СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационная безопасность – это стратегический инструмент развития бизнеса для большинства современных компаний. Потребности бизнеса в защите конфиденциальной информации бизнеса в целом растут пропорционально росту угроз безопасности.

Один из источников значимой информации компании - это совещания, где представляются материалы по планам и результатам работы. Наличие большого числа людей и значительные размеры помещений ставят перед организациями задачу сохранения коммерческой тайны. С развитием рыночных отношений большинство средств ранее находившихся под контролем спецслужб стали доступными для частного сектора и вопрос их получения связан только с рыночной стоимостью и умением их использовать.

Защита информации при проведении совещаний с участием представителей сторонних компаний имеет актуальную важность и основные задачи для обеспечения информационной безопасности - это своевременная локализация и выявление возможных технических каналов утечки информации и объясняется актуальность выбранной темы дипломной работы.

Цель работы является обеспечение защиты информации в переговорной комнате.

Предмет: информация, возникающая в процессе проведения переговоров в переговорной комнате.

В современных условиях информация играет решающую роль, как в процессе экономического развития, так и в ходе конкурентной борьбы на внутреннем и внешнем рынках.

Успешное функционирование и развитие предприятий все больше зависит от совершенствования их деятельности в области обеспечения информационной безопасности в сфере производства, бизнеса и предпринимательства.

Таким образом, каждый собственник информации стремится сохранить ее в тайне, создавая для этого систему защиты от несанкционированного доступа со стороны злоумышленников. Злоумышленником, в свою очередь, может быть лицо или организация, заинтересованные в получении возможности несанкционированного доступа к конфиденциальной информации, предпринимающие попытку такого доступа или совершившие его.

Совершенствование инженерно-технической защиты информации в помещение для проведения переговоров является одной из мер защиты информации в организации. Поскольку в переговорной комнате могут обсуждаться сведения, составляющие тайну организации или ее партнеров, которая является конфиденциальной.

Целью данной дипломной работы является разработка обеспечение комплексной системы защиты информации в переговорной комнате. Отсюда вытекают следующие задачи:

- исследовать предметную область в соответствии с темой;
- создание проекта безопасности комнаты переговоров;
- провести анализ основных мер по обеспечению защиты информации в переговорной комнате.

ГЛАВА 1. ХАРАКТЕРИСТИКА ОСНОВНЫХ ПОТЕНЦИАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ И КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ПЕРЕГОВОРОВ И СОВЕЩАНИЙ

1.1 Безопасность в организации

Защите подлежат:

-Помещения. В первую очередь закрытию подлежат те помещения, в которых находятся ресурсы (информационные, материальные, людские), потеря, порча, модификация или разглашение которых может привести к полной или частичной остановке производственного цикла получения основной статьи доходов предприятия. К закрываемым помещениям относят также те, в которых есть ценности, потеря которых болезненно отразится на основном производстве, хотя и не приведет к фатальным последствиям, а также помещения, где находится оборудование, которое трудно восполнить или имеющее высокую стоимость. Сама фирма является ценностью, поэтому не забудьте включить в зону охраны всю ее территорию.

-Группы лиц.

Традиционно выделяются три главные группы лиц - это сотрудники вашей организации, посетители и злоумышленники (вместе с первыми и вторыми).

Очень часто выделяется большее число групп лиц, например, осуществляется деление сотрудников на “командный состав” и “рядовых сотрудников”, постоянных работников и временных, а посетителей разделить на разовых, временных и постоянных.

- Угрозы.

Следующий этап работы является анализ возможных угроз. Даже поверхностная оценка позволяет найти меры, которые необходимо принять для обеспечения безопасности, и оценить (в сравнении со стоимостью сберегаемых ценностей) расходы, которые позволительно понести.

Как правило, каждому помещению (приемная, вход, бухгалтерия, склад, кабинет руководителя, отделы, АСУ, производственная площадка, туалет, …) ставятся в соответствие потенциальные угрозы (хулиганство, воровство внешнее или внутреннее, установка средств прослушивания, доступ к вычислительным средствам, доступ к документами, архивам, выведение из строя оборудования, ...)

Согласно ГОСТу 350922-96, защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1.2 Человеческий фактор в обеспечении ИБ

Преступления, в том числе в информационной сфере, совершаются людьми. Большинство систем не может нормально функционировать без участия человека. Пользователь системы, с одной стороны, - ее необходимый элемент, а с другой - он же является причиной и движущей силой нарушения или преступления. Вопросы безопасности систем (компьютерных в том числе), таким образом, большей частью есть вопросы человеческих отношений и человеческого поведения.

Особенно актуально это в сфере информационной безопасности, т.к. утечка информации в подавляющем большинстве случаев происходит по вине сотрудников предприятия.

Можно выделять четыре основные причины нарушений: безответственность, самоутверждение, месть и корыстный интерес пользователей (персонала).

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия,

не связанные, тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Маловероятно, чтобы разработчики системы защиты могли предусмотреть все такие ситуации. Более того, во многих случаях система в принципе не может предотвратить подобные нарушения (например, случайное уничтожение своего собственного набора данных).

Даже лучшая система защиты будет скомпрометирована, если она неграмотно настроена. Наряду с неподготовленностью пользователей к точному соблюдению мер защиты, это обстоятельство может сделать систему уязвимой к этому виду нарушений.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру "пользователь против системы" ради самоутверждения либо в собственных глазах, либо в глазах коллег. Хотя намерения могут быть и безвредными, эксплуатация ресурсов АСОИБ считается нарушением политики безопасности.

