Повышение качества исследований основано на средствах измерений, обеспечивающих необходимую

точность. Интеграция средств измерений с элементами вычислительной техники, внедрение их в измерительный процесс решает задачу повышения точности оценки контроля параметров в каналах утечки информации и эффективности защиты информации. Эффективность защиты информации – степень соответствия достигнутых результатов рациональных действий поставленной цели защиты информации. Критерий эффективности – мера успешности, представляемая вероятностью выполнения заданной задачи [4, 5]. Развитие методов и способов защиты информации и повышение эффективности их применения – актуальная задача, решение которой в значительной степени зависит от совершенствования существующей и внедрения более надежной обработки сигналов. Таковыми являются помехоустойчивые способы обработки наблюдаемых процессов. Качество защиты информации определяется степенью доверия к результату ее оценки. Доверие характеризует вероятность того, что определяемые воспроизводимостью измерений параметры и характеристики находятся в пределах, указанных стандартами, требованиями, нормами, чертежами, рекомендациями.

2. Методы достижения условия защищённости.

Современные методики управления рисками, проектирования и сопровождения корпоративных систем защиты информации должны позволять решить ряд задач перспективного стратегического развития компании.

Во-первых, количественно оценить текущий уровень информационной безопасности компании, что потребует выявления рисков на правовом, организационно-управленческом, технологическом, а также техническом уровнях обеспечения защиты информации.

Во-вторых разработать и реализовать комплексный план совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании. Для этого необходимо:

- обосновать и произвести расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности компании, создать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;
- обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными

доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Решение названных задач открывает новые широкие возможности перед должностными лицами разного уровня.

Руководителям верхнего звена это поможет объективно и независимо оценить текущей уровень информационной безопасности компании, обеспечить формирование единой концепции безопасности, рассчитать, согласовать и обосновать необходимые затраты на защиту компании. На основе полученной оценки начальники отделов и служб смогут выработать и обосновать необходимые организационные меры (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях). Менеджеры среднего звена смогут обоснованно выбрать средства защиты информации, а также адаптировать и использовать в своей работе количественные показатели оценки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической эффективности компании.

Практические рекомендации по нейтрализации и локализации выявленных уязвимостей системы, полученные в результате аналитических исследований, помогут в работе над проблемами информационной безопасности на разных уровнях и, что особенно важно, определить основные зоны ответственности, в том числе материальной, за ненадлежащее использование информационных активов компании. При определении масштабов материальной ответственности за ущерб, причиненный работодателю, в том числе разглашением коммерческой тайны, следует руководствоваться положениями гл. 39 Трудового кодекса РФ.

3. Обзор систем контроля защищенности.

Средства анализа защищенности

Арсенал программных средств, используемых для анализа защищенности АС достаточно широк. Причем, во многих случаях, свободно распространяемые программные продукты ничем не уступают их коммерческим аналогам. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами.

Удобным и мощным средством анализа защищенности ОС является рассматриваемый ниже свободно распространяемый программный продукт CIS Windows 2000 Level I Scoring Tool, а также аналогичные средства разработчиков ОС, предоставляемые бесплатно, такие как ASET для ОС Solaris или MBSA (Microsoft Security Baseline Analyzer) для ОС Windows 2000.

Одним из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности АС. Управление агентами осуществляет по сети программой менеджером. Менеджеры являются центральными компонентом подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все

данные полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был использован при построении комплексной системы управления безопасностью организации Symantec ESM.

Другим широко используемым методом анализа защищенности является активное тестирование механизмов защиты путем эмуляции действий злоумышленника по осуществлению попыток сетевого вторжения в АС. Для этих целей применяются сетевые сканеры, эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак). Рассматриваемые ниже сетевые сканеры Nessus и Symantec NetRecon являются достойными представителями данного класса программных средств анализа защищенности.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки и на практике взаимно дополняют друг друга.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому, в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего агента (своего для каждой ОС).

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, в общем случае, трудно отличить сеанс сканирования от действительных попыток осуществления атак. Сетевыми сканерами также с успехом пользуются злоумышленники.

Системы анализа защищенности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства лучше применять совместно. Кроме того, сканеры являются более простым, доступным, дешевым и, во многих случаях, более эффективным средством анализа защищенности.

Средства анализа параметров защиты (Security Benchmarks)
Уровень защищенности компьютерных систем от угроз безопасности определяется многими факторами. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного ПО, средств защиты информации и активного сетевого оборудования существующим рискам. Перечисленные компоненты АС имеют сотни параметров, значения которых оказывают влияние на защищенности системы, что делает их ручной анализ трудновыполнимой задачей. Поэтому в современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации зачастую используются специализированные программные средства.

Анализ параметров защиты осуществляется по шаблонам, содержащим списки параметров и их значений, которые должны быть установлены для обеспечения необходимого уровня защищенности. Различные шаблоны, определяют конфигурации для различных программно-технических средств.

Относительно коммерческих корпоративных сетей, подключенных к сети Интернет, можно говорить о некотором базовом уровне защищенности, который в большинстве случаев можно признать достаточным. Разработка спецификаций (шаблонов) для конфигурации наиболее распространенных системных программных средств, позволяющих обеспечить базовых уровень защищенности, в настоящее время осуществляется представителями международного сообщества в лице организаций и частных лиц, профессионально занимающихся вопросами информационной безопасности и аудита АС, под эгидой международной организации Центр Безопасности Интернет (Center of Internet Security). На данный момент закончены, либо находятся в разработке следующие спецификации (Security Benchmarks):

- Solaris (Level-1)
- Windows 2000 (Level-1)
- CISCO IOS Router (Level-1/Level-2)
- Linux (Level-1)
- HP-UX (Level-1)
- AIX (Level-1)
- Check Point FW-1/VPN-1 (Level-2)
- Apache Web Server (Level-2)
- Windows NT (Level-1)
- Windows 2000 Bastion Host (Level-2)
- Windows 2000 Workstation (Level-2)
- Windows IIS5 Web Server (Level-2)

В приведенном списке спецификации первого уровня (Level-1) определяют базовый (минимальный) уровень защиты, который требуется обеспечить для большинства систем, имеющих подключения к Интернет. Спецификации второго уровня (Level-2) определяют продвинутый уровень защиты, необходимый для систем, в которых предъявляются повышенные требования по безопасности.

Перечисленные спецификации являются результатом обобщения мирового опыта обеспечения информационной безопасности.

Для анализа конфигурации компонентов АС на соответствие этим спецификациям используются специализированные тестовые программные средства (CIS-certified scoring tools).

В качестве примера, рассмотрим спецификацию базового уровня защиты для ОС MS Windows 2000 и соответствующий программный инструментарий для анализа конфигурации ОС.

Windows 2000 Security Benchmark
CIS Windows 2000 Security Benchmark является программой, позволяющей осуществлять проверку соответствия настроек ОС MS Windows 2000 минимальному набору требований безопасности, определяющих базовый уровень защищенности, который, в общем случае, является достаточным для коммерческих систем. Требования к базовому уровню защищенности ОС Windows 2000 были выработаны в результате обобщения практического опыта. Свой вклад в разработку этих спецификаций внесли такие организации, как SANS Institute, Center for Internet Security, US NSA и US DoD.

В состав инструментария CIS Windows 2000 Security Benchmark входит шаблон политики безопасности (cis.inf), позволяющий осуществлять сравнение текущих настроек ОС с эталонными и производить автоматическую переконфигурацию ОС для обеспечения соответствия базовому уровню защищенности, задаваемому данным шаблоном.

CIS Windows 2000 Security Benchmark позволяет осуществлять количественную оценку текущего уровня защищенности анализируемой ОС по 10-бальной шкале. Уровень 0 соответствует минимальному уровню защищенности (после установки ОС, ее уровень защищенности как раз и будет равен 0). Уровень 10 является максимальным и означает полное соответствие анализируемой системы требованиям базового уровня защищенности для коммерческих систем.

Рисунок 3. Windows 2000 Level 1 Security Scoring Tool

Все проверки, выполняемые при анализе системы, делятся на 3 категории:

1. Service Packs and Hotfixes (Пакеты обновлений и программные коррекции)

2. Account and Audit Policies (Политика управления пользовательскими бюджетами и политика аудита безопасности)

3. Security Options (Опции безопасности)

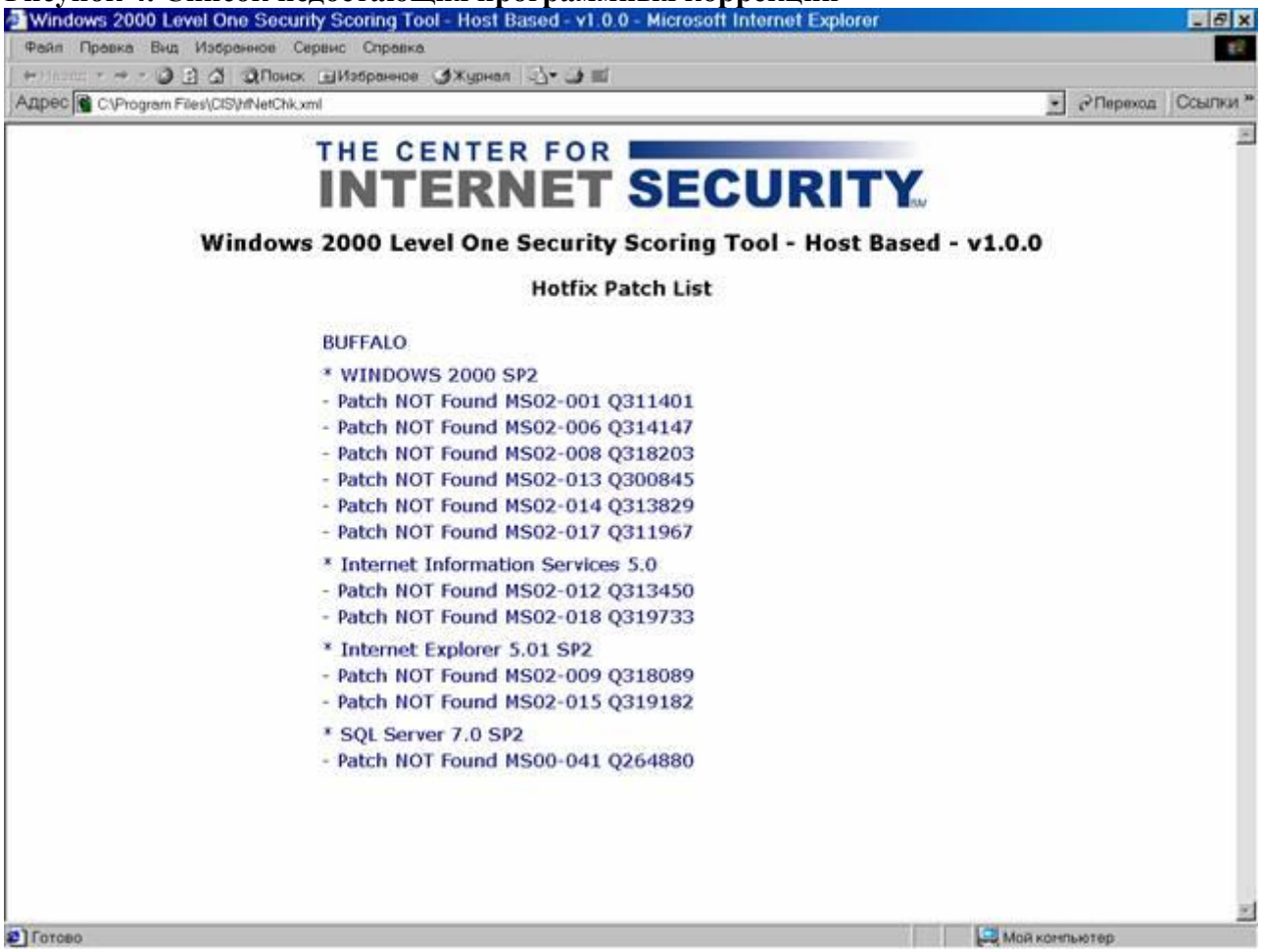
Первая категория включает проверку установки последних пакетов обновлений (Service Packs) и текущих программных коррекций (Hotfixes) от Microsoft.

Вторая категория включает проверки параметров политики безопасности по управлению пользовательскими бюджетами (включая политику управления паролями) и осуществлению аудита безопасности.

Третья категория включает проверки всех остальных параметров безопасности ОС, не относящиеся к первым двум категориям, включая запрет анонимных сессий (NULL sessions), правила выделения внешних устройств, параметры защиты протокола TCP/IP, установки прав доступа к системным объектам и т.п.

Для проверки наличия установленных текущих программных коррекций используется утилита MS Network Security Hotfix Checker (HFNetCheck), которая автоматически скачивается с сайта Microsoft и устанавливается во время осуществления проверок. Подробную информацию об этой утилите можно получить по адресу: http://www.microsoft.com/technet/...
Используя список недостающих программных коррекций (Hotfixes), сгенерированный утилитой HFNetCheck, следует осуществить поиск и установку этих коррекций. Для этого используется Microsoft Security Bulletin Search Web-сайт: http://www.microsoft.com/technet/...

Рисунок 4. Список недостающих программных коррекций



Для осуществления мониторинга установки необходимых программных коррекций, помимо утилит Microsoft, можно использовать более мощные средства третьих фирм, например программу UpdateExpert, разработки St. Bernard Software (www.stbernard.com). Для настройки ОС с использованием шаблона CIS.INF используется Security Configuration and Analysis Snap-In – стандартное средство ОС Windows 2000 для осуществления анализа и настройки параметров безопасности ОС.

Порядок подключения данного средства к MMC (Microsoft Management Console), загрузки шаблона, его использования для анализа и изменения конфигурации ОС описывается в «CIS Win2K Level 1 Implementation Guide», входящем в комплект программной документации, которая содержит также подробное описание всех производимых проверок и соответствующих параметров настройки ОС.

Сетевые сканеры

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования

заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора, либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers) использовавшиеся с начала 80-х и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

- идентификация доступных сетевых ресурсов
- идентификация доступных сетевых сервисов
- идентификация имеющихся уязвимостей сетевых сервисов
- выдача рекомендаций по устранению уязвимостей

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время, существует большое количество как коммерческих, так и свободно распространяемых сканеров, как универсальных, так и специализированных - предназначенных для выявления только определенного класса уязвимостей. Многие из них можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров медленно но уверенно приближается к 1000.

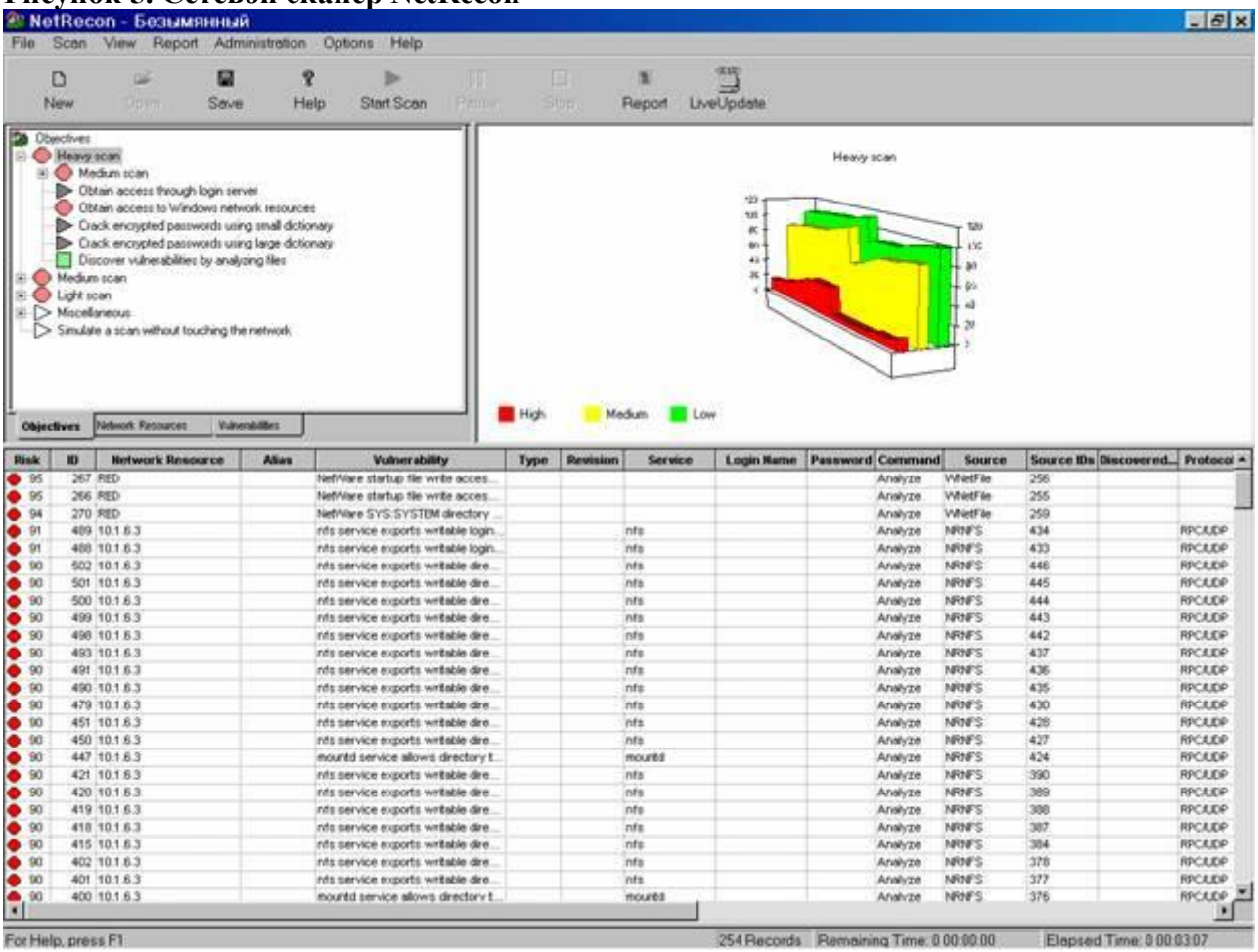
Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база данных которого содержит около 800 уязвимостей UNIX, Windows и NetWare систем и постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление обо всех продуктах этого класса.

Сетевой сканер NetRecon

Сетевой сканер NetRecon является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентов. Например, NetRecon позволяет находить уязвимости в таких сетевых сервисах, как ftp, telnet, DNS,

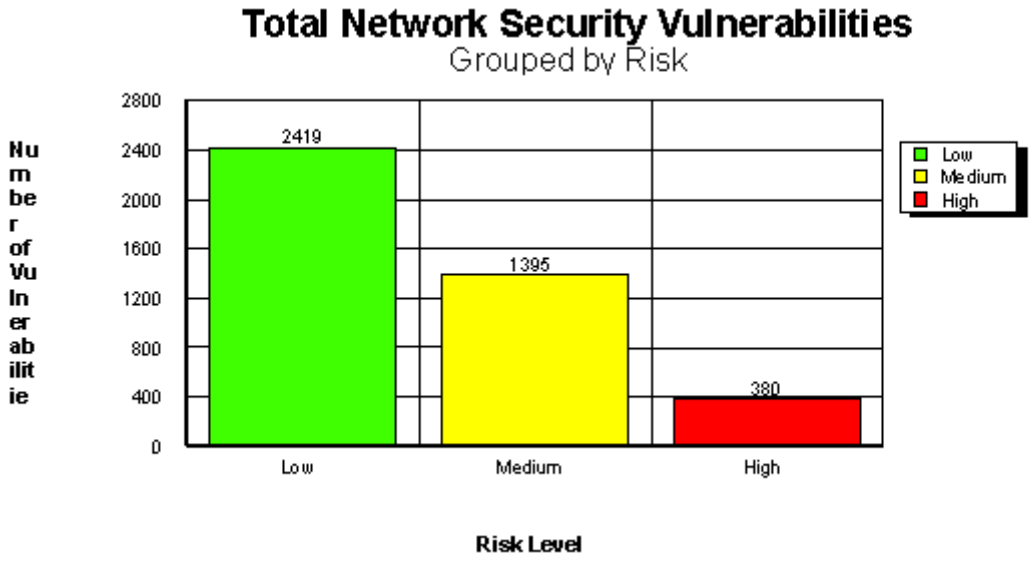
электронная почта, Web-сервер и др. При этом проверяются версии и конфигурации сервисов, их защищенность от сетевых угроз и устойчивость к попыткам проникновения. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.

Рисунок 5. Сетевой сканер NetRecon



Программа работает в среде ОС Windows NT и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и в табличной форме в реальном масштабе времени.

Рисунок 6. Суммарное количество уязвимостей, обнаруженных сканером NetRecon



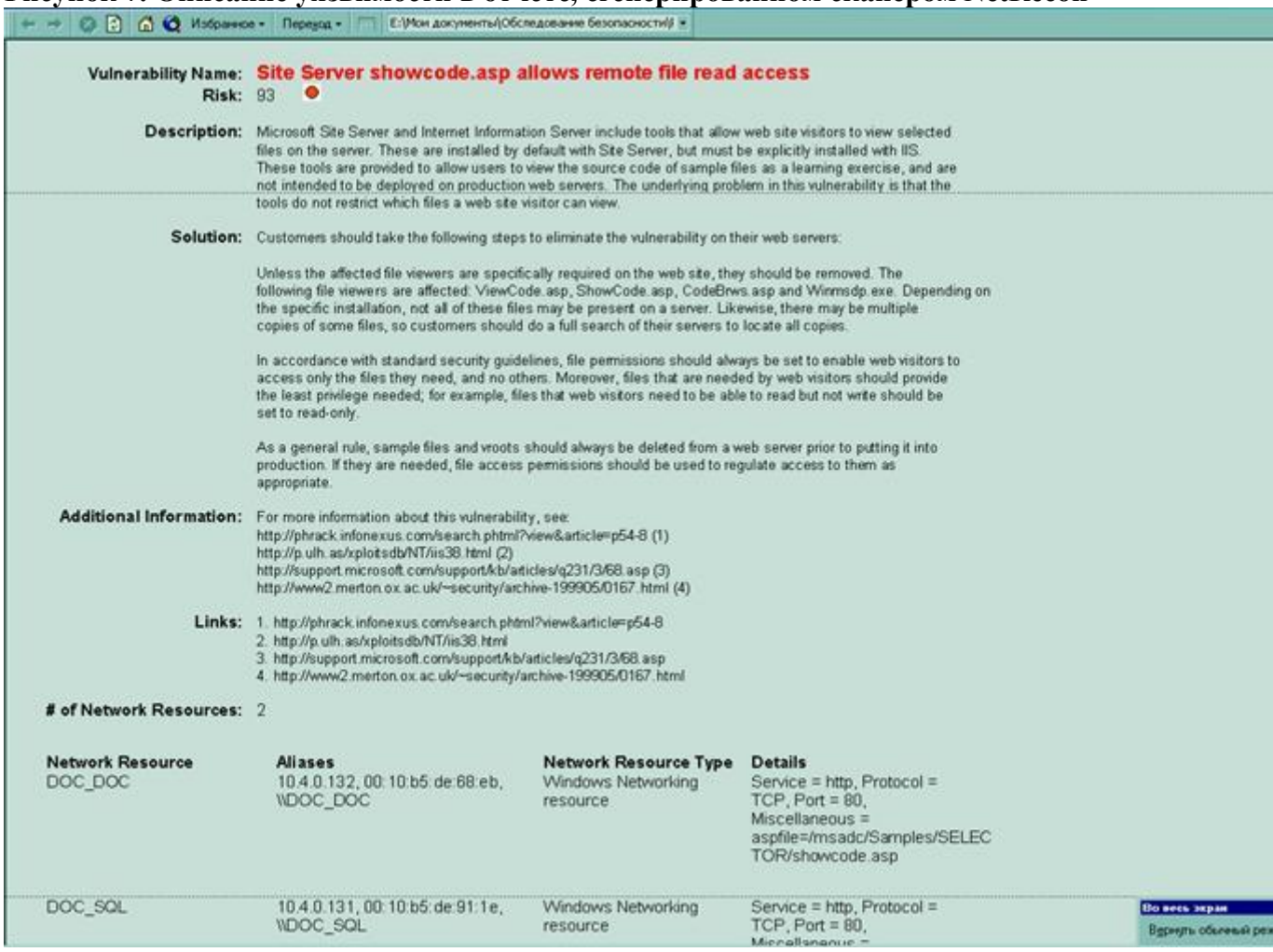
Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей, подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и многие другие. Наряду с сообщениями о найденных уязвимостях и их описаниями, приводятся рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

Для генерации отчетов в NetRecon используется ПО Crystal Report, предоставляющее удобные средства для просмотра отчетов и их экспорта во все популярные форматы представления данных. Найденные уязвимости ранжируются, при этом каждой из них присваивается числовой рейтинг, что позволяет отсортировать их по степени критичности для облегчения последующего анализа результатов сканирования.

Пример описания уязвимости в отчете, сгенерированном сканером NetRecon, приведен на Рисунок 7. В NetRecon используется следующий формат описания уязвимости (который однако является общим и для всех остальных сетевых сканеров):

- Vulnerability Name (Название уязвимости)
- Risk (Уровень риска)
- Description (Описание уязвимости)
- Solution (Способы ликвидации уязвимости)
- Additional Information (Дополнительная информация)
- Links (Ссылки на источники информации о данной уязвимости)
- # of Network Resources (Кол-во сетевых ресурсов, подверженных данной уязвимости)
- Network Resource (Список сетевых ресурсов)

Рисунок 7. Описание уязвимости в отчете, сгенерированном сканером NetRecon



NetRecon самостоятельно определяет конфигурацию сети и позволяет выбрать сетевые ресурсы для сканирования. Может осуществляться параллельное сканирование всех сетевых ресурсов, сканирование по диапазону сетевых адресов, сканирование отдельных систем или подсетей. Сеанс сканирования может включать в себя все виды проверок, либо отдельные проверки по выбору пользователя. Глубина сканирования определяется продолжительностью сеанса сканирования, которая задается пользователем. Например, проверки, связанные с подбором пользовательских паролей по словарю, сопряжены с существенными временными затратами и не могут быть завершены в течение короткого сеанса сканирования.

Для поиска сетевых уязвимостей в NetRecon используется запатентованная технология UltraScan. Производимые NetRecon проверки тесно взаимосвязаны и результаты одной проверки используются для выполнения другой. Как и в случае реальных атак, в технологии UltraScan, информация об обнаруженных уязвимостях используется для выявления других связанных с ними уязвимостей. Например, если NetRecon удалось получить доступ к файлу, содержащему пароли пользователей, и расшифровать несколько паролей, то эти пароли будут использованы для имитации атак на другие системы, входящие в состав сети.

NetRecon позволяет пользователю отслеживать путь поиска уязвимости, представляющий собой последовательность проверок, производимых NetRecon, которая привела к выявлению данной уязвимости. Путь поиска уязвимости позволяет проследить действия возможного нарушителя, осуществляющего атаку на сетевые ресурсы.

Используемая NetRecon база данных содержит описание известных уязвимостей и сценариев атак. Она регулярно пополняется новыми данными. Обновление этой базы данных производится через Web-узел компании Symantec автоматически, при помощи механизма LiveUpdate.

Сетевой сканер NESSUS

Сетевой сканер Nessus может рассматриваться в качестве достойной альтернативы коммерческим сканерам. Nessus является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс позволяет определять параметры сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты.

По своим функциональным возможностям сканер защищенности Nessus находится в одном ряду, а по некоторым параметрам и превосходит такие широко известные коммерческие сканеры, как NetRecon компании Symantec, Internet Scanner компании ISS и CyberCop Scanner компании NAI.

Версии 0.99 серверной части сканера Nessus была сертифицирована в Гостехкомиссии России (Сертификат N 361 от 18 сентября 2000 г.).

Сценарии атак реализованы в NESSUS в качестве подключаемых модулей (plugins). Количество подключаемых модулей постоянно увеличивается, в настоящее время насчитывается более 700. Новые внешние модули, эмулирующие атаки, можно инсталлировать, скопировав файлы, содержащие их исходные тексты, с web-сервера разработчиков www.nessus.org.

Nessus предоставляет очень широкие возможности по поиску уязвимостей корпоративных сетей и исследованию структуры сетевых сервисов. Помимо использования стандартных способов сканирования TCP и UDP портов, Nessus позволяет осуществлять поиск уязвимостей в реализациях протоколов управления сетью ICMP и SNMP. Кроме того, поддерживаются различные стелс-режимы сканирования, реализуемые популярным некоммерческим стелс-сканером nmap, который можно рассматривать в качестве одного из компонентов сканера Nessus. Другой популярный некоммерческий сканер queso используется в составе Nessus для определения типа и номера версии сканируемой ОС.

Высокая скорость сканирования достигается за счет использования при реализации сканера Nessus многопотоковой архитектуры программирования, позволяющей осуществлять одновременное параллельное сканирование сетевых хостов. Для сканирования каждого хоста сервером nessusd создается отдельный поток выполнения.

Подробное описание используемых методов сканирования TCP/UDP портов можно найти в онлайновой документации на сканер nmap. Они включают в себя следующее:

- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- TCP Xmas Tree scan
- TCP Null scan
- UDP scan

При реализации Nessus использована нетипичная для сетевых сканеров клиент/серверная архитектура. Взаимодействие между клиентом и сервером осуществляется по защищенному клиент-серверному протоколу, предусматривающему использование надежной схемы аутентификации и шифрование передаваемых данных. Сервер nessusd, работает только в среде UNIX и предназначен для выполнения сценариев сканирования. Механизмы собственной безопасности, реализованные в сервере nessusd позволяют осуществлять аутентификацию пользователей сканера, ограничивать полномочия пользователей по выполнению сканирования и регистрировать все действия пользователей в журнале регистрации событий на сервере.

Клиентская часть Nessus работает и в среде UNIX и в среде Windows и реализует графический интерфейс пользователя для управления сервером nessusd. Пользователь сканера, перед запуском сеанса сканирования, определяет параметры сканирования, указывая диапазон сканируемых IP-адресов и TCP/UDP портов, максимальное количество потоков сканирования (число одновременно сканируемых хостов), методы и сценарии сканирования (plugins), которые будут использоваться.

Все сценарии сканирования разделены на группы по типам реализуемых ими сетевых атак (Рисунок 8), обнаруживаемых уязвимостей, а также по видам тестируемых сетевых сервисов. Так, имеется специальная группа сценариев Backdoors для обнаружения троянских программ, Gain Shell Remotely - для реализации атак на получение пользовательских полномочий на удаленной UNIX системе, Firewalls – для тестирования МЭ, FTP – для тестирования FTP-серверов, Windows – для поиска уязвимостей Windows-систем и т.п.