Пользователи с более серьезными намерениями могут найти конфиденциальные данные, попытаться испортить или уничтожить их при этом. Такой вид нарушения называется зондированием системы. Большинство систем имеет ряд средств противодействия подобным "шалостям". В случае необходимости администратор защиты использует их временно или постоянно.

Нарушение безопасности АБС может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в АБС информации. Даже если АБС имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно. Тот, кому успешно удалось

проникновение - очень квалифицирован и опасен. Проникновение - опаснейший вид нарушений, правда, он встречается чрезвычайно редко, так как требуют необычайного мастерства и упорства.

Как показывает практика, ущерб от каждого вида нарушений обратно пропорционален его частоте: чаще всего встречаются нарушения, вызванные халатностью и безответственностью, обычно ущерб от них незначителен и легко восполняется. Например, случайно уничтоженный набор данных можно восстановить, если сразу заметить ошибку. Если информация имеет важное значение, то необходимо хранить регулярно обновляемую резервную копию, тогда ущерб вообще практически незаметен.

Ущерб от зондирования системы может быть гораздо больше, но и вероятность его во много раз ниже. Для таких действий необходима достаточно высокая квалификация, отличное знание системы защиты и определенные психологические особенности. Наиболее характерным результатом зондирования системы является блокировка: пользователь в конце концов вводит АБС в состояние зависания, после чего администраторы и системные программисты должны тратить много времени для восстановления работоспособности системы.

Проникновение - наиболее редкий вид нарушений, но и наиболее опасный. Отличительной чертой проникновения обычно является определенная цель: доступ (чтение, модификация, уничтожение) к определенной информации, влияние на работоспособность системы, слежение за действиями других пользователей и др. Для выполнения подобных действий нарушитель должен обладать теми же качествами, что и для зондирования системы, только в усиленном варианте, а также иметь точно сформулированную цель.

В силу этих обстоятельств ущерб от проникновения может оказаться в принципе невосполнимым. Например, для банков это может быть полная или частичная модификация счетов с уничтожением журнала транзакций.

Таким образом, для организации надежной защиты необходимо четко отдавать себе отчет, от каких именно нарушений важнее всего избавиться, Для защиты от нарушений, вызванных халатностью нужна минимальная защита, для защиты от зондирования системы - более жесткая и самая жесткая вместе с постоянным контролем - от проникновения.

Целью таких действий должно служить одно - обеспечение работоспособности АБС в целом и ее системы защиты в частности.

Не будет преувеличением сказать, что проблема умышленных нарушений функционирования АБС различного назначения в настоящее время является одной из самых актуальных.

Под угрозой безопасности понимается потенциально возможное воздействие на автоматизированную систему обработки информации, которое может прямо или косвенно нанести урон пользователям или владельцам АБС. Приводимая ниже классификация охватывает только умышленные угрозы безопасности АБС.

Угрозы безопасности АБС можно классифицировать по следующим признакам:

По цели реализации угрозы.

Реализация той или иной угрозы безопасности АБС может преследовать следующие цели:

- нарушение конфиденциальности информации. Информация, хранимая и обрабатываемая в АБС, может иметь большую ценность для ее владельца. Ее использование другими лицами наносит значительный ущерб интересам владельца;

- нарушение целостности информации. Потеря целостности информации (полная или частичная, компрометация, дезинформация) - угроза близкая к ее раскрытию. Ценная информация может быть утрачена или обесценена путем ее несанкционированного удаления или модификации. Ущерб от таких действий может быть много больше, чем при нарушении конфиденциальности,

- нарушение (частичное или полное) работоспособности АБС (нарушение доступности). Вывод из строя или некорректное изменение режимов работы компонентов АБС, их модификация или подмена могут привести к получению неверных результатов, отказу АБС от потока информации или отказам при обслуживании. Отказ от потока информации означает непризнание одной из

взаимодействующих сторон факта передачи или приема сообщений. Имея в виду, что такие сообщения могут содержать важные донесения, заказы, финансовые согласования и т.п., ущерб в этом случае может быть весьма значительным. Так как диапазон услуг, предоставляемых современными АБС, весьма широк, отказ в обслуживании может существенно повлиять на работу пользователя.

По способу воздействия на объект атаки

При активном воздействии:

- непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа.

- воздействие на систему разрешений (в том числе захват привилегий). При этом способе несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом. Примером может служить захват привилегий, что позволяет затем беспрепятственно получить доступ к любому набору данных или программе.

При опосредованном воздействии (через других пользователей):

- "маскарад". В этом случае пользователь присваивает себе каким-либо образом полномочия другого пользователя, выдавая себя за него. При этом такие действия другому пользователю могут быть разрешены. Такие нарушения также называются симуляцией или моделированием.

- "использование вслепую". При таком способе воздействия один пользователь заставляет другого выполнить необходимые действия (которые для системы защиты не выглядят несанкционированными, ведь их выполняет пользователь, имеющий на это право), причем последний о них может и не подозревать. Для реализации этой угрозы может использоваться вирус (вирус выполняет необходимые действия и сообщает тому, кто его внедрил о результате).

Два последних способа, особенно "использование вслепую", чрезвычайно опасны. Для предотвращения подобных действий требуется постоянный контроль как со стороны администраторов и операторов за работой АБС в целом, так и со стороны пользователей за своими собственными наборами данных.

Обеспечение безопасности АБС в целом предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также попыток хищения, модификации, выведения из строя или разрушения ее компонентов. То есть защиту всех компонентов системы: оборудования, программного обеспечения, данных и персонала.

В этом смысле, защита информации от несанкционированного доступа является только частью общей проблемы обеспечения безопасности АБС, а борьбу следует вести не только с "несанкционированным доступом" (к информации), а шире, - с "несанкционированными действиями".

Обычно различают внешнюю и внутреннюю безопасность АБС. Внешняя безопасность включает защиту АБС от стихийных бедствий (пожар, наводнение и т.п.) и от проникновения злоумышленников извне с целями хищения, получения доступа к носителям информации или вывода системы из строя. Предметом внутренней безопасности является обеспечение надежной и корректной работы системы, целостности ее программ и данных.

Все усилия по обеспечению внутренней безопасности АБС фокусируются на создании надежных и удобных механизмов регламентации деятельности всех ее пользователей и обслуживающего персонала,

соблюдении установленной в организации дисциплины прямого или косвенного доступа к ресурсам системы и к информации.

Учитывая то обстоятельство, что основным предназначением АБС является переработка (сбор, хранение, обработка и выдача) информации, то проблема обеспечения безопасности информации является для АБС центральной.

Очевидно, что все они тесно связаны с безопасностью информации, поскольку, например, отказ в обслуживании клиента или несвоевременное предоставление пользователю хранящейся в АБС важной информации из-за неработоспособности этой системы по своим последствиям равноценны потере информации (несанкционированному ее уничтожению).

Обеспечение безопасности АБС в целом предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также попыток хищения, модификации, выведения из строя или разрушения ее компонентов. То есть защиту всех компонентов системы: оборудования, программного обеспечения, данных и персонала. В этом смысле, защита информации от несанкционированного доступа является только частью общей проблемы обеспечения безопасности АБС, а борьбу следует вести не только с "несанкционированным доступом" (к информации), а шире, - с "несанкционированными действиями".

Обычно различают внешнюю и внутреннюю безопасность. Внешняя безопасность включает защиту АБС от стихийных бедствий (пожар, наводнение и т.п.) и от проникновения злоумышленников извне с целями хищения, получения доступа к носителям информации или вывода системы из строя. Предметом внутренней безопасности является обеспечение надежной и корректной работы системы, целостности ее программ и данных.

Все усилия по обеспечению внутренней безопасности АБС фокусируются на создании надежных и удобных механизмов регламентации деятельности всех ее пользователей и обслуживающего персонала,

соблюдении установленной в организации дисциплины прямого или косвенного доступа к ресурсам системы и к информации.

Учитывая то обстоятельство, что основным предназначением АБС является переработка (сбор, хранение, обработка и выдача) информации, то проблема обеспечения безопасности информации является для АБС центральной.

Очевидно, что все они тесно связаны с безопасностью информации, поскольку, например, отказ в обслуживании клиента или несвоевременное предоставление пользователю хранящейся в АБС важной информации из-за неработоспособности этой системы по своим последствиям равноценны потере информации (несанкционированному ее уничтожению).

Объектом защиты в данной дипломной работы согласно Гост Р51275-99. об Объекте информатизации, то есть - это совокупность информационных средств и систем обработки информации, используемые в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещение или объектов, в которых они установлены или помещения и объекты, предназначенные ведения конфиденциальных переговоров. Будет являться Помещение состоящего из 1 компьютера и проектора для презентаций. Используется для проведения заседаний совета директоров. На компьютере содержатся данные относящиеся к коммерческой тайне.

Помещение находится в здании региона в региональном отделе автоматизированной системы управления, для проведения информационных заседаний и решения различных вопросов по отделу. Объект защищается на уровне Регионального отдела автоматизированной системы управления занимающийся деятельностью информационных ресурсов, поставке и настройке программного обеспечения ПК для пользователей различных предприятий. Данное помещение используется отделом для заседаний и советов по решению различных информационных вопросов в количестве 7 ответственных лиц заседания. Угроза безопасности информации -

совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными и непреднамеренными воздействиями на нее.

Определение перечня внутренних угроз

В реальности существует два вида угроз информационной безопасности:

Внутренняя:

- несанкционированный доступ в помещение;

-несанкционированный доступ к данным внутри корпоративной сети и данных ПК без ведома сотрудника;

- возможность записи информации на переносные устройства (флэш-накопители и т.п.);

- пересылка фотоснимков бумажных носителей и экранов мониторов с помощью мобильных телефонов и другими способами, через удаленный доступ к ПК;

- программные вирусы и «троянские» программы;

- незаконное скачивание и распространение за пределами предприятия лицензионных программ организации;

- не контролируемая электронная почта;

- вынос техники организации, без соответствующего документа;

- внос посторонней техники на территорию организации;

определение перечня внешних угроз

Внешняя:

- несанкционированный доступ из сети Интернет;

- снятие информации с кабельных систем (ЛВС и электропитания) при помощи технических средств;

- запись разговоров на расстоянии сквозь стены (окна, двери) и т. д.;

-несанкционированная установка, микрофонов в помещениях;

1.3 Современные методы решения задач мониторинга

Для создания надежной системы инженерно-технической защиты информации необходимо учитывать возможные каналы утечки информации.