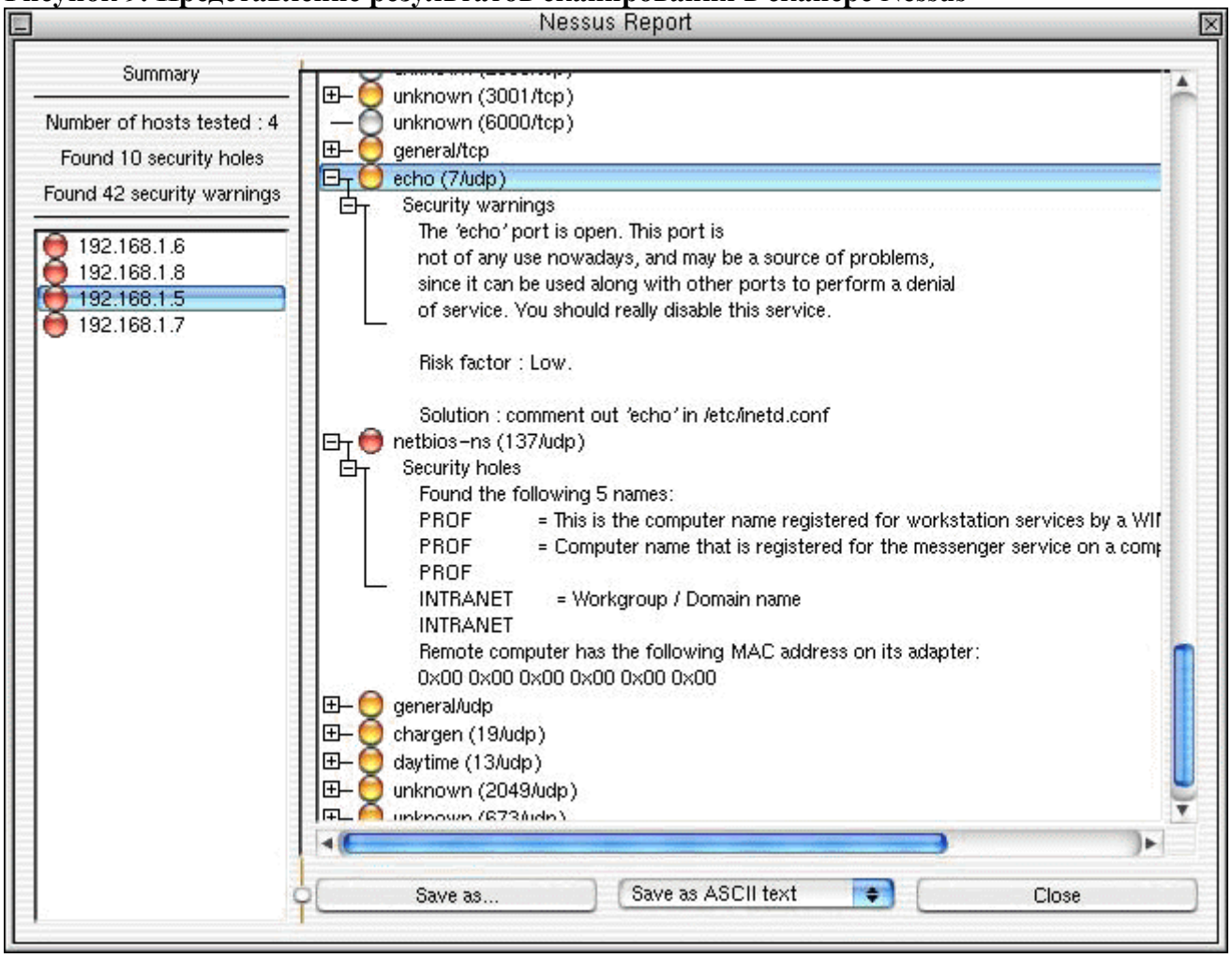
Особую группу сценариев сканирования Denail of Service составляют атаки на отказ в обслуживании (DoS). Единственный способ убедиться в том, что сканируемая система подвержена той или иной DoS – это выполнить эту атаку и посмотреть на реакцию системы. Эта группа сценариев, однако, является потенциально опасной, т.к. их запуск может привести к непредсказуемым последствиям для сканируемой сети, включая сбои в работе серверов и рабочих станций, потерю данных и «полный паралич» корпоративной сети. Поэтому большинство DoS в данной группе по умолчанию отключено.

Для написания сценариев атак служит специализированный C-подобный язык программирования высокого уровня NASL (Nessus Attack Scripting Language). Существует также интерфейс прикладного программирования (API) для разработки подключаемых модулей со сценариями атак на языке C, однако предпочтительным является все же использование NASL.

NASL является интерпретируемым языком программирования, что обеспечивает его независимость от платформы. Он предоставляет мощные средства для реализации любых сценариев сетевого взаимодействия, требующих формирования IP-пакетов произвольного вида.

Результаты работы сканера Nessus представлены на Рисунок 9. Данные об обнаруженных уязвимостях отсортированы по IP-адресам просканированных хостов. Найденные уязвимости проранжированы. Наиболее критичные (security holes) выделены красным цветом, менее критичные (security warning) – желтым. По каждой уязвимости приводится ее описание, оценка ассоциированного с ней риска (Risk Factor) и рекомендации по ее ликвидации (Solution).

Рисунок 9. Представление результатов сканирования в сканере Nessus



Средства контроля защищенности системного уровня

Обеспечение безопасности компьютерных систем, по существу, заключается в определении множества возможных угроз, оценке величины связанных с ними рисков, выборе адекватных контрмер, реализации этих контрмер процедурными и программно-техническими средствами и контроле их осуществления. Последний вопрос является, пожалуй, одним из наиболее сложных. Реализация программно-технических мер защиты требует произведения настроек большого количества параметров ОС, МЭ, СУБД, сетевых сервисов, прикладных программ и активного сетевого оборудования. Когда речь идет о защите отдельного сервера или рабочей станции, то задача хоть и является сложной, но ее решение вполне по силам опытному системному администратору. В этом случае для контроля значений параметров программ, связанных с безопасностью, используются специальные списки проверки. Когда же речь заходит о настройке десятков и сотен сетевых устройств, функционирующих на различных программно-аппаратных платформах, в соответствии с единой политикой безопасности, контроле параметров защиты и мониторинге безопасности в реальном масштабе времени, то без специальных средств автоматизации уже не обойтись. Производители ОС предоставляют специальный инструментарий для контроля целостности и анализа защищенности ОС (утилита C2 Configuration в Windows NT Resource Kit, утилита ASET в ОС Solaris и т.п.). Имеется немало свободно распространяемых и широко используемых продуктов, предназначенных для решения подобных задач, таких как программа COPS для ОС UNIX. Однако эти средства, функционирующие на системном уровне, позволяют обеспечить только некоторый базовый уровень защищенности самой ОС. Для контроля приложений, сетевых сервисов, активного сетевого оборудования в распределенных системах, функционирующих в динамичной агрессивной среде необходимо использовать

специализированный инструментарий, поддерживающий распределенные архитектуры, централизованное управление, различные программно-аппаратные платформы, различные виды приложений, использующий изощренные алгоритмы поиска и устранения уязвимостей, интегрированный с другими средствами защиты и удовлетворяющий многим другим требованиями, предъявляемым к современным продуктам этого класса.

Автоматизированная система управления безопасностью предприятия Enterprise Security Manager

Мощным средством анализа защищенности системного уровня, выполняющим проверки конфигурационных параметров ОС и приложений «изнутри» является автоматизированная система управления безопасностью предприятия ESM компании Symantec. Программные агенты ESM устанавливаются на каждом контролируемом компьютере сети, выполняя проверки параметров ПО, связанных с безопасностью и корректируя их по мере необходимости. Программные агенты обычно способны выполнять более сложные проверки и анализировать параметры ПО, недоступные сетевым сканерам, т. к. они действуют изнутри. Анализ защищенности, выполняемый программными агентами, может планироваться по времени и выполняться одновременно на всех контролируемых компьютерах. Кроме того, в отличие от сетевых сканеров, программные агенты не оказывают большого влияния на пропускную способность сети и осуществляют шифрование результатов проверок при передаче данных по сети.

Архитектура ESM

Система ESM построена на архитектуре консоль/менеджер/агент. Она стоит из трех типов компонентов, которые могут быть распределены по сети произвольным образом: административной консоли (ESM Console), менеджеров (ESM Manager) и агентов (ESM Agent).

Консоль ESM

Административная консоль представляет собой графический пользовательский интерфейс для управления менеджерами и функционирует в среде Windows NT. Для управления менеджерами может также использоваться интерфейс командной строки (CLI).

Административная консоль используется для выполнения следующих задач:

- управление регистрационными записями пользователей на ESM-менеджере
- определение пользовательских полномочий в системе ESM
- сбор и анализ информации о состоянии сети от ESM-менеджеров
- ранжирование уязвимостей и определение уровней защищенности контролируемых систем
- создание и изменение политик безопасности
- активизация политик безопасности на контролируемых доменах
- установка расписание выполнения проверок
- отображение результатов выполнения проверок в табличной и графической формах
- генерация и просмотр отчетов по результатам выполняемых проверок

- коррекция некоторых параметров ОС

Менеджер ESM

Центральным компонентом системы является ESM-менеджер. Он выполняет две основные функции:

- хранит данные о политиках безопасности и осуществляет управление этими данными, а также передает эти данные агентам и административной консоли

- осуществляет управление данными о результатах выполненных проверок, получает эти данные от ESM-агентов и передает их на административную консоль

Основным компонентом менеджера является сервер управления данными - CIF-сервер. Все данные о пользователях ESM, полномочиях, агентах, доменах, политиках безопасности, результатах проверок и шаблонах, а также сообщения от агентов хранятся в файлах управляющей информации (Control Information Files). CIF-сервер управляет доступом к CIF-файлам. Он предоставляет необходимую информацию по запросам административной консоли и интерфейса командной строки. CIF-сервер также перенаправляет запросы на выполнение другим компонентам менеджера. Например, сообщает менеджеру задач (Job Starter) о необходимости активизировать выполнение политики безопасности на домене. Сетевой сервер (Net Server) являет еще одним компонентом менеджера, обеспечивающим связь CIF-сервера и других компонентов с удаленными агентами. Связь между распределенными компонентами ESM осуществляется по защищенному клиент-серверному протоколу ESM's Client Server Protocol (CSP) прикладного уровня, реализованному поверх сетевых протоколов TCP/IP и SPX/IPX. Защита трафика между менеджерами и агентами от прослушивания осуществляется шифрованием по алгоритму DESX, являющегося усовершенствованной версией американского стандарта шифрования DES.

Агенты ESM

Агенты ESM также как и менеджеры имеют модульную структуру. Они включают в себя серверную часть, модули безопасности и средства коммуникаций. Они собирают информацию о безопасности системы. Сбор и анализ информации начинается с момента получения указания от менеджера на активизацию политики безопасности. Серверный компонент агента собирает данные о результатах проверок от модулей безопасности и посылает их менеджеру. Агенты выполняют также ряд других важных функций:

- сохраняют мгновенные снимки, содержащие данные о состоянии системы и пользовательских бюджетах

- осуществляют обновление мгновенных снимков состояния системы

- осуществляют коррекцию некоторых параметров системы по запросам пользователя

Политики безопасности ESM

Политика безопасности ESM представляет собой совокупность модулей безопасности. ESM содержит набор предопределенных политик безопасности, предназначенных для обеспечения различных уровней защищенности. Политика безопасности предприятия реализуется на основе предопределенных политик ESM путем настройки модулей безопасности с целью изменения количества и содержания выполняемых ими проверок.

Доменная организация агентов позволяет распространить действие политик безопасности на отдельные системы, группы систем и предприятие в целом.

Политика безопасности задает набор правил, которым должны соответствовать контролируемые системы. ESM осуществляет анализ защищенности систем путем сравнения значений их конфигурационных параметров с теми, которые заданы в политике безопасности. ESM осуществляет ранжирование результатов проверок по степени критичности и определяет общий уровень защищенности системы, суммируя числовые рейтинги обнаруженных уязвимостей.

Задачу начального конфигурирования ESM существенно облегчает наличие предопределенных политик безопасности, перечисленных ниже в порядке увеличения строгости и глубины проверок:

- Phase 1
- Phase 2
- Phase 3:a Relaxed
- Phase 3:b Cautious
- Phase 3:c Strict

Политика первого уровня (Phase 1) включает в себя модули безопасности, предназначенные для проверки наиболее существенных и потенциально опасных видов уязвимостей, устранение которых позволяет обеспечить минимально необходимый для большинства систем уровень защищенности.

Политика второго уровня (Phase 2) включает в себя все имеющиеся в ESM модули безопасности, в которых однако активизированы только ключевые виды проверок, являющиеся наиболее важными.

Политики третьего уровня (Phase 3) включают в себя:

- базовую версию, идентичную политике второго уровня (Relaxed);
- усиленную версию, содержащую дополнительные виды проверок (Cautious);
- строгую версию, включающую все виды проверок во всех модулях безопасности поддерживаемых для данной ОС (Strict).

Помимо перечисленных в ESM имеется еще несколько специализированных политик безопасности. Предопределенная политика Queries включает в себя только информационные модули, предоставляющие информацию о пользователях, группах и системах на которых не установлены ESM и ITA агенты. Она разработана для платформ NetWare и Windows NT.

Специальная политика NetRecon используется для интеграции со сканером NetRecon на платформе Windows NT, позволяя просматривать и анализировать результаты сканирования сканером NetRecon средствами ESM консоли. Она осуществляет преобразование записей об уязвимостях, сгенерированных сканером NetRecon, в формат сообщений ESM.

Контроль защищенности корпоративной сети при помощи ESM обычно производится путем постепенного ужесточения требований безопасности, предъявляемых к информационной системе. Начинать следует с активизации политик первого и второго уровня на контролируемых системах. Для большинства коммерческих систем такой уровень защищенности является вполне приемлемым. В случае успешного завершения всех проверок на особо критичных системах можно активизировать политики безопасности третьего уровня, которые позволяют осуществлять наиболее глубокий анализ параметров защиты.

Имеется возможность на основе предопределенных политик создавать свои собственные, которые наилучшим образом соответствуют требованиям организации. Для создания политик безопасности в составе ESM имеется графический инструментарий, полностью исключающий какое-либо программирование.

Модули ESM

Модули ESM агентов – это программные модули, осуществляющие проверки, предписываемые политикой безопасности. Имеется две разновидности модулей ESM: модули безопасности и модули запросов. Модули безопасности контролируют различные области безопасности, включая управление пользовательскими бюджетами и параметрами авторизации, настройку сетевых параметров и параметров сервера, атрибуты файловых систем и каталогов. Модули запросов предназначены для сбора информации о состоянии системы. Например, получение списка пользователей, входящих в определенную группу, либо пользователей, наделенных административными полномочиями.

Модули запросов (информационные модули)

Информационные модули служат для сбора информации о различных параметрах системы, существенных при выполнении задач администрирования безопасности. В следующей таблице приводится описание некоторых информационных модулей.

Таблица 1. Информационные модули ESM

Account Information	Данный модуль служит для получения информации о регистрационных записях пользователей ОС. В Windows NT он возвращает информацию о полномочиях пользователей, список пользователей с права администратора, список заблокированных и отключенных регистрационных записей пользователей, список групп и списки пользователей, входящих в каждую группу. В ОС NetWare модуль возвращает список групп и списки пользователей, входящих в каждую группу, эквиваленты безопасности, эффективные права доступа, отношения доверия и т. п.
Discovery	Данный модуль осуществляет сканирование TCP-портов, с целью определения которые из низ активны, пытается идентифицировать сетевые ресурсы и составляет список хостов, которые не находятся под контролем программных агентов ESM и ITA.
File Information	Возвращает список параметров доступа к файлам, специфичных для ОС NetWare.

Модули безопасности

Модули безопасности выполняют наборы проверок с целью поиска уязвимостей в ОС и приложениях, попадающих в одну из трех областей:

- Идентификация, аутентификация и авторизация пользователей при входе в систему, управление паролями и пользовательскими бюджетами;
- Конфигурация сетевых протоколов и сервисов;
- Управление доступом к файлам и каталогам.

Пользователь имеет возможность выбора из набора проверок, доступных внутри данного модуля. Каждая проверка осуществляет поиск некоторого типа уязвимостей. Например, проверки, входящие в состав модуля Login Parameters проверяют систему на наличие неактивных пользователей, зарегистрированных в системе, на наличие паролей с истекшим сроком действия и установку ограничения на количество неудачных попыток входа в систему.

(Одни модули безопасности используются только для проверки параметров определенных ОС и приложений, другие – более универсальные и охватывают несколько ОС). В следующей таблице приводится описание основных модулей безопасности.