– На основании проведенной оценки угроз для данного защищаемого помещения выявлены следующие актуальные каналы утечки информации:

– акустический канал– запись звука, подслушивание и прослушивание;

– оптический канал – визуальные методы, фотографирование, видео съемка, наблюдение;

– радиоэлектронный канал - копирование полей путем снятия индуктивных наводок;

– материально – вещественный канал — информация на бумаге или других физических носителях информации.

Возможные каналы утечки информации с объекта защиты представлены в таблице 1.3.1.

Таблица 1.3.1- Возможные каналы утечки информации с объекта защиты

Вид канала	Индикаторы
1	2
Оптический канал	Окно №1 со стороны офисного здания с парковочной площадкой
	Окно №2 со стороны офисного здания с парковочной площадкой
	Окно №3 со стороны многоэтажного жилого дома
	Окно №4 со стороны многоэтажного жилого дома

		Дверь в коридор
	Радиоэлектронный канал	Многоэтажный жилой дом
		Офисное здание с парковочной площадкой
		Телефон
		Розетки
		ПЭВМ
		Воздушная линия электропередачи
		Система оповещения
		Система пожарной сигнализации
	Акустический канал	Дверь
		Пол контролируемого помещения
		Стены помещения
		Батареи
		Окна контролируемого помещения
	Материально-вещественный канал	Документы на бумажных носителях
		Участник совещания
		Персонал предприятия
		Производственные отходы

Возможности утечки информации с совещания зависят от многих факторов, основными из которых являются:

- возможность организации злоумышленниками каналов утечки информации;

- условия обеспечения разведывательного контакта в рамках того или иного канала утечки информации.

Канал утечки информации представляет собой физический путь от источника коммерческой тайны к злоумышленнику (конкуренту), посредством которого может быть реализован несанкционированный доступ к ограниченным сведениям. Для установления канала утечки информации необходимы определенные энергетические, пространственные и временные условия и соответствующие технические средства восприятия и фиксации

информации. В качестве основных угроз безопасности информации во время проведения совещания выступают:

подслушивание и несанкционированная запись речевой информации с помощью закладных устройств, систем лазерного подслушивания, стетоскопов, диктофонов;

регистрация на неконтролируемой территории с помощью радиомикрофонов участниками, выполняющими агентурное задание;

перехват электромагнитных излучений при работе звукозаписывающих устройств и электроприборов.

Такие угрозы безопасности информации как модификация и уничтожение в данном случае не актуальны.

- Логи.

Лог – это текстовый файл, понятный даже новичку, в котором каждому событию соответствует одна строка с временем и некоторыми дополнительными сведениями. Для удобства пользователей лог-файлы часто группируются по датам, что облегчает поиск необходимых сведений.

У такого подхода есть множество недостатков. Например, обнаружение событий по постфактуму, а не в режиме реального времени. Конечно, обнаружение самого факта нарушения это уже хорошо, но в такой ситуации уже вряд ли можно будет возместить ущерб, который был причинен. Плюс ко всему здесь вся ответственность за обнаружение нарушений ИБ возлагается на человека, который, как известно, является самым слабым звеном в любой информационной системе.

- SPAN-порт.

SPAN – это коммутирующий порт для анализа, который является великолепным способом легко и без нарушения связи получить данные для анализа. По определению, SPAN-порт обычно указывает на возможность скопировать трафик с любого или со всех портов данных на один неиспользуемый порт, но, как правило, запрещает двунаправленный трафик на этот порт, чтобы защитить сеть от передачи обратного трафика.

Некоторые считают SPAN порт пассивным решением доступа к данным - но пассивный означает «не воздействующий», а зеркалирование (зеркальное копирование) оказывает некоторое воздействие на данные.

Зеркалирование меняет временные параметры взаимодействия кадров (увиденное и полученное – две разные вещи).

Spanning-алгоритм не рассматривался в качестве основной функции устройств, такой как коммутация или маршрутизация, таким образом приоритетом будет не spanning и если дублирование кадра становится проблемой, аппаратное устройство временно прекращает процесс SPAN.

Если скорость SPAN-порта станет чрезмерной, загруженные кадры теряются.

Для правильного зеркалирования от сетевого инженера требуется должным образом сконфигурировать коммутаторы, а для этого придется отвлечься от более серьёзных задач, выполняемых сетевым инженером, и часто конфигурация становится вопросом политики (постоянно возникающие разногласия между IT структурой, структурой безопасности и структурой соответствия требованиям.)

SPAN-порт отбрасывает все поврежденные пакеты или пакеты, размер которых меньше минимального, таким образом, не все кадры проходят.

Все эти события могут возникать в сети и пользователь не будет получать никаких уведомлений, так что нет гарантии, что будут представлена вся информация, необходимая для правильного анализа

Таким образом тот факт, что SPAN-порт в действительности не является пассивной технологией доступа к данным, и даже то, что он позволяет тестировать сеть без прерывания связи может стать проблемой для мониторинга.

Технология зеркалирования вполне жизнеспособна для определённых ситуаций, но с момента перехода на FDX Gigabit и 10 Gigabit сети и с требованиями просмотра всех кадров должна быть использована технология

«реального» доступа (taps), чтобы отвечать современным требованиям технологий

комплексного анализа и мониторинга. Если требований к технологии недостаточно, сетевые специалисты могут сфокусировать оборудование инфраструктуры на задачах коммутации и маршрутизации и не тратить ценные ресурсы и время на настройку SPAN портов или перемаршрутизацию доступа к данным.

- Ответвители сетевого трафика(TAP - агенты)

Ответвители сетевого трафика – альтернатива SPAN-портам в области сбора трафика. Ответвители – это устройства, подключенные в разрыв между коммутаторами, межсетевыми экранами и серверами. Ответвители имеют преимущества над SPAN-портами, в особенности потому, что позволяют трафику беспрепятственно перемещаться между сетевыми устройствами, пока они копируют его для целей мониторинга.

Ответвители – это постоянная точка видения сетевого трафика и будут обеспечивать целостность соединения, даже если питание на ответвителе будет отключено. Ответвитель копирует видимый им сетевой трафик без существенной задержки или потери пакетов между сетевыми устройствами. Поскольку ответвители подключаются последовательно, им не нужен порт на коммутаторе или маршрутизаторе.

Хотя ответвители трафика способны видеть больше информации, чем SPAN-порты, они не видят внутренний трафик коммутаторов. Большинство ответвителей не требуют настройки – они просто постоянно работают. Некоторые ответвители могут делать множество копий сетевого трафика; таким образом разные приборы видят один и тот же набор данных

Ответвители сетевого трафика бывают разными и работают на разных скоростях. Если необходимо предоставить нескольким приборам доступ к каналу, неудобно для каждого прибора использовать отдельный ответвитель. Это слишком удорожит процесс. Намного практичнее иметь один

ответвитель, воспроизводящий трафик на несколько портов для подключения устройств для мониторинга по необходимости или желанию.

В этом случае копии трафика поступают в канал один раз, минимизируя потерю оптического сигнала (если это волоконно-оптический ответвитель) и позволяя предоставить каждому прибору точную копию данных. Сегодня, когда безопасность сетей имеет важнейшее значение, сетевые ответвители оказываются надежнее SPAN-портов, поскольку порты мониторинга могут быть однонаправленными и невидимыми для других сетевых компонентов.

При установке ответвителей соединение между сетевыми устройствами необходимо прервать (отключить), но после установки оно может работать непрерывно.

Одно устройство для анализа сети может видеть множество сетевых сегментов, используя ответвитель трафика, агрегирующий данные из этих сегментов. Экономия, связанная с необходимостью в меньшем количестве зондов для анализа сети, позволит быстро окупить затраты на ответвитель сетевого трафика. Ответвители трафика используются в любых сетях, где необходима 100% видимость и работоспособность – от самых важных и крупных до самых небольших

1.4 Постановка задачи. Общие принципы настройки механизмов защиты

Как уже отмечалось выше, настройка механизмов защиты - дело сугубо индивидуальное для каждой системы и даже для каждой задачи. Поэтому дать ее подробное описание довольно трудно. Однако существуют общие принципы, которых следует придерживаться, чтобы облегчить себе работу, так как они проверены практикой. Рассмотрим их:

Группирование.

Это объединение множества субъектов под одним групповым именем; всем субъектам, принадлежащим одной группе, предоставляются равные права. Принципы объединения пользователей в группы могут быть самые разные: одинаковый характер вычислений, работа над совместным проектом и т.д. При этом один и тот же субъект может входить в несколько различных групп, и, соответственно, иметь различные права по отношению к одному и тому же объекту.

Механизм группирования может быть иерархическим. Это означает, что каждый субъект является членом нескольких групп, упорядоченных по отношению "быть подмножеством". Контроль за состоянием групп очень важен, поскольку члены одной группы имеют доступ к большому числу объектов, что не способствует их безопасности.

Правила умолчания.

Большое внимание при назначении привилегий следует уделять правилам умолчания, принятым в данных средствах защиты; это необходимо для соблюдения политики безопасности. Во многих системах, например, субъект, создавший объект и являющийся его владельцем, по умолчанию получает все права на него.

Кроме того, он может эти права передавать кому-либо. В различных средствах защиты используются свои правила умолчания, однако принципы назначения привилегий по умолчанию в большинстве систем одни и те же. Корректное использование правил умолчания способствуют поддержанию целостности политики безопасности.

Минимум привилегий.

Это один из основополагающих принципов реализации любой политики безопасности, используемый повсеместно. Каждый пользователь и процесс должен иметь минимальное число привилегий, необходимых для работы. Определение числа привилегий для всех пользователей, с одной стороны, позволяющих осуществлять быстрый доступ ко всем необходимым для работы объектам, а, с другой, - запрещающих доступ к чужим объектам -

проблема достаточно сложная. От ее решения во многом зависит корректность реализации политики безопасности.

Принцип "надо знать".

Этот принцип во многом схож с предыдущим. Согласно ему, полномочия пользователей назначаются согласно их обязанностям. Доступ разрешен только к той информации, которая необходима им для работы. Согласно принципу, пользователь должен знать обо всех доступных ему ресурсах. В том случае, если пользователь не знает о них, такие ресурсы должны быть отключены.

Объединение критичной информации.

Во многих системах сбор, хранение и обработка информации одного уровня производится в одном месте (узле сети, устройстве, каталоге). Это связано с тем, что проще защитить одним и тем же способом большой массив информации, чем организовать индивидуальную защиту для каждого набора данных. Для реализации этого принципа могут быть разработаны специальные программы, управляющие обработкой таких наборов данных. Это будет простейший способ построения защищенных областей.

Иерархия привилегий.