Таблица 2. Модули безопасности ESM

Модуль безопасности	Описание
Account Integrity	Проверяются привилегии пользователей, политика управления паролями и регистрационными записями пользователей.
Backup Integrity	Проверяются параметры подсистемы резервного копирования, выявляются файлы, для которых не были созданы резервные копии.
File Access	Проверяется соответствие прав доступа к файлам установленным правилам политики безопасности.
File Attributes	Осуществляется контроль целостности атрибутов файлов данных.
File Find	Проверка целостности файлов и контроль файлов на наличие вирусов.
Login Parameters	Проверяются параметры регистрации в системе на соответствие установленным правилам политики безопасности.
Object Integrity	Контролируются изменения прав владения, прав доступа и других атрибутов исполняемых файлов.
Password Strength	Проверяется соответствие паролей пользователей установленным правилам политики управления паролями. Выявляются «слабые» пароли, а также их отсутствие.
Startup Files	Проверяются командные файлы, исполняемые при загрузке системы, на наличие в них уязвимостей.
System Auditing	Проверка параметров подсистемы аудита и осуществление мониторинга журналов аудита Windows NT.

System Mail	Проверка конфигурационных параметров системы электронной почты, связанных с безопасностью.
System Queues	Проверяются параметры настройки очередей системных утилит cron, batch и at ОС UNIX, а также параметры подсистемы спулинга ОС OpenVMS.
User Files	Проверка прав владения и прав доступа к файлам пользователей.
Registry	Проверка прав доступа и атрибутов ключей реестра ОС Windows NT.
Network Vulnerabilies	Осуществляется анализ уязвимостей настроек сетевых параметров Windows NT, обнаруженных сетевым сканером NetRecon.

С целью упрощения задачи управления безопасностью при помощи ESM, все агенты ESM объединяются в домены. Доменом ESM называется группа агентов, объединенных по определенному признаку. Это позволяет активизировать политику безопасности одновременно на всех агентах, входящих в домен. По умолчанию все агенты объединены в домены по типу операционной системы. Таким образом, изначально существует Windows NT домен, UNIX домен, NetWare домен и OpenVMS домен. Доменная организация может также отражать организационную или территориальную структуру предприятия.

В ходе осуществления проверок ESM выполняет поиск нарушений политики безопасности. Нарушения политики безопасности могут быть двух типов:

- несоответствие правилам политики безопасности;
- несоответствие текущего состояния системы последнему мгновенному снимку, сохраненному в ходе проведения предыдущих проверок.

Мгновенные снимки состояния системы

Мгновенные снимки используются ESM для осуществления контроля целостности программной и информационной частей ОС и приложений, и для отслеживания изменений в конфигурации системы. Мгновенные снимки содержат значения атрибутов объектов, специфичные для данной системы, такие как времена создания и модификации, контрольные суммы и права доступа к файлам, привилегии пользователей и т. п. Файлы, содержащие мгновенные снимки, создаются при первом запуске политики безопасности на контролируемой системе. В ходе последующих запусков состояние системы сравнивается с мгновенными снимками предыдущих состояний и все различия, обнаруженные в параметрах конфигурации и атрибутах системных объектов, рассматриваются в качестве потенциальных уязвимостей. Состояния объектов сравниваются с мгновенными снимками и сообщения обо всех отличиях посылаются Менеджеру, где они записываются в базу данных безопасности.

Каждый агент ESM создает несколько файлов мгновенных снимков под названиями: File, User, Group, Device и т. п. Файлы User, Group и Device содержат информацию о состоянии соответствующих системных объектов. Файл User содержит данные пользовательских бюджетов, включающие пользовательские полномочия и привилегии. Файл Group содержит данные о группах пользователей, включая полномочия и привилегии для группы, а также список членов группы. Файл Device содержит имена владельцев, права доступа и атрибуты устройств.

В отличие от других файлов мгновенных снимков File используется для сравнения со специальными шаблонами с целью обнаружения подозрительных изменений фалов, вирусов и троянских коней.

Специализированные модули безопасности, дополнительно устанавливаемые на агентов Oracle modules, Web modules и т. п.), могут использовать собственные виды мгновенных снимков.

Шаблоны ESM
Шаблоны используются для выявления несоответствий конфигурации системы правилам политики безопасности. Они представляют собой списки системных объектов и их состояний. Так модуль File Attributes проверяет атрибуты системных файлов ОС Windows 2000 Professional по шаблону (fileatt.w50), а модуль OS Patches проверяет по шаблону (patch.pw5) наличие установленных программных коррекций для ОС.

Файлы шаблонов хранятся на Менеджере. При запуске политики модули безопасности определяют по шаблонам объекты и атрибуты объектов, которые будут проверяться.

Основные возможности и характеристики

ESM лучше многих других конкурирующих продуктов подходит для использования в крупных и быстрорастущих сетях, так как обладает хорошими характеристиками масштабируемости. Управляющая консоль ESM 5.0 способна поддерживать до 40 менеджеров и до 10000 агентов. ESM-менеджер на процессоре Pentium 120 MHz или SPARC 276 MHz способен поддерживать до 400 агентов. Управляющая консоль функционирует в различных графических средах, включая X-Window, Windows 3.x, Windows 95/98/NT.

В настоящее время ESM осуществляет более 1000 проверок параметров настройки ОС и приложений. Поддерживается 55 различных продуктов в том числе: ОС, маршрутизаторы, МЭ, Web-серверы, СУБД Oracle и Lotus Notes. Среди поддерживаемых ОС различные версии UNIX, а также Windows NT, NetWare, OpenVMS и т. д.

Возможности ESM могут быть расширены с целью обеспечения поддержки новых приложений. Программный инструментарий ESM SDK позволяет создавать новые модули безопасности для поддержки новых приложений, таких как серверы СУБД, Web-серверы, почтовые серверы, МЭ и т. п. Разработка новых модулей осуществляется при помощи библиотечных функций ESM API. В настоящее время разработаны политики безопасности для контроля соответствия настроек ОС требованиям стандарта ISO 17799, а также специализированная антивирусная политика для контроля серверной части NAV Corporate Edition 7.6. Количество политик безопасности, предназначенных для контроля различных аспектов функционирования АС и различных видов приложений, постоянно увеличивается. Список доступных политик и реализующих их модулей безопасности ESM, можно найти на Web-сайте Symantec Security Response Team http://securityresponse.symantec.com/.
В состав ESM также входят специальные модули для его интеграции со средствами сетевого управления HP OpenView и Tivoli.

Несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому их лучше применять совместно с сетевыми сканерами.

Система контроля защищенности ОС Solaris - ASET

Система контроля защищенности ASET (Automated Security Enhancement Tool) является стандартным средством ОС Solaris. ASET выполняет семь основных задач по анализу конфигурации ОС, выявлению уязвимостей, контролю неизменности атрибутов безопасности и системных файлов. ASET контролирует атрибуты доступа файлов, проверяет установленные значения параметров в критичных системных файлах конфигурации.

Задачи, выполняемые системой ASET, включают в себя следующее:

- Проверка прав доступа к системным файлам
- Проверка целостности системных файлов
- Проверка пользователей и групп
- Проверка содержимого системных файлов конфигурации
- Проверка пользовательских окружений
- Проверка параметра eeprom
- Установка межсетевого экрана

При выполнении каждой задачи генерируется отчет, содержащий информацию об обнаруженных уязвимостях и изменениях, внесенных в содержимое системных конфигурационных файлов. При функционировании на высоком уровне безопасности, ASET пытается исправить все обнаруженные уязвимости. Если исправить уязвимость не удается, то в отчет включается сообщение об уязвимости.

ASET осуществляет проверку целостности системных файлов путем сравнения их текущего состояния с описанием, содержащимся в главном файле. Главный файл создается при первом выполнении программой ASET этой задачи. Он содержит параметры системных файлов, соответствующие списку проверки данного уровня защищенности.

Для каждого уровня защищенности определяется список каталогов, содержимое которых подвергается проверке. Администратор может использовать стандартный список или изменить его в случае необходимости, в соответствии с требованиями политики безопасности.

Критерий проверки системных файлов включает в себя следующие параметры:

- владелец и группа файла
- битовая маска прав доступа к файлу
- размер файла и контрольная сумма
- количество ссылок на файл
- время последней модификации файла

Любые обнаруженные несоответствия записываются в файл cklist.rpt. Этот файл содержит результаты сравнения размеров системных файлов, прав доступа и значений контрольных сумм с соответствующим описанием, находящимся в главном файле.

ASET может функционировать на одном их трех уровней: низком, среднем и высоком. На вышестоящих уровнях осуществляется более строгий контроль безопасности системы.

- Низкий уровень безопасности включает проверку атрибутов безопасности системных файлов. На этом уровне осуществляется ряд проверок, при этом никаких изменений в конфигурацию системы не вносится. Изменение конфигурации сетевых сервисов на этом уровне не производится.

- Средний уровень безопасности. На этом уровне модифицируются некоторые атрибуты системных файлов и параметров конфигурации ОС. Изменение конфигурации сетевых сервисов на этом уровне не производится.

- Высокий уровень безопасности. На этом уровне изменяется значительное количество параметров конфигурации системы, максимально ограничивающих возможности пользователей ОС. На этом уровне большинство системных команд и приложений продолжают нормально функционировать, но соображениям безопасности отдается предпочтение перед соображениями функциональности.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Семинарские занятия РУП не предусмотрены.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие № 1-2 (4 часа).

Тема: «Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации»

3.1.1 Задание для работы:

1. Основные понятия о методах защиты.
2. Обеспечение КОИБАС

3.1.2 Краткое описание проводимого занятия:

1. Основные понятия о методах защиты.

Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от НСД — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим НСД к защищаемой информации, может выступать государство, юридическое лицо, группа

физических лиц, в т. ч. общественная организация, отдельное физическое лицо.
Система защиты информации — совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.
Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной.
Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар) и т. п.
Современная автоматизированная система (АС) обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.
Компоненты АС можно разбить на следующие группы:
• аппаратные средства — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);
• программное обеспечение — приобретенные программы, исходные, объектные, загрузочные модули; ОС и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
• данные — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;
• персонал — обслуживающий персонал и пользователи.
Одной из особенностей обеспечения информационной безопасности в АС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, соответствуют физические представления в компьютерной среде:
• для представления информации — машинные носители информации в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;
• объектам системы — пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем

информации;

• субъектам системы — активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Перечисленные выше базовые свойства информации нуждаются в более полном толковании.

Конфиденциальность данных — это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести, например, следующие: личную информацию пользователей; учетные записи (имена и пароли); данные о кредитных картах; данные о разработках и различные внутренние документы; бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Установление градаций важности защиты защищаемой информации (объекта защиты) называют категорированием защищаемой информации.

2. Обеспечение КОИБАС

"Комплексное обеспечение информационной безопасности автоматизированных систем" - область науки и техники, охватывающая совокупность проблем, связанных с построением, исследованием и эксплуатацией систем и технологий обеспечения информационной безопасности автоматизированных систем.

Объектами профессиональной деятельности выпускника являются автоматизированные системы обработки, хранения и передачи информации определенного уровня конфиденциальности, методы и средства обеспечения информационной безопасности автоматизированных систем.

Выпускник в соответствии с фундаментальной и специальной подготовкой может осуществлять следующие виды профессиональной деятельности. Проектно-конструкторская:

- разработка проектов нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;

- участие в разработке новых систем аппаратуры контроля, средств автоматизации

контроля, моделей и систем защиты информации;
- участие в анализе технических заданий на проектирование, выполнении технических и рабочих про¬ектов подсистем информационной безопасности автоматизированных систем, с учетом действующих нормативных и методических документов.
Организационно-технологическая:
- выполнение полного объема работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;
- анализ материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации;
- анализ существующих методов и средств, применяемых для контроля и защиты информации, разработка предложений по их совершенствованию и повышению их эффективности;
- участие в работах по проведению оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений.
Эксплуатационная:
- осуществление регламентных работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем, и работ, осуществляемых в режимах нештатных ситуаций, в том числе мероприятий, обязательных для автоматизированных систем, содержащих сведения, составляющие государственную тайну;
- анализ эксплутационной и иной документации организаций и подразделений ведомства с целью подготовки решений по совершенствованию подсистем, обеспечивающих защиту информации; - обеспечение эффективного использования средств автоматического контроля, обнаружения и закрытия возможных каналов утечки конфиденциальных сведений;
Организационно-управленческая:
- выполнение оперативного управления деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик; - текущий анализ материалов с целью подготовки решений по оперативному управлению процессами обеспечения режима защиты конфиденциальной информации;
- работа по оценке технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-управленческих решений. Конкретные виды деятельности

определяются содержанием образовательной профессиональной программы, разработанной вузом.

3.1.3 Результаты и выводы:

В ходе работы студенты ознакомились с основными целями, задачами и содержанием курса в целом, его ролью и местом в подготовке специалистов по комплексной защите информации.

3.2 Практическое занятие № 3-4 (4 часа).

Тема: «Государственная система защиты информации в Российской Федерации от утечки по техническим каналам»

3.2.1 Задание для работы:

1. Классификация систем защиты информации.
2. Российские системы защиты информации.

3.2.2 Краткое описание проводимого занятия:

1. Классификация систем защиты информации.

Системы защиты ПО широко распространены и находятся в постоянном развитии, благодаря расширению рынка ПО и телекоммуникационных технологий. Необходимость использования систем защиты (СЗ) ПО обусловлена рядом проблем, среди которых следует выделить: незаконное использование алгоритмов, являющихся интеллектуальной собственностью автора, при написании аналогов продукта (промышленный шпионаж); несанкционированное использование ПО (кража и копирование); несанкционированная модификация ПО с целью внедрения программных злоупотреблений; незаконное распространение и сбыт ПО (пиратство).

Существующие системы защиты программного обеспечения можно классифицировать по ряду признаков, среди которых можно выделить:

1) метод установки;

2) используемые механизмы защиты;

3) принцип функционирования.

Системы защиты ПО по методу установки можно подразделить на:

1) системы, устанавливаемые на скомпилированные модули ПО;

2) системы, встраиваемые в исходный код ПО до компиляции;

3) комбинированные.

Системы первого типа наиболее удобны для производителя ПО, так как легко можно

защитить уже полностью готовое и аттестированное ПО, а потому и наиболее популярны. В то же время стойкость этих систем достаточно низка (в зависимо- сти от принципа действия СЗ), так как для обхода защиты достаточно определить точку завершения работы "конверта" за- щиты и передачи управления защищенной программе, а затем принудительно ее сохранить в незащищенном виде.

Системы второго типа неудобны для производителя ПО, так как возникает необходимость обучать персонал работе с программным интерфейсом (API) системы защиты с вытекающими отсюда денежными и временными затратами. Кроме того, усложняется процесс тестирования ПО и снижается его надежность, так как кроме самого ПО ошибки может содержать API сис- темы защиты или процедуры, его использующие. Но такие системы являются более стойкими к атакам, потому что здесь исчезает четкая граница между системой защиты и как таковым ПО.

Наиболее живучими являются комбинированные системы защиты. Сохраняя достоинства и недостатки систем второго типа, они максимально затрудняют анализ и дезактивацию своих алгоритмов.

По используемым механизмам защиты СЗ можно классифицировать на:

1) системы, использующие сложные логические механизмы;

2) системы, использующие шифрование защищаемого ПО;

3) комбинированные системы.

Системы первого типа используют различные методы и приемы, ориентированные на затруднение дизассемблирования, отладки и анализа алгоритма СЗ и защищаемого ПО. Этот тип СЗ наименее стоек к атакам, так как для преодоления защиты достаточно проанализировать логику процедур проверки и должным образом их модифицировать. Более стойкими являются системы второго типа. Для дезактивации таких защит необходимо определение ключа дешифрации ПО. Самыми стойкими к атакам являются комбинированные системы.

Для защиты ПО используется ряд методов, таких как:

1. Алгоритмы запутывания – используются хаотические переходы в разные части кода, внедрение ложных процедур – "пустышек", холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п.

2. Алгоритмы мутации – создаются таблицы соответствия операндов-синонимов и замена их друг на друга при каждом запуске программы по определенной схеме или случайным образом, случайные изменения структуры программы.

3. Алгоритмы компрессии данных – программа упаковывается, а затем распаковывается по мере выполнения.

4. Алгоритмы шифрования данных – программа шифруется, а затем расшифровывается по мере выполнения.

5. Вычисление сложных математических выражений в процессе отработки механизма защиты – элементы логики защиты зависят от результата вычисления значения какой-либо формулы или группы формул.

6. Методы затруднения дизассемблирования – используются различные приемы, направленные на предотвращение дизассемблирования в пакетном режиме.

7. Методы затруднения отладки – используются различные приемы, направленные на усложнение отладки программы.

8. Эмуляция процессоров и операционных систем – создается виртуальный процессор и/или операционная система (не обязательно существующие) и программа-переводчик из системы команд IBM в систему команд созданного процессора или ОС, после такого перевода ПО может выполняться только при помощи эмулятора, что резко затрудняет исследование алго- ритма ПО.

9. Нестандартные методы работы с аппаратным обеспечением – модули системы защиты обращаются к аппаратуре

ЭВМ, минуя процедуры ОС, и используют малоизвестные или недокументированные ее возможности.

По принципу функционирования СЗ можно подразделить на:

1) упаковщики/шифраторы;

2) СЗ от несанкционированного копирования;

3) СЗ от несанкционированного доступа (НСД).

2. Российские системы защиты информации

Государственная система защиты информации представляет собой совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации. Так же является составной частью системы обеспечения национальной безопасности Российской Федерации и призвана защищать безопасность государства от внешних и внутренних угроз в информационной сфере. Организацию деятельности государственной системы технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной Государственной системой осуществляет ФСТЭК России. Государственная система защиты информации как система более сложная, включает в себя подсистемы лицензирования деятельности предприятий в области защиты информации, сертификации средств защиты информации и аттестации объектов

информатизации

по требованиям безопасности информации.

Выше перечисленные подсистемы представляют в совокупности деятельность следующих органов:

- Федеральная служба технического и экспортного контроля (ФСТЭК России) и ее территориальные органы (региональные управления в субъектах Российской Федерации)
- Федеральные органы исполнительной власти, другие органы и организации Российской Федерации, руководящие работники которых входят в состав коллегии ФСТЭК России по должности (Минюст, Минобороны, МЧС, МВД, МИД, Минпромэнерго, Минэкономразвития, Минприроды, ФСО, ФСБ, СВР, ГУСП, РАН, ЦБР)
- Структурные подразделения по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации
- Предприятия, проводящие работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделения по защите информации
- Научно-исследовательские организации по проблемам защиты информации
- Организации-разработчики средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации
- Предприятия, оказывающие услуги в области защиты информации
- Организации Федерального агентства по техническому регулированию и метрологии (бывшего Госстандарта России), выполняющие работы по стандартизации в области защиты информации
- Органы системы лицензирования деятельности в области защиты информации
- Органы системы сертификации средств защиты информации
- Органы системы аттестации объектов защиты по требованиям безопасности информации

Функционирование государственной системы защиты информации осуществляется на основании законности:

- Конституция Российской Федерации
- ФЗ «О безопасности»
- ФЗ «О государственной тайне»
- ФЗ «Об информации, информатизации и защите информации»
- ФЗ «Об участии в международном информационном обмене»
- Доктрина информационной безопасности Российской Федерации
- Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от утечки по техническим (утверждено Постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №912–51)
- Указы президента Российской Федерации (№1085 от 16.8.2004 г.)
- Постановления правительства Российской Федерации
- Другие правовые акты федеральных органов власти в области защиты информации

Так же деятельность государственной системы защиты информации реализуется на основе подчиненности Президенту РФ. А так же основываясь на разграничении полномочий федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций по защите информации.

Обеспечение условий, способствующих реализации политики Российской Федерации в сфере безопасности Государства, содействие экономическому и научно - техническому прогрессу страны, предотвращение или существенное снижение ущерба национальной

безопасности Российской Федерации с использованием методов и средств защиты информации - все это цели преследуемые государственной системой защиты информации, для достижения которых необходимо решить следующие задачи:

- Проведение единой технической политики, организация и координация работ по защите информации в военной, экономической, научно-технической и других сферах деятельности
- Исключение или существенное затруднение добывания информации техническими средствами разведки
- Принятие правовых актов, регулирующих отношения в области защиты информации
- Организация сил, создание средств защиты информации и контроля их эффективности
- Контроль состояния защиты информации в органах государственной власти и на предприятиях
- Анализ состояния государственной системы, выявление ключевых проблем в области защиты информации
- Определение приоритетных направления государственной системы защиты информации
- Нормативно-методическое и информационное обеспечение работ по защите информации

3.2.3 Результаты и выводы:

В ходе работы студенты ознакомились с государственной системой защиты информации в Российской Федерации от утечки по техническим каналам.

3.3 Практическое занятие № 5-6 (4 часа).

Тема: «Особенности утечки информации. Возможные каналы утечки информации, акустический и виброакустический каналы. Этапы развития DLP-систем»

3.3.1 Задание для работы:

1. Определение возможности утечки.
2. Виброакустические каналы.
3. Этапы развития DLP-систем

3.3.2 Краткое описание проводимого занятия:

1. Определение возможности утечки.

Определение и нейтрализация внедрённых средств негласного съема информации – одно из главных направлений в защите информации в любых организациях.

Чтобы представлять возможные каналы утечки информации необходимо знать, что нужно защитить. Это позволит оценить потенциальные пути проникновения «противника» и выявить наиболее уязвимые места в организации. Как говорил китайский мудрец Сунь-цзы: «Знать наперед намерения противника – это, по сути, действовать как Бог!». Необходимо определить главные пути поиска, разграничить объекты обследования по группам, к каждой из которых будет необходим свой подход и соответствующее методическое и аппаратурное обеспечение. Перечислим некоторые из основных групп для обследования [3]:

- технические средства, обрабатывающие конфиденциальную информацию, и обнаружение в них побочных излучений;
- вспомогательные технические средства и системы, содержащие электронные компоненты и узлы;
- помещения и ограждающие их конструкции;
- радиоэфир и определение радиосигналов, излучаемых средствами съема информации;
- предметы обихода, такие как мебель;
- инженерные сети;
- проводные коммуникации и электроустановочные изделия.

Одним из главных методов технической защиты является проведение глубокой проверки или, так называемые, поисковые мероприятия.

Их смысл заключается в оценке безопасности объекта, нахождении «жучков» и в дальнейшей разработке и выполнении комплекса мероприятий, исключающих возможность утечки и перехвата информации в будущем.

Исходя из вышесказанного, следует, что при проведении всех подобных мероприятий решаются следующие практические задачи [2]:

- определяется вероятный злоумышленник, и оцениваются его возможности по проникновению в помещение;
- изучается помещение и окружающие его объекты;
- изучается режим посещения помещения;
- устанавливаются все факты ремонта, монтажа или демонтажа коммуникаций, установки или замены мебели или предметов интерьера;
- анализируются конструктивные особенности ограждающих конструкций помещения и всего здания в целом;
- изучаются все коммуникации, входящие в помещение или проходящие через него.

После решения задач начинаются работы по проведению поисковых мероприятий и непосредственная зачистка помещений от технических средств съема информации.

К основным методам определения закладных устройств можно отнести [1]:

- обследование выделенных помещений;
- определение радиозакладок с использованием индикаторов поля, радиочастотомеров и интерсепторов, сканерных приемников и анализаторов спектра;
- определение радиозакладок с использованием программно-аппаратных комплексов контроля;
- определение портативных звукозаписывающих устройств с использованием детекторов диктофонов (по наличию в них побочных электромагнитных излучений генераторов подмагничивания и электродвигателей);
- определение портативных видеозаписывающих устройств с использованием детекторов видеокамер (по наличию в них побочных электромагнитных излучений генераторов подмагничивания и электродвигателей);
- определение закладок с использованием нелинейных локаторов, рентгеновских комплексов;
- проверка линий электропитания, радиотрансляции и телефонной связи;

- измерение параметров линий электропитания, телефонных линий связи и т.д. (так называемая паспортизация);
- проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов автоматической телефонной станции.

Согласно П.П. Шаповалову [4], зрительный осмотр и проверка предметов, находящихся на объекте поиска, должны начинаться со зрительного фиксирования или фотографирования мест расположения всех предметов в обследуемом помещении. Перед осмотром обращается внимание на возможные метки, которые могут оставляться с различной целью, в том числе и с целью фиксирования места размещения предметов, имеющих средства съема информации.

Метками могут быть определенные расположения разных предметов, нитки, волосы, лежащие в определенном порядке, следы пальцев, пыли, а также метки, наносимые специальным химическим составом и другие характерные пометки.

Зрительный осмотр и диагностику предметов, имеющихся в местах проведения поисковых мероприятий, необходимо реализовывать в определенном порядке. Первым делом осмотру подлежит вся территория обследования. Проверяется, не изменено ли расположения вещей от ранее установленного порядка (смещены, повернуты, переставлены местами и т.д.). Исследуются неплотно прилегающие к стене плинтусы, обои, розетки и т.д.

Особое внимание уделяется изменению оттенка (потемнению или просветлению) обоев, ковровых покрытий, пола, а также свежеокрашенным стенам, потолкам, изменениям в обшивке автомашин, срубленным деревьям, помятой траве и т.д., временным стоянкам автомобилей и другим подозрительным изменениям особенностей мест и предметов.

После общего досмотра выносится из помещения вся мебель, основные технические средства и системы и другие предметы, находившиеся в помещении, и приступают к пристальному досмотру конкретных предметов на предмет потенциальных каналов утечки информации, ведь даже с виду безобидных клавиатур и мышек можно снять информационные сигналы. Описание такой процедуры есть у А. Барисани и Д. Бьянко [5].

Кабель, к которому клавиатура подключается к ПК, он же PS/2, состоит из следующих проводов:

- Pin 1: Передаваемые данные.
- Pin 2/6: Не используются.
- Pin 3: Земля/Корпус. Общий вывод для питания.
- Pin 4: Питание, +5В. Используется для подачи питания на подключаемое устройство.
- Pin 5: Частотный вывод, или CLK (Clock). Включается при передаче данных мышью.

PS/2 сигнал представляет собой привлекательную и относительно благоприятную мишень для подслушивающих. Основным преимуществом сигнала является последовательный характер, поскольку данные передаются один бит за один раз, каждое нажатие клавиши отправляется в кадре, состоящим из 11-12 разрядов.

Так как провода очень близко расположены и не экранированы друг от друга, то предполагается, что случайная утечка информации идет из кабеля данных к кабелю заземления и/или по экрану кабеля из-за электромагнитного взаимодействия. Провод заземления, также как экран кабеля, проложены к адаптеру, который затем подключен к разъему питания и, наконец, к электрической сети.

В конечном итоге нажатие клавиш приводит к утечке информативных сигналов в электрическую сеть, которые затем могут обнаруживаться на самой вилке питания, в том числе и на соседней.
Существуют и другие факторы, приводящие к утечке такие, как колебания мощности микроконтроллера клавиатуры. Они сложны для обнаружения, но если присутствуют, то могут только усиливать утечку информации.
Частота синхронизации PS/2 сигнала ниже, чем любого другого компонента или сигнала, излучаемого ПК (все остальные значения, как правило, выше МГц), это позволяет фильтровать шумы и добычу сигнала нажатия клавиш.
В целях реализации атаки на землю из соседней розетки сигнал направляется на аналого-цифровой преобразователь (АЦП) с использованием модифицированного кабеля питания, который отделяет провод заземления для исследования и включает в себя резистор между парой щупов. Ток рассеивается на земле и измеряется с помощью разности потенциалов между двумя концами резистора. С «близкой» розетки мы идентифицируем все, подключенное к той же электрической системе с небольшого расстояния.
Для того, чтобы измерить «эталон» земли АЦП, потребуется правильное основание для своей собственной работы, но, в то же время, электрическое заземление является объектом наших исследований. Потому главная земля не может быть использована в качестве оборудования земли, поскольку это приведет к нулю разность потенциалов на двух концах датчика.
С целью выделения требуемого диапазона частот используется полосовой фильтр пропускания частот 1-20 кГц. С конечной импульсной характеристикой фильтр является лишь одним из многих возможных методов фильтрации, причем, это – не самый эффективный метод.
Измерялась разность потенциалов на расстоянии 1, 5, 10, 15 метров от фактической цели. Во всех случаях с использованием цифрового осциллографа в качестве АЦП, путем отбора проб и хранения разности потенциалов, можно получить данные об активности провода заземления. В то время как нефильтрованный сигнал, по-видимому, не имеет никакой полезной информации, можно было успешно отфильтровать нажатия клавиш пользователя от исходного шума с помощью фильтра с конечной импульсной характеристикой (FIR фильтра). PS/2 прямоугольный импульсный сигнал сохраняется с хорошим качеством и может быть декодирован в первоначально вводимую пользователем информацию. При этом не было значительного ухудшения качества сигнала на расстоянии 1 метр и 15 метров, поэтому предполагается, что такое ослабление не является проблемой в этом вопросе.
Основной способ защиты от подобной атаки (кроме, очевидно, использования ноутбуков, которые не подключены к розетке и имеют экранированное питание) – это эффективное экранирование оборудования ПК.
Считается, что USB-клавиатуры не подвержены этой атаке, так как они используют дифференциальные сигналы для снижения шума, хотя USB-микроконтроллеры в клавиатуре гораздо более «шумны», чем PS/2, и есть шанс, что какие-то случайные излучения все-таки возможны. Таким образом, результаты ясно показывают, что информация, вводимая с клавиатуры, действительно просачивается в цепи электропитания электросети и может быть считана.

Продолжая изучение проблемы съема информации, следует заострить внимание на проверке предметов, находящихся в помещении, при этом необходимо скрупулезно проверить дверные ручки, вешалки и другие приспособления.

Особое внимание следует обратить на подозрительные отверстия, чужеродные вставки, неестественно запачканные места и другие необычные особенности предметов, находящихся на объекте, где проводятся поисковые мероприятия. Осмотр необходимо проводить с помощью лупы, а недоступные места (вентиляционные каналы, места за батареями отопления, дымоходы и т.д.) осматривают с помощью специальных досмотровых комплектов.

Проведение комплексных специальных проверок помещений не сможет полностью защитить охраняемые сведения от различных угроз. Необходима постоянно развивающаяся система информационной безопасности, сводящая возможные угрозы к минимуму.

Создание такой системы – одна из основных задач служб безопасности различных организаций. Немаловажным условием, способствующим улучшению ситуации с уменьшением угроз съема информации, будет также тщательный отбор и обучение персонала, что способствует уменьшению текучки кадров и более рациональному решению проблемы «человеческого фактора».

Таким образом, непрерывно возрастающему уровню угроз должен быть противопоставлен постоянный рост технической оснащённости организаций и предприятий и профессионализма специалистов, работающих в области защиты информации.

2. Виброакустические каналы.

В виброакустических (вибрационных) технических каналах утечки информации акустические сигналы, возникающие при ведении разговоров в выделенном помещении, при воздействии на строительные конструкции (стены, потолки, полы, двери, оконные рамы и т.п.) и инженерно-технические коммуникации (трубы водоснабжения, отопления, канализации, воздуховоды и т.п.) вызывают в них упругие (вибрационные) колебания, которые и регистрируются датчиками средства разведки (рис. 1,2.)