Контроль объектов системы может иметь иерархическую организацию. Такая организация принята в большинстве коммерческих систем. При этом схема контроля имеет вид дерева, в котором узлы - субъекты системы, ребра - право

контроля привилегий согласно иерархии, корень - администратор системы, имеющий право изменять привилегии любого пользователя. Узлами нижележащих уровней являются администраторы подсистем, имеющие права изменять привилегии пользователей этих подсистем (в их роли могут выступать руководители организаций, отделов). Листьями дерева являются все пользователи системы.

Вообще говоря, субъект, стоящий в корне любого поддерева, имеет право изменять защиту любого субъекта, принадлежащего этому поддереву.

Достоинство такой структуры - точное копирование схемы организации, которую обслуживает АБС. Поэтому легко составить множество субъектов, имеющих право контролировать данный объект. Недостаток иерархии привилегий - сложность управления доступом при большом количестве субъектов и объектов, а также возможность получения доступа администратора системы (как высшего по иерархии) к любому набору данных.

Привилегии владельца.

При таком контроле каждому объекту соответствует единственный субъект с исключительным правом контроля объекта - владелец. Как правило, это его создатель. Владелец обладает всеми разрешенными для этого типа данных правами на объект, может разрешать доступ любому другому субъекту, но не имеет права никому передать привилегию на корректировку защиты.

Однако такое ограничение не касается администраторов системы - они имеют право изменять защиту любых объектов. Главным недостатком принципа привилегий владельца является то, что при обращении к объекту, пользователь должен предварительно получить разрешение у владельца (или администратора). Это может приводить к сложностям в работе (например; при отсутствии владельца или просто нежелании его разрешить доступ). Поэтому такой принцип обычно используется при защите личных объектов пользователей.

Свободная передача привилегий.

При такой схеме субъект, создавший объект, может передать любые права

на него любому другому субъекту. Тот, в свою очередь, может передать все эти права другому субъекту. Естественно, при этом возникают большие трудности в определении круга субъектов, имеющих в данный момент доступ к объекту (права на объект могут распространяться очень

быстро и так же быстро исчезать), и поэтому такой объект легко подвергнуть несанкционированной обработке.

В силу этих обстоятельств подобная схема применяется достаточно редко - в основном в исследовательских группах, работающих над одним проектом (когда все имеющие доступ к объекту заинтересованы в его содержимом).

В чистом виде рассмотренные принципы реализации политики безопасности применяются редко. Обычно используются их различные комбинации. Ограничение доступа к объектам в ОС включает в себя ограничение доступа к некоторым системным возможностям, например, ряду команд, программам и т.д., если при использовании их нарушается политика безопасности.

Вообще набор полномочий каждого пользователя должен быть тщательно продуман, исключены возможные противоречия и дублирования, поскольку большое количество нарушений происходит именно из-за этого. Может произойти утечка информации без нарушения защиты, если плохо была спроектирована или реализована политика безопасности.

Недостатки стандартных способов обеспечения безопасности БД:

Использование стандартных способов обеспечения безопасности неэффективно по следующим причинам:используемые механизмы шифрования требуют серьезных изменений в базах данных и бизнес-приложениях, кроме того, они не защищают информацию от несанкционированных действий привилегированных пользователей, работающих с базами данных через бизнес-приложенияштатные средства журналирования СУБД не способны охватить все операции с данными (например, операцию чтения) штатные средства СУБД не идентифицируют конечных пользователей бизнес-приложений при работе с базой данных через пул соединений («connectionpool»)используемые SIEM-решения (Security Informationand Event Management) основаны на штатных средствах

журналирования СУБД, к тому же такие системы ориентированны только на анализ данных о СУБД.

Рассмотрим наиболее важные моменты в организации мониторинга обращений к БД.

Инженерно-техническая защита информации - одна из основных составляющих комплекса мер по защите информации, составляющей государственную, коммерческую и личную тайну. Этот комплекс включает нормативно-правовые документы, организационные и технические меры, направленные на обеспечение безопасности секретной и конфиденциальной информации.

Инженерно-техническая защита информации представляет собой достаточно быстро развивающуюся область науки и техники на стыке теории систем, физики, оптики, акустики, радиоэлектроники, радиотехники, электро- и радиоизмерений и других дисциплин. Круг вопросов, которыми вынуждена заниматься инженерно-техническая защита, широк, и обусловлен многообразием источников и носителей информации, способов и средств её добывания, а, следовательно, и защиты.

Основным направлением инженерно-техническая защита информациияявляется противодействие средствам технической разведки и формирования рубежей охраны территории, зданий, помещений, оборудования, с помощью комплексов технических средств. По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

Физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий.

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа-выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Эти средства (техническая защита информации) применяются для решения следующих задач:

- охрана территории предприятия и наблюдение за ней;
- охрана зданий, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещения.
- Аппаратные средства защиты информации — это различные технические устройства, системы и сооружения (техническая защита информации), предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.

Использование аппаратных средств защиты информации позволяет решать следующие задачи:

- проведение специальных исследований технических средств на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие НСД (несанкционированному доступу) к источникам конфиденциальной информации и другим действиям.
- Программные средства. Программная защита информации — это система специальных программ, реализующих функции защиты информации.

Выделяют следующие направления использования программ для обеспечения безопасности конфиденциальной информации:

- защита информации от несанкционированного доступа;
- защита информации от копирования;
- защита информации от вирусов;
- программная защита каналов связи

Криптографические средства — это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Основные направления использования криптографических методов — передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

ГЛАВА 2 ХРАНЕНИЯ И ОБРАБОТКА ДАННЫХ АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ И ОПИСАНИЕ ФУНКЦИЙ СИСТЕМ

2.1 Мониторинг привилегированных пользователей

Из факторов, влияющих на эффективность инженерно-технической защиты информации, ее методы должны обеспечить реализацию следующих направлений инженерно-технической защиты информации:

предотвращение и нейтрализацию преднамеренных и случайных воздействий на источник информации;

скрытие информации и ее носителей от органа разведки (злоумышленника) на всех этапах добывания информации.