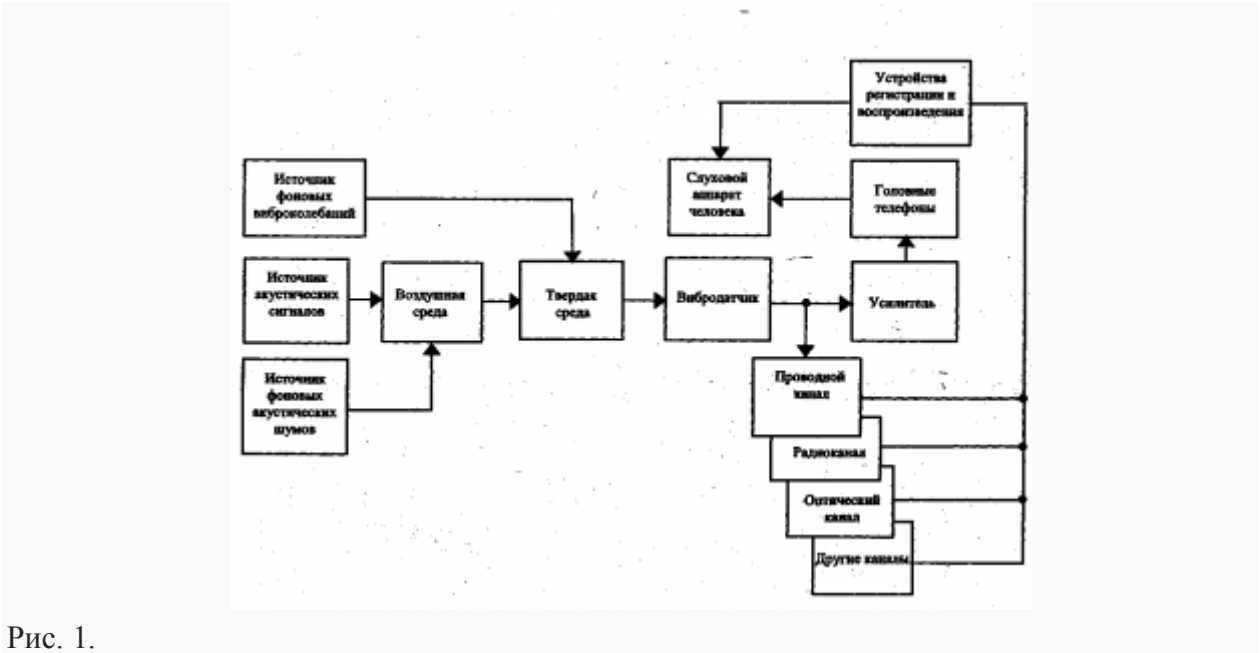


Рис. 1.

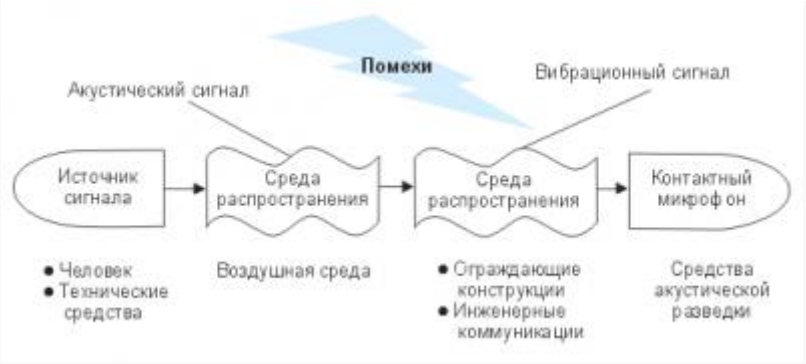


Рис. 2.

Перехват речевой информации по виброакустическим каналам.

Для перехвата речевой информации по виброакустическим каналам в качестве средств акустической разведки используются электронные стетоскопы и закладные устройства с датчиками контактного типа. Наиболее часто для передачи информации с таких закладных устройств используется радиоканал, поэтому их называют радиостетоскопами.

В качестве датчиков средств акустической разведки используются контактные микрофоны (вибропребразователи), чувствительность которых составляет от 50 до 100 мкВ/Па, что, дает возможность прослушивать разговоры и улавливать слабые звуковые колебания (шорохи, тиканье часов и т.д.) через бетонные и кирпичные стены толщиной более 100 см, а также двери, оконные рамы и инженерные коммуникации.

Электронные стетоскопы и закладные устройства с датчиками контактного типа позволяют перехватывать речевую информацию без физического доступа “агентов” в выделенные помещения. Их датчики наиболее часто устанавливаются на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

При этом возможности по перехвату информации будут во многом определяться затуханием информационного сигнала в ограждающих конструкциях и уровнем внешних шумов в месте установки контактного микрофона (табл. 1, 2) [2 – 4].

Таблица 1. Затухание вибрационных сигналов на ограждающих конструкциях

Наименование конструкции	Затухание сигнала, дБ
Стена в 0,5 кирпича	40 – 48
Стена в 1 кирпич	44 – 53
Стена в 2 кирпича	46 – 60

Стена из железобетонных блоков (100 мм)	40 – 50
Стена из железобетонных блоков (200 мм)	44 – 60
Окно одинарное (4 мм)	22 – 28
Окно двойное (4 мм)	32 – 48
Дверь типовая	23 – 34
Дверь металлическая, облицованная	32 – 48

Таблица 2. Средний интегральный уровень вибрационных шумов

Наименование конструкции	Уровень шума, дБ
Внешняя конструкция здания	15 – 35
Внутренняя конструкция здания	10 – 30
Внешнее стекло окна	25 – 30
Внутреннее стекло окна	10 – 15
Трубопровод отопления с водой	15 – 20
Трубопровод отопления без воды	10 – 15

Проведенные измерения и расчеты показали, что качество добываемой средствами акустической разведки речевой информации по прямому акустическому и

виброакустическому каналам вполне достаточно для составления подробной справки о содержании перехваченного разговора (табл. 3) [1].

Таблица 3. Разборчивость речи при перехвате информации средствами разведки по виброакустическому каналу

Место установки датчика аппаратуры акустической разведки	Словесная разборчивость, %
На оконной раме или внешнем оконном стекле при закрытой форточке	71 – 80
На перегородке из материалов типа гипсолит, асбестоцемент	84 – 95
На железобетонной стене	80 – 98
На трубопроводе (через этаж)	95 – 97

Необходимо отметить, что чем тверже материал преграды на пути распространения акустических колебаний, тем лучше он передает вибрации, вызываемые ими. Поэтому, если стена помещения сделана из гипсолита, сухой штукатурки и т.п., необходимо вбить в нее металлический предмет (можно использовать обычный крупный гвоздь) и крепить датчик стетоскопа непосредственно к нему. Бели стена бетонная или кирпичная, но покрыта штукатуркой или обоями, то желательно зачистить участок до твердого основания и стетоскоп крепить именно на это место. В качестве звукопровода можно использовать трубы водоснабжения, канализации, батареи отопления и т.д. Крепление вибродатчиков к элементам конструкции, по которой распространяются вибрации, может осуществляться с помощью специальных мастик, клеевых составов, магнитов и т.д. На качество приема вибросигналов кроме свойств вибродатчика и материала твердой среды влияют ее толщина, а также уровни фоновых акустических шумов в помещении и вибраций в твердой среде. В ряде случаев, когда нет возможности разместить пункт прослушивания в непосредственной близости от места установки вибродатчика (стетоскопа), в состав аппаратуры прослушивания включают проводные, радио- и другое каналы передачи информации, аналогичные каналам, используемым в закладных подслушивающих устройствах.

3. Этапы развития DLP-систем

Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности. Однако первоначально внешние угрозы считались более опасными. В последние годы на внутренние угрозы стали обращать

больше внимания, и популярность DLP-систем возросла. Необходимость их использования стала упоминаться в стандартах и нормативных документах (например, раздел "12.5.4 Утечка информации" в стандарте ГОСТ ISO/IEC 17799-2005 <#"justify">Первыми появились технологии сетевого мониторинга - без возможности блокировки утечки через сетевые протоколы (HTTP, SMTP…). В дальнейшем производители добавляли функции блокировки информации при передаче через сеть. Затем появились возможности контроля рабочих станций за счет внедрения программных "агентов", чтобы можно было предотвратить передачу конфиденциальной информации с этих устройств: контроль функций "copy/paste", снятия скриншотов, а также контроль передачи информации на уровне приложений: например, в одном приложении функций "copy/paste" разрешен, в другом - запрещен.

И, наконец, появились технологии поиска конфиденциальной информации на сетевых ресурсах и ее защиты, если информация обнаружена в тех местах, где ее не должно быть. Конфиденциальная информация при этом задается предварительно ключевыми словами, словарями, регулярными выражениями, "цифровыми отпечатками". В результате поиска система может показать - где она обнаружила конфиденциальную информацию, и какие политики безопасности при этом нарушаются. Далее сотрудник службы безопасности может принимать соответствующие меры. Есть решения, которые не просто показывают наличие конфиденциальной информации в неположенном месте, а переносят эту информацию "в карантин", оставляя в файле, где была обнаружена информации, запись - куда перенесена конфиденциальная информация и к кому обратиться за получением доступа к этой информации.

3.3.3 Результаты и выводы:

В ходе работы студенты ознакомились с особенностями утечки информации, возможными каналами утечки информации, акустическим и виброакустическим каналами и основными этапами развития DLP-систем.

3.4 Практическое занятие № 7-8 (4 часа).

Тема: «Каналы утечки информации при эксплуатации ЭВМ. Анализ передаваемой информации»

3.4.1 Задание для работы:

1. Возможности утечки.
2. Анализ информации.
3. Предотвращения утечек.

3.4.2 Краткое описание проводимого занятия:

1. Возможности утечки.

В настоящее время одной из наиболее актуальных проблем в области информационной безопасности является проблема защиты от утечки конфиденциальной информации. Технические варианты решения данной проблемы, рассмотренные в статье, могут быть сгруппированы в два типа. Первый тип предполагает изменение топологии защищаемой АС путём создания изолированной системы обработки конфиденциальной информации,

либо выделения в составе АС сегмента терминального доступа к конфиденциальным данным. Второй вариант технических решений заключается в применении различных средств защиты АС, включая средства активного мониторинга, контентного анализа, а также средства криптографической защиты информации. Результаты анализа этих двух типов технических решений показали, что каждое из них характеризуется своими недостатками и преимуществами. Выбор конкретного средства защиты зависит от множества факторов, включая особенности топологии защищаемой АС, тип прикладного и общесистемного ПО, установленного в системе, количество пользователей, работающих с конфиденциальной информацией и многих других. При этом необходимо подчеркнуть, что наибольшая эффективность может быть получена при комплексном подходе, предусматривающим применение как организационных, так и технических мер защиты информационных ресурсов от утечки.

2. Анализ информации.

Понимание потребностей в основе любой задачи по анализу информации тесно связано с пониманием бизнеса компании. Сбор данных из подходящих источников требует опыта в их подборе, независимо от того, насколько окончательный процесс сбора данных может быть автоматизирован. Для превращения собранных данных в аналитические выводы и эффективного применения их на практике необходимы глубокие знания бизнес-процессов и наличие навыков консультирования.

Процесс анализа информации представляет собой цикличный поток событий, который начинается с анализа потребностей в рассматриваемой области. Затем следует сбор информации из вторичных и (или) первичных источников, ее анализ и подготовка отчета для лиц, ответственных за принятие решений, которые будут его использовать, а также давать свои отзывы и готовить предложения.

На международном уровне процесс анализа информации характеризуется следующим образом:

- Сначала в ключевых бизнес-процессах определяются этапы принятия решений, которые сопоставляются со стандартными конечными результатами анализа информации.
- Процесс анализа информации начинается с оценки потребностей на международном уровне, т. е. с определения будущих потребностей, связанных с принятием решений, и их проверкой.
- Этап сбора информации автоматизирован, что позволяет выделить время и ресурсы на первичный анализ информации и, соответственно, повысить ценность уже имеющейся вторичной информации.
- Значительная часть времени и ресурсов тратится на анализ информации, выводы и интерпретацию.
- Полученная в результате аналитическая информация доводится до сведения каждого лица, ответственного за принятие решений, в индивидуальном порядке с отслеживанием процесса ее дальнейшего использования.
- У членов группы, которая занимается анализом информации, сформирована установка на непрерывное совершенствование.

3. Предотвращения утечек.

Предотвращение утечек (англ. *Data Leak Prevention, DLP*) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Используются также следующие термины, обозначающие приблизительно то же самое:

- Data Loss Prevention (DLP);
- Data Leak Prevention (DLP);
- Data Leakage Protection (DLP);
- Information Protection and Control (IPC);
- Information Leak Prevention (ILP);
- Information Leak Protection (ILP);
- Information Leak Detection & Prevention (ILDP);
- Content Monitoring and Filtering (CMF);
- Extrusion Prevention System (EPS).

Из этой группы пока не выделился один термин, который можно было бы назвать основным или самым распространённым.

3.4.3 Результаты и выводы:

В ходе работы студенты ознакомились с каналами утечки информации при эксплуатации ЭВМ, анализом передаваемой информации.

3.5 Практическое занятие № 9-10(4 часа).

Тема: Подходы к созданию комплексной системы защиты информации в организации. Основные критерии оценки защиты информации от утечки.

3.5.1 Задание для работы:

1.Комплексное обеспечение информации.
2.Критерии защиты информации.
3. Встроенная защита каналов.

3.5.2 Краткое описание проводимого занятия:

1.Комплексное обеспечение информации.

"Комплексное обеспечение информационной безопасности автоматизированных систем" - область науки и техники, охватывающая совокупность проблем, связанных с построением, исследованием и эксплуатацией систем и технологий обеспечения информационной безопасности автоматизированных систем.
Объектами профессиональной деятельности выпускника являются автоматизированные системы обработки, хранения и передачи информации определенного уровня конфиденциальности, методы и средства обеспечения информационной безопасности автоматизированных систем.
Выпускник в соответствии с фундаментальной и специальной подготовкой может осуществлять следующие виды профессиональной деятельности. Проектно-конструкторская:
- разработка проектов нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;
- участие в разработке новых систем аппаратуры контроля, средств автоматизации контроля, моделей и систем защиты информации;
- участие в анализе технических заданий на проектирование, выполнении технических и рабочих про¬ектов подсистем информационной безопасности автоматизированных систем, с учетом действующих нормативных и методических документов.
Организационно-технологическая:
- выполнение полного объема работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;
- анализ материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации;
- анализ существующих методов и средств, применяемых для контроля и защиты информации, разработка предложений по их совершенствованию и повышению их эффективности;
- участие в работах по проведению оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений.
Эксплуатационная:
- осуществление регламентных работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем, и работ, осуществляемых в режимах нештатных ситуаций, в том числе мероприятий, обязательных для автоматизированных систем, содержащих сведения, составляющие государственную тайну;
- анализ эксплутационной и иной документации организаций и подразделений ведомства с целью подготовки решений по совершенствованию подсистем, обеспечивающих защиту информации; - обеспечение эффективного использования средств автоматического контроля, обнаружения и закрытия возможных каналов утечки конфиденциальных сведений;
Организационно-управленческая:
- выполнение оперативного управления деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик; - текущий анализ материалов с целью подготовки решений по оперативному управлению процессами обеспечения режима защиты конфиденциальной информации;
- работа по оценке технико-экономического уровня и эффективности предлагаемых и

реализуемых организационно-управленческих решений. Конкретные виды деятельности определяются содержанием образовательной профессиональной программы, разработанной вузом.

2.Критерии защиты информации.

Защиту информации оценивают и контролируют в условиях сложной помеховой обстановки, так как контролируемые параметры, как правило, ниже уровня непреднамеренных (фоновых) либо маскирующих (организованных) помех. Результаты измерений должны отвечать требованиям помехозащищенности, а также требованиям достоверности (верности) и степени соответствия нижнего порогового уровня защищенности, оцениваемого по параметрам сигналов при отношении сигнал/шум меньше единицы.

Нормативно-методические документы должны устанавливать воспроизводимость измерений (отображающаяся близость друг к другу результатов измерений, выполненных в различных условиях, в различное время, в различных местах, различными методами и средствами).

Воспроизводимость измерений должна быть высокой и соответствовать необходимой точности. Сложность помеховой обстановки, разнородность элементов и связей, высокая степень неопределенности сложной системы обусловливает временную задержку представления результатов оценки параметров, определяющих защиту информации. Методики измерений совершенствуются для уменьшения временной задержки.