Кроме того, учитывая, что для добывания информации злоумышленник может использовать различные специальные средства (закладные устройства, диктофоны и др.), третье направление включает методы обнаружения, локализации и уничтожения и этих средств, а также подавления их сигналов.

Первое направление объединяют методы, при реализации которых:

- затрудняется движение злоумышленника или распространение стихийных сил к источнику информации;
- обнаруживается вторжение злоумышленника или стихийных сил в контролируемую зону и их нейтрализация.

Затруднение движения источников угроз воздействия к источникам информации обеспечивается в рамках направления, называемого физической защитой. Физическая защита обеспечивается методами инженерной защиты и технической охраны. Инженерная защита создается за счет использования естественных и искусственных преград на маршрутах возможного распространения источников угроз воздействия.

Искусственные преграды создаются с помощью различных инженерных конструкций, основными из которых являются заборы, ворота, двери, стены, межэтажные перекрытия, окна, шкафы, ящики столов, сейфы, хранилища. Так как любые естественные и искусственные преграды могут быть преодолены, то для

обеспечения надежной защиты информации, как и иных материальных ценностей, необходимы методы обнаружения вторжений в контролируемые зоны и их нейтрализации.

Эти методы называются технической охраной объектов защиты. Под объектами защиты понимаются как люди и материальные ценности, так и носители информации, локализованные в пространстве, К таким носителям относятся бумага, машинные носители, фото и кино пленка, продукция, материалы и т. д., то есть все, что имеет четкие размеры и вес.

Носители информации в виде электромагнитных и акустических полей, электрического тока не имеют четких границ, поэтому для их защиты применяется метод скрытия информации.

Скрытие информации предусматривает такие изменения структуры и энергии носителей, при которых злоумышленник не может непосредственно или с помощью технических средств выделить информацию с качеством, достаточным для использования ее в собственных интересах.

Различают информационное и энергетическое скрытие. Информационное скрытие достигается изменением или созданием ложного информационного портрета семантического сообщения, физического объекта или сигнала

Информационным портретом можно назвать совокупность элементов и связей между ними, отображающих смысл сообщения (речевого или данных), признаки объекта или сигнала. Элементами дискретного семантического сообщения, например, являются буквы, цифры или другие знаки, а связи между ними определяют их последовательность.

Информационными портретами объектов наблюдения, сигналов и веществ являются их эталонные признаковые структуры.

Возможны следующие способы изменения информационного портрета:

– удаление части элементов и связен, образующих информационный узел (наиболее информативную часть) портрета;

– изменение части элементов информационного портрета при сохранении

– неизменности связей между оставшимися элементами;

– удаление или изменение связей между элементами информационного портрета при сохранении их количества.

Другой метод информационного скрытия заключается в трансформации исходного информационного портрета в новый, соответствующий ложной семантической информации или ложной признаковой структуре, и "навязывании" нового портрета органу разведки или злоумышленнику. Такой метод защиты называется дезинформированием.

Принципиальное отличие информационного скрытия путем изменения информационного портрета от дезинформирования состоит в том, что первый метод направлен на затруднение обнаружения объекта с информацией среди других объектов (фона), а второй - на создании на этом фоне признаков ложного объекта.

Дезинформирование относится к числу наиболее эффективных способов защиты информации по следующим причинам:

– создает у владельца защищаемой информации запас времени, обусловленный проверкой разведкой достоверности полученной информации;

– последствия принятых конкурентом на основе ложной информации решений могут быть для него худшими по сравнению с решениями, принимаемыми при отсутствии добываемой информации.

Однако этот метод защиты практически сложно реализовать. Основная проблема заключается в обеспечении достоверности ложного информационного портрета.

Эффективным методом скрытия информации является энергетическое скрытие. Оно заключается в применении способов и средств защиты информации, исключающих или затрудняющих выполнение энергетического условия разведывательного контакта.

Энергетическое скрытие достигается уменьшением отношения энергии (мощности) сигналов, т.е. носителей (электромагнитного или акустического полей и электрического тока) с информацией, и помех.

Уменьшение отношения сигнал/помеха возможно двумя методами:

- снижением мощности сигнала;

- увеличением мощности помехи на входе приемника.

Воздействие помех приводит к изменению информационных параметров носителей: амплитуды, частоты, фазы. Если носителем информации является амплитудно-модулированная электромагнитная волна, а в среде распространения канала присутствует помеха в виде электромагнитной волны, имеющая одинаковую с носителем частоту, но случайную амплитуду и фазу, то происходит интерференция этих волн.

В результате этого значения информационного параметра (амплитуды суммарного сигнала) случайным образом изменяются и информация искажается. Чем меньше отношение мощностей, а следовательно, амплитуд, сигнала и помехи, тем значительнее значения амплитуды суммарного сигнала будут отличаться от исходных (устанавливаемых при модуляции) и тем больше будет искажаться информация.