3. Встроенная защита каналов.

- **Для корпоративных и частных пользователей:**
  - недорогое и эффективное решение по защите канала передачи корпоративной и личной информации от несанкционированных проникновений из интернета.
- **Для малого и среднего бизнеса:**
  - эффективные, интегрированные и защищенные коммуникации в едином решении, ранее доступные только крупным корпорациям. Корпоративная система защиты каналов связи позволяет при использовании общедоступного канала доступа в интернет интегрировать в одно целое функциональность ряда прикладных защитных программ без опасения потери, искажения или кражи важной для бизнеса информации.
- **Для крупного бизнеса:**
  - возможность превратить все «тяжелые» и затратные системы в сфере корпоративных сетей в более гибкие, недорогие и при этом не менее функциональные решения на базе интернет-/интранет-технологий без опасения потери конфиденциальной информации;
  - возможность для топ-менеджмента не зависеть от ИТ-подразделений: решения для защиты каналов связи используют раздельные центры

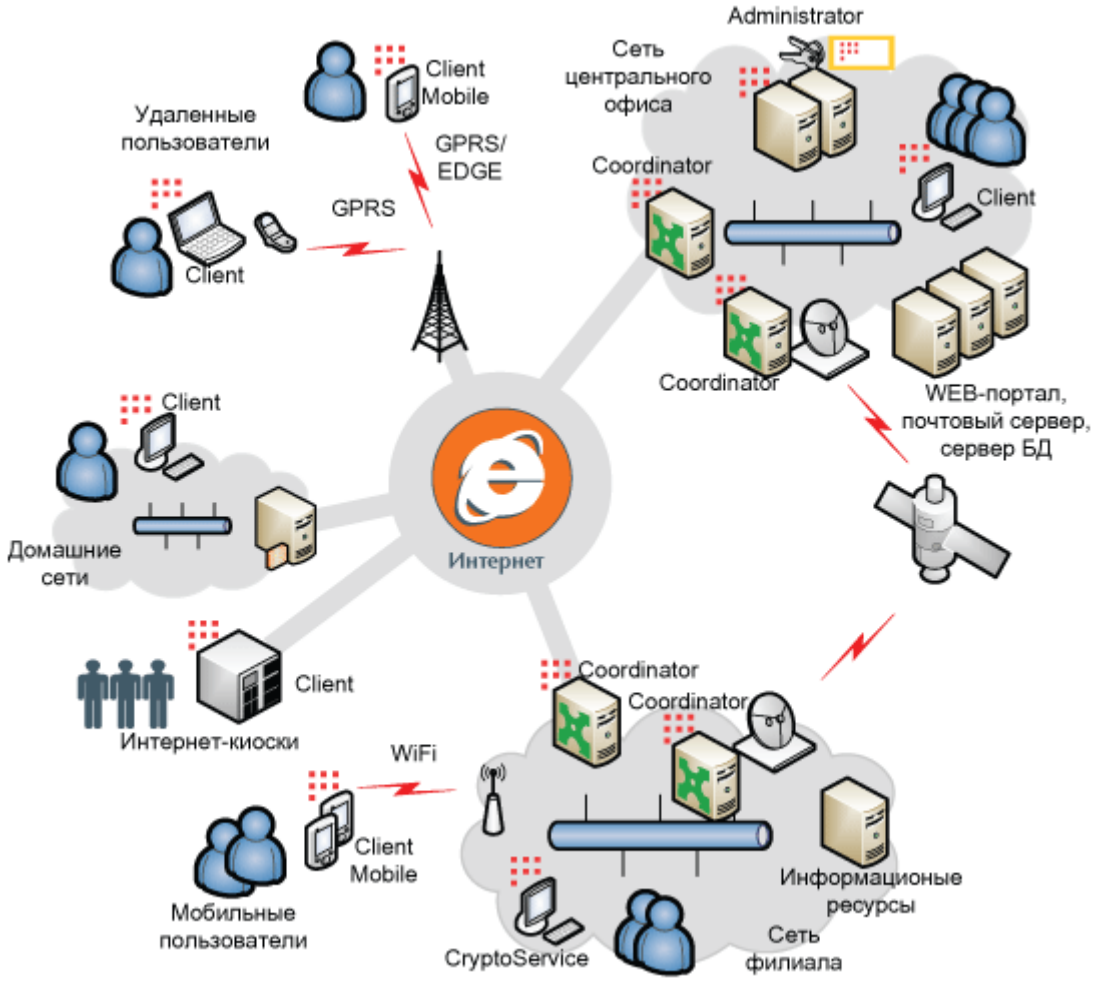
управления безопасностью и сетью и позволяют руководству корпорации вести самостоятельный визуальный контроль состояния всей сети.

В построении **корпоративной системы защиты каналов связи** используются решения ведущих российских и зарубежных производителей средств защиты информации, таких как:

- ViPNet Custom, разрабатываемого и поставляемого партнером компании LETA – компанией «ИнфоТеКС»;
- StoneGate FW\VPN – решение одного из ведущих мировых производителей средств сетевой безопасности.

ViPNet Custom это:

- сертификаты Федеральной службы по техническому и экспортному контролю (ФСТЭК, или Гостехкомиссии) России на соответствие необходимым классам защищенности и уровням доверия;
- сертификаты ФСБ России на средство криптографической защиты информации;
- более 10 различных компонент и модулей, позволяющих реализовать множество сценариев защиты информации в современных мультисервисных сетях связи;
- возможность объединять в единую защищенную виртуальную сеть произвольное число локальных сетей и рабочих станций;
- возможность комбинировать гибкий набор компонент и их функций для любых потребностей небольших структур (объединение нескольких компьютеров через открытые каналы связи) и крупных коммерческих и государственных организаций (большие территориально распределенные сети);
- дополнительные возможности защищенного обмена информацией (встроенные службы мгновенного обмена сообщениями – чат и конференция, файлами, собственная защищенная почтовая служба с элементами автоматизации обмена письмами и поддержкой механизмов ЭЦП).

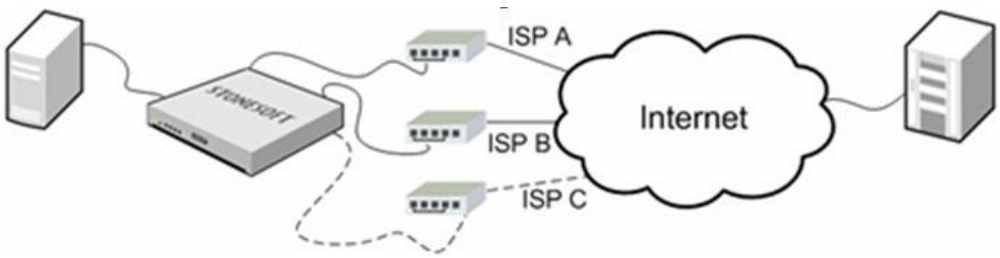


Примеры использования ViPNet для защиты сетей различных масштабов

Корпоративная система защиты каналов связи строится на базе комплекса программного и программно-аппаратного обеспечения ViPNet Custom, разрабатываемого и поставляемого партнером компании LETA – компанией «ИнфоТеКС».

StoneGate FW\VPN удовлетворяет всем современным требованиям к системам безопасности, при этом в его основе лежат уникальные архитектурные решения, не требующие применения вспомогательных специализированных дорогостоящих средств, как в ряде решений конкурентов.

Высокая производительность (до 12 Гб на устройство) и поддержка кластеризации (до 16 устройств) делают решение одним из самых высокопроизводительных и отказоусточивых на рынке сетевой безопасности.



При построении защищенных VPN, StoneGate поддерживает не только стандартные зарубежные криптоалгоритмы, такие как (3)DES, AES, но и «экзотические» варианты Blowfish, Twofish, CAST-128. Более того, в нем также поддерживается модуль шифрования с Российским криптопровайдером и, как следствие, StoneGate FW позволяет создавать VPN на базе алгоритма ГОСТ 28147-89.

Используемые продукты:

- CSP VPN
- ViPNet Custom
- АПКШ «Континент» 3.6

3.5.3 Результаты и выводы:

В ходе работы студенты ознакомились с подходами к созданию комплексной системы защиты информации в организации.

3.6 Практическое занятие № 11-12 (4 часа).

Тема: «Организация и осуществление работ по выявлению каналов утечки информации. Компоненты системы предотвращения утечек. Процесс внедрения DLP-систем»

3.6.1 Задание для работы:

1.DLP-системы.
2. Компоненты систем защиты от утечек.

3.6.2 Краткое описание проводимого занятия:

1.DLP-системы.

Внедрять системы DLP довольно просто, однако настроить их так, чтобы они начали приносить ощутимые выгоды, не так легко. На данный момент при внедрении систем мониторинга и контроля информационных потоков (мой вариант описания термина DLP) чаще всего используют один из следующих подходов:

3. ***Классический***. При таком подходе в компании уже определена критичная информация и требования по ее обработке, а система DLP только контролирует их выполнение.
4. ***Аналитический***. При этом в компании есть общее представление о том, что необходимо контролировать распространение критичной инофрмации (обычно конфиденциальной информации), однако поимание потоков информации и необъодимых требований к ним еще не определены. Тогда система DLP выступает в роде инструментария, собирающего необходимые данные, анализ которых позволит четко сформулировать требования по обработке информации, а затем уже и дополнительно, более точно, настроить и саму систему.

Кратко приведу примеры шагов по внедрению DLP, характерных для каждого из подходов..

Классический подход по внедрению DLP:

11. ***Определить основные бизнес процессы и проанализировать их***. На выходе внеобходимо получить документ "*Перечень конфиденциальной информации*" (иногда это может быть более расширенный перечень, что-то типа рабочего документа "*Перечень контролируемой информации*", т.к. например вы хотите контролировать и пресекать в

электронной переписке использование ненормативной лексики) и рабочий документ "Перечень владельцев информации". Понимание того, кто является владельцем той или иной информации, необходимо для того, чтобы в последствии определить требования по ее обработке.

12. ***Определить основные носители информации и способы передачи.*** Необходимо понять, на каких носителях может присутствовать контролируемая иноформация в рамках ИТ-инфраструктуры организации. При этом хорошей практикой является разработка таких рабочих документов как "*Перечень носителей информации*" и "*Перечень возможных каналов утечки информации*".
13. ***Определить требования по использованию информации и сервисов***. Часто бывает, что такие требования формулируются в отдельных политиках, например, в документах "Политка использования электронной почты", "Политика использования сети Интернет" и другие. Однако удобнее разработать единую "*Политику допустимого использования ресурсов*". В ней имеь смысл указывать требования по следующим блокам: работа с электроной почтой и сетью Интернет, использование съемных носителей; использование рабочих станций и ноутбуков, обработка информации на персональных устройствах (кпк, смартфоны, планшеты и пр.), использование копировально-множительной техники и сетевых хранилищ данных, общение в социальных сетях и блогах, использование сервисов мгновенных сообщений, обработка информации, закрепленнной на твердых носителях (бумага).
14. ***Ознакомить сотрудников с требованиями по использованию информации и сервисов, определенными на предыдущем шаге.***
15. ***Спроектировать систему DLP***. С точки зрения технического проектирования, я рекомендую разрабатывать как минимум "*Техническое задание*" и "*Программу и методику испытаний*". также дополнительно пригодятся и такие документы как "*Корпоративный стандарт по настройке политик DLP*", в котором вы должны детально указать то, как система будет фильтравать информацию и реагировать на события и инциденты, и "*Положение по распределению ролей по управлению и обслуживанию DLP*", в котором Вы зафиксируете роли и границы ответственности за управление DLP.
16. ***Внедрить и настроить систему DLP, запустить в опытную эксплуатацию.***Первоначально это лучше всего сделать в режиме мониторинга.
17. ***Провести обучение персонала, ответственного за управление и обслуживание DLP.*** На данном этапе Вам желатьльно разработать *Комплект ролевых иснструкций по DLP* (управление и обеспечение).
18. ***Проанализировать итоги и результаты опытной эксплуатации, внести правки (при необходимости), запустить в промышленную эксплуатацию.***
19. ***Внести правки (при отсутствии, разработать) в процедуру управления инцидентами (или аналоги).***
20. ***Регулярно проводить анализ инцидентов и совершенствовать политику настройки DLP .***

Аналитический подход по внедрению DLP:

10. ***Спроектировать систему DLP***. На данном этапе будет достаточно простого "*Технического задания*" и "*Программы и методики испытаний*".

11. ***Определить и настроить минимальные политики DLP.*** Нашей задачей является не мониторинг и блокирование любых активностей, а именно сбор аналитической информации о том, какими каналами и средствами пользуются для передачи той или иной корпоративной информации.

12. ***Провести обучение персонала, ответственного за управление и обслуживание DLP.*** Тут можно использовать стандартные "вендорские" инструкции.

13. ***Внедрить и настроить систему DLP, запустить в опытную эксплуатацию*** (в режиме мониторинга).

14. ***Проанализировать итоги и результаты опытной эксплуатации.*** Задача - выявить и проанализировать основные информационные потоки.

15. ***Внести правки (разработать) основные документы, регламентирующие мониторинг и контроль информации, ознакомить с ними сотрудников.*** Документы "*Перечень конфиденциальной информации*" и "*Политика допустимого использования*".

16. ***Внести правки в настройки DLP, определить процедуру управления и обслуживания DLP, запустить в промышленную эксплуатацию***. Разработать документы "*Корпоративный стандарт по настройке политик DLP*", "*Положение по распределению ролей по управлению и обслуживанию DLP*", "*Комплект ролевых инструкций по DLP*".

17. ***Внести правки (при отсутствии, разработать) в процедуру управления инцидентами (или аналоги).***

18. ***Регулярно проводить анализ инцидентов и совершенствовать политику настройки DLP.***

Подходы отличаются, но и тот и другой вполне подходят для внедрения систем DLP. Надеюсь, что представленная выше информация сможет навести Вас на новые удачные мысли по защите информации от утечек.

2. Компоненты систем защиты от утечек.

Системы защиты от утечек конфиденциальной информации (Data Loss Prevention - DLP) предназначены для отслеживания и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети. Помимо предотвращения утечек информации DLP система может выполнять функции по отслеживанию действий пользователей, записи и анализу их коммуникаций через e-mail, социальные сети, чаты и т.д. Основная задача систем DLP – обеспечение выполнения принятой в организации политики конфиденциальности (защита информации от утечки).

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый или репутационный ущерб, а также для организаций, которые настороженно относятся к лояльности своих сотрудников. Решения класса DLP по предотвращению утечек информации обеспечивают защиту такой конфиденциальной информации, как условия тендеров, заказы на услуги и решения, номера пластиковых карт, сведения о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и т.д.

Основные функции DLP-систем

- контроль передачи информации через Интернет с использованием E-Mail, HTTP, HTTPS, FTP, Skype, ICQ и других приложений и протоколов;
- контроль сохранения информации на внешние носители - CD, DVD, flash, мобильные телефоны и т.п.;

- защита информации от утечки путем контроля вывода данных на печать;
- блокирование попыток пересылки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий, использование карантинной папки;
- поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам;
- предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.

Обычно система класса DLP включает следующие компоненты:

- центр управления и мониторинга;
- агенты на рабочих станциях пользователей;
- сетевой шлюз DLP, устанавливаемый на Интернет-периметр.

3.6.3 Результаты и выводы:

В ходе работы студенты ознакомились с компонентами системы предотвращения утечек, процессом внедрения DLP-систем.

3.7 Практическое занятие № 13-14 (4 часа).

Тема: «Общая характеристика средств защиты информации от утечки по техническим каналам. Обзор средств активной защиты. Средства защиты от утечки по каналам ПЭМИН. Устройства защиты телефонных линий. Программные решения, представленные на рынке»

3.7.1 Задание для работы:

1. Активные средства защиты.
2. Наиболее востребуемые программные решения .

3.7.2 Краткое описание проводимого занятия:

1. Активные средства защиты.
В соответствии с требованиями СТР ВС-96 использование ВТ, устанавливаемой для обработки секретной информации в КСА, допускается только после выполнения следующих мероприятий по спецзащите:
- специальной проверки (СП);
- специальных исследований (сертификационных испытаний) (СИ);
- доработок (закрытие каналов утечки секретной информации) по результатам объектовых специальных исследований. Специальная проверка (СП) ОТСС проводится на наличие возможно внедренных электронных устройств перехвата (уничтожения) информации. Она выполняется специализированными

государственными организациями, имеющими лицензию ФАПСИ на производство указанных работ. Специальные исследования (СИ) ОТСС проводятся для выявления возможных каналов утечки секретной информации. СИ выполняются специализированными организациями, имеющими лицензии Гостехкомиссии РФ на производство указанных работ. Комплекс мероприятий по защите информации от утечки включает:
- защиту информации ОТСС от утечки за счет ПЭМИ;
- защиту ВТСС от утечки информации за счет наведенных ПЭМИ от ОТСС. Защита информации осуществляется выполнением организационных и технических мероприятий. К техническим мероприятиям относятся:
- подавление или маскирование информационных сигналов ПЭМИ от ОТСС;
- подавление или маскирование наведенных информационных сигналов на оборудование и электрические цепи, имеющие выход за пределы КЗ.

Реализация технических мероприятий осуществляется с помощью технических средств. Технические средства защиты подразделяются на пассивные и активные. К пассивным средствам защиты относятся:
- экранирование помещений объекта с малой КЗ, в которых размещены ОТСС;
- установка в цепях электропитания ОТСС электрических помехоподавляющих фильтров. К средствам активной защиты (САЗ) относятся:
- средства пространственного зашумления;
- экранирование помещений применяется в случаях, когда контролируемая зона от ОТСС превышает размеры контролируемой зоны объекта.

Наиболее приемлемым материалом для изготовления экрана всего объема помещения является сталь листовая.

Толщина металлического листа, обеспечивающего необходимую эффективность экранирования, определяется расчетом. Конструкция швов экрана должна обеспечивать надежный электрический контакт с низким переходным сопротивлением высокочастотным токам по периметру соединяемых деталей экрана. Для обеспечения этого требования соединение листов экрана должно производиться герметичным швом электродуговой сварки в среде защитного газа по ГОСТ 14771-76. Выполнение экранировки требует значительных экономических затрат и большого расхода материалов, весьма трудоемко, сложно в изготовлении входов в помещения вентиляции и вводов коммуникаций. Для выполнения работ по экранировке требуется высокая квалификация исполнителей. При использовании металлических сеток эффективность экранирования значительно меньше.

Сетевые помехоподавляющие фильтры применяются в сетях электропитания для защиты от высокочастотных наводок. Основными критериями выбора фильтров являются:
- затухание, выраженное в Дб, в заданном диапазоне частот;
- номинальное рабочее напряжение и номинальный рабочий ток.

Фильтры должны иметь сертификат соответствия требованиям безопасности информации Гостехкомиссии.

Средства активной защиты (САЗ) применяются в случаях, когда контролируемая зона ОТСС превышает размеры контролируемой зоны объекта, и способы пассивной защиты неэффективны или экономически и технически нецелесообразны. Системы пространственного зашумления применяются для

создания маскирующих помех в окружающем ОТСС пространстве. Пространственное зашумление рекомендуется осуществлять генераторами шума типа “Гном-3” (“Гном-3М”), “Волна”. Для ПЭВМ оптимальным вариантом САЗ является устройство защиты “Салют”.

Изделие “Салют” ИТСВ.469 435.006-02ТУ предназначено для защиты обрабатываемой информации на персональном компьютере (ПЭВМ) от перехвата электромагнитных излучений, возникающих при его работе.

Изделие предназначено для защиты системного блока, дисплея, соединительных кабелей, подсоединенных периферийных устройств, а также цепей электропитания. В основу метода защиты положено:
- создание вокруг ПЭВМ и периферийных устройств маскирующего поля. Поле создается из ложной, изменяющейся по случайному закону видеоинформации, синхронизированной точными и кадровыми, изменяющимися также по случайному закону, синхроимпульсами;
- создание по строчным и кадровым цепям дисплея дополнительного маскирующего поля, добиваясь, тем самым, идеального совмещения информационного и защитного полей;
- создание нестабильности, изменяющейся по случайному закону, кадровых и строчных синхроимпульсов дисплея;
- создание наведенного маскирующего сигнала в цепях электропитания и подсоединенных периферийных устройствах и вспомогательных технических средствах.

Изделие “Салют” не требует никаких конструктивных изменений в ПЭВМ, так как встраивается в любой свободный слой ISA материнской платы. Изделие комплектуется платой “Салют”, кабелем, антенной, антенными хомутами (зажимами) и паспортом. Плата смонтирована на печатной плате из отечественных ЭРЭ, кроме разъемов, с габаритными размерами 210-95-20 мм. Вход платы с помощью кабеля подключается к выходу видеоадаптера, а выход платы к дисплею, антенну подсоединяют к антенному выходу платы и с помощью хомутов вешают на дисплейный кабель, добиваясь тем самым максимально возможного совмещения излучателей информационного и защитного полей. Система контроля функционирования изделия обеспечивает выдачу светового и звукового сигналов при снижении уровня шума на 6 Дб. Питание изделия осуществляется от материнской платы ПЭВМ + 5 В, потребляемая электрическая мощность не более 3 ВА. При использовании изделия “Салют” обеспечивается:
- радиус возможного перехвата информации по электромагнитному полю не более 2 м от ПЭВМ и его устройств;
- допустимое расположение от устройств ПЭВМ до телефонных аппаратов, других вспомогательных технических средств, имеющих выход за пределы контролируемой территории и их кабелей не более 0,5 м;
- возможность перемещения ПЭВМ и ее периферийных устройств без повторных СИ;
- возможность функционирования ПЭВМ без фильтров по питающим цепям.
Учитывая вышеизложенное, рекомендуется использовать комплексный метод защиты информации - пассивный и активный одновременно. Такой метод защиты позволяет максимально использовать возможности каждого из технических средств и, как следствие, минимизировать затраты на их приобретение и монтаж при выполнении предъявленных требований к защите информации от утечки

2. Наиболее востребуемые программные решения .

Облачные решения — самая актуальная на сегодняшний день концепция организации ИТ-инфраструктуры. Они позволяют значительно снизить стоимость создания и владения ИТ-инфраструктурой, упростить управление ею. Организацию соответствующей среды и, при необходимости, заботу о ней возьмет на себя компания "Ай-Теко".

На данный момент мы предоставляем облачные сервисы разного уровня: от платформы и средств управления до аренды бизнес-приложений.

Инфраструктура как сервис (IaaS)

MakeCloud — уникальный для российского рынка облачных услуг сервис, позволяющий пользователю самостоятельно конструировать полнофункциональную виртуальную ИТ-инфраструктуру с помощью широкого набора элементов: различные конфигурации серверов, виртуальные изолированные сети, файерволы, маршрутизаторы, балансировщики и др.

eCloud — платформа для построения виртуальной IT-инфраструктуры, реализованная на базе технологий виртуализации VMware и предназначенная для крупных компаний и проектов особой сложности.

Платформа как сервис (PaaS)

РУСТЭК — первая российская защищённая облачная платформа для развёртывания виртуальной ИТ- инфраструктуры, соответствующая требованиям обеспечения информационной безопасности к хранению персональных данных и конфиденциальной информации.

ПО как сервис (SaaS)

Магазин облачных сервисов и решений i-Oblako — это интернет-витрина, где размещены наиболее востребованные и зарекомендовавшие себя SaaS-решения для организации основных бизнес-процессов для любого типа и размера бизнеса.

Виртуальный рабочий стол (DaaS)

Виртуальное рабочее место, базирующееся на технологиях компании Microsoft — это быстрый и удобный способ организовать полноценный мобильные рабочие места с привычным интерфейсом и с установленным набором наиболее востребованного лицензионного офисного ПО.

3.7.3 Результаты и выводы:

В ходе работы студенты ознакомились с общей характеристикой средств защиты информации от утечки по техническим каналам.

3.8 Практическое занятие № 15 (2 часа).

Тема: «Методы оценки защищенности информации от утечки по техническим каналам. Обзор средств контроля защищенности. Программные решения, представленные на рынке»

3.8.1 Задание для работы:

1.Методы оценки защиты.
2.Средства контроля защиты.

3.8.2 Краткое описание проводимого занятия:

1.Методы оценки защиты.

Понятие системности заключается не просто в создании соответствующих механизмов защиты, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла ИС. При этом все средства, методы и мероприятия, используемые для защиты информации объединяются в единый целостный механизм - систему защиты.
К сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания у пользователей современных ИС.
Сегодня специалисты из самых разных областей знаний, так или иначе, вынуждены заниматься вопросами обеспечения информационной безопасности. Это обусловлено тем, что в ближайшие лет сто нам придется жить в обществе (среде) информационных технологий, куда перекочуют все социальные проблемы человечества, в том числе и вопросы безопасности:
Каждый из указанных специалистов по-своему решает задачу обеспечения информационной безопасности и применяет свои способы и методы для достижения заданных целей. Самое интересное, что при этом каждый из них в своем конкретном случае находит свои совершенно правильные решения. Однако, как показывает практика, совокупность таких правильных решений не дает в сумме положительного результата - система безопасности в общем и целом работает не эффективно.
Если собрать всех специалистов вместе, то при наличии у каждого из них огромного опыта и знаний, создать СИСТЕМУ информационной безопасности зачастую так и не удается. Разговаривая об одних и тех же вещах, специалисты зачастую не понимают друг друга поскольку у каждого из них свой подход, своя модель представления системы защиты информации. Такое положение дел обусловлено отсутствием системного подхода, который определил бы взаимные связи (отношения) между существующими понятиями, определениями, принципами, способами и механизмами защиты:
Постановка задачи.
Одиннадцать отдельно взятых футболистов (даже очень хороших) не составляют команду до тех пор, пока на основе заданных целей не будет отработано взаимодействие каждого с каждым. Аналогично СЗИ лишь тогда станет СИСТЕМОЙ, когда будут установлены логические связи между всеми ее составляющими.
Как же организовать такое взаимодействие? В футболе команды проводят регулярные тренировки, определяя роль, место и задачи каждого игрока. Качество или эффективность команд оценивается по игре в матчах, результаты которых заносятся в турнирную таблицу. Таким образом, после проведения всех встреч команд (каждой с каждой), можно сделать вывод об уровне состояния мастерства как команды в целом, так и отдельных ее

игроков. Побеждает тот, у кого наиболее четко организовано взаимодействие:
Выражаясь терминами современного бизнеса, для решения вопросов взаимодействия нужно перейти от "чисто" технического на "конкретно" логический уровень представления процессов создания и функционирования СИСТЕМ защиты информации.
Хотелось бы, чтобы все специалисты, считающие себя профессионалами в информационных технологиях, поднялись чуть выше "багов" и "кряков" и уже сейчас задумались над тем как их знания и опыт будут логически увязаны со знаниями и опытом других специалистов.
В "строгой научной постановке" задача автора состоит в предоставлении пользователям вспомогательного инструмента "елки" - (модели СЗИ), а задача читателя (пользователя) - украсить эту "елку" новогодними игрушками - (своими знаниями и решениями). Даже если "игрушек" пока еще нет, наличие "елки" поможет выбрать и приобрести нужные "украшения".
Конечный результат работы (степень красоты елки) зависит от ваших желаний, способностей и возможностей. У кого-то получится хорошо, у кого-то - не совсем: Но это естественный процесс развития, приобретения знаний и опыта.
Кстати, оценить красоту елки (эффективность системы защиты) весьма проблематично, поскольку у каждого из нас свои требования и вкусы, о которых, как известно, не спорят, особенно с руководством.
Таким образом, многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. В то же время, большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том как же приступить к созданию системы защиты информации для конкретной информационной системы, с учетом присущих ей особенностей и условий функционирования. Как сказал классик юмора: ":многообразие ваших вопросов порождает многообразие наших ответов:"
Возникает вопрос: можно ли сформировать такой подход к созданию систем защиты информации, который объединил бы в нечто единое целое усилия, знания и опыт различных специалистов? При этом желательно что бы указанный подход был универсальным, простым, понятным и позволял бы в одинаковой степени удовлетворить любые вкусы (требования) гурманов информационной безопасности?
Модель представления системы информационной безопасности.
Практическая задача обеспечения информационной безопасности состоит в разработке модели представления системы (процессов) ИБ, которая на основе научно-методического аппарата, позволяла бы решать задачи создания, использования и оценки эффективности СЗИ для проектируемых и существующих уникальных ИС. Что понимается под моделью СЗИ? Насколько реально создать такую модель? В упрощенном виде модель СЗИ представлена на Рис.1.

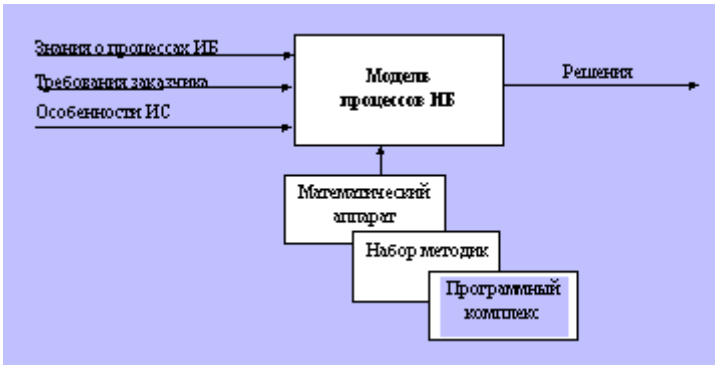


Рис.1. Модель СЗИ

Основной задачей модели является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.
Специфическими особенностями решения задачи создания систем защиты являются:
· неполнота и неопределенность исходной информации о составе ИС и характерных угрозах;
· многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей (требований) СЗИ;
· наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ;
· невозможность применения классических методов оптимизации.

2.Средства контроля защиты.

Средства защиты информации и **средства контроля защищенности** - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну и сведений конфиденциального характера, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.
Компанией ФГУП «НПП «Гамма» осуществляется разработка и дальнейшая **поставка средств защиты** информации, а именно:

- Разработка, производство, реализация и эксплуатация шифровальных криптографических средств защиты информации, используемых в системах обработки конфиденциальной информации (персональные данные, коммерческая, банковская, служебная тайна и пр.) и информации, содержащей сведения, составляющие государственную тайну органов государственной власти, различных ведомств, государственных и коммерческих структур;
- Разработка, производство, реализация, эксплуатация и **поставка средств защиты** информации (генераторы шума, фильтры помехоподавляющие, средства доверенной загрузки, однонаправленные шлюзы, межсетевые экраны, системы обнаружения компьютерных атак и пр.) используемых в системах обработки конфиденциальной информации (персональные данные, коммерческая, банковская, служебная тайна и пр.) и информации содержащей сведения, составляющие государственную тайну органов государственной власти, различных ведомств, государственных и коммерческих структур;
- Разработка, производство, реализация и эксплуатация средств контроля защищенности. **Средства контроля защищенности** — это программно-аппаратные комплексы измерений и расчетов от утечки информации за счет ПЭМИН, АЭП и ВЧН, недостаточности звуко- и виброизолирующих свойств, ограждающих конструкций и коммуникаций систем жизнеобеспечения и пр., конфиденциальной информации (персональные данные, коммерческая, банковская, служебная тайна и пр.) и информации, содержащей сведения, оставляющие государственную тайну органов государственной власти, различных ведомств, государственных и коммерческих структур.

3.8.3 Результаты и выводы:

В ходе работы студенты ознакомились с методами оценки защищенности информации от утечки по техническим каналам.

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ СЕМИНАРСКИХ ЗАНЯТИЙ

Семинарские занятия РУП не предусмотрены.