Атмосферные и промышленные помехи, которые постоянно присутствуют в среде распространения носителя информации, оказывают наибольшее влияние на амплитуду сигнала, в меньшей степени - на его частоту. Но ЧМ-сигналы имеют более широкий спектр частот. Поэтому в функциональных каналах, допускающих передачу более широкополосных

сигналов, например, в УКВ диапазоне, передачу информации осуществляют, как правило ЧМ сигналами как более помехоустойчивыми, а в узкополосных ДВ, СВ и КВ диапазонах - АМ сигналами.

В общем случае качество принимаемой информации ухудшается с уменьшением отношения сигнал/помеха. Характер зависимости качества принимаемой информации от отношения сигнал/помеха отличается для

различных видов информации (аналоговой, дискретной), носителей и помех, способов записи на носитель (вида модуляции), параметров средств приема и обработки сигналов.

Наиболее жесткие требования к качеству информации предъявляются при передаче данных (межмашинном обмене): вероятность ошибки знака по плановым задачам, задачам статистического и бухгалтерского учета оценивается порядка - 10-5-10-6, но денежным данным 10-8-10-9. Для сравнения, в телефонных каналах хорошая слоговая разборчивость речи обеспечивается при 60-80%, т.е. требования к качеству принимаемой информации существенно менее жесткие.

Это различие обусловлено избыточностью речи, которая позволяет при пропуске отдельных звуков и даже слогов восстанавливать речевое сообщение. Вероятность ошибки знака 10-5 достигается при его передаче двоичным АМ сигналом и отношении мощности сигнала к мощности флуктуационного шума на входе приемника приблизительно 20, при передаче ЧМ сигналом - около 10.

Для обеспечения разборчивости речи порядка 85% превышение амплитуды сигнала над шумом должно составлять около 10 дБ, для получения удовлетворительного качества факсимильного изображения - приблизительно 35 дБ, качественного телевизионного изображения - более 40 дБ.

В общем случае при уменьшении отношения сигнал/помеха до единицы и менее качество информации настолько ухудшается, что она не может практически использоваться. Доля конкретных видов информации и

модуляции сигнала существуют граничные значения отношения сигнал/помеха, ниже которых обеспечивается энергетическое скрытие информации.

Так как разведывательный приемник в принципе может быть приближен к границам контролируемой зоны организации, то значения отношения сигнал/помеха измеряются, прежде всего, на границе этой зоны. Обеспечение на границе зоны значений отношения сигнал/помеха ниже минимально допустимой величины гарантирует безопасность защищаемой информации от утечки за пределами контролируемой зоны.

В компании существуют правила доступа привилегированных пользователей к критической информации. К таким пользователям относятся администраторы баз данных, разработчики программного обеспечения, сотрудники служб HelpDesk и другие сотрудники, должностные обязанности которых предусматривают неограниченный доступ к критической информации, хранящейся в базах данных компании.

Администраторы баз данных, кроме полного доступа к информации, также имеют доступ к структурам баз данных, в том числе к добавлению/удалению критических таблиц (DDL-команды) и управлению доступами к базам данных (DCL-команды). Для работы привилегированные пользователи, как правило, используют несколько учетных записей СУБД, это еще больше усложняет процесс контроля их действий.

Существующие в компании политики доступа, как правило, носят только формальный характер, а механизмы мониторинга на данный момент не являются эффективными. В тоже время, для соответствия требованиям таких стандартов как PCI-DSS, 152-ФЗ необходимо отслеживать все действия привилегированных пользователей.

Мониторинг привилегированных пользователей в компании обеспечит:

конфиденциальность информации – только авторизованные пользователи будут иметь доступ к критическим данным и использовать его только в рамках своих служебных обязанностейцелостность данных – все

изменения структур баз данных и критических параметров (разрешения, права доступа и пр.) не будут выходить за рамки установленных правил

Мониторинг привилегированных пользователей также играет важную роль в защите от внешних атак, так как очень часто цель атаки – получение привилегированных прав доступа. Например, злоумышленник из удаленного расположения получил доступ к критической информации. Для выявления несанкционированного доступа необходимо проанализировать о нем дополнительную информацию – расположение. Штатные средства СУБД не позволяют сделать это.

Многозвенные распределенные корпоративные приложения, такие как Oracle, SAP хранят наиболее важную критическую информацию компании (финансовые данные, данные о клиентах, сотрудниках и пр.).

Обеспечить эффективную защиту таких приложений затруднительно из-за большого числа способов доступа – «толстые» клиенты, VPN-доступ, WEB-доступ. Дополнительные трудности в защите создает многозвенная архитектура, при использовании которой скрываются имена конечных пользователей бизнес-приложений, так как все соединения производятся через «пул соединений» («connectionpool»).

При таком способе доступа все данные из баз данных получаются посредством нескольких учетных записей для бизнес-приложения. Как следствие, очень сложно сопоставить транзакции в базе данных с определенными именами сотрудников (пользователями бизнес-приложений).

Основная цель мониторинга бизнес-приложений – выявление аномальных действий, производимых в базе данных через корпоративные приложения.

Отслеживая все связи между бизнес-приложениями и базой данных на сетевом уровне и уровне операционных систем, нужно обеспечить гарантированное определение имен пользователей бизнес-приложений (ID). Полученные данные должны быть использованы для составления отчетов, формирования данных для аудита, оповещений, корреляции данных.

Основные факты:

- сопоставление конечных пользователей бизнес-приложений с конкретными запросами к базам данных
- детализированная отчетность по всем действиям пользователей бизнес-приложений, включая отчеты по личным данным пользователей (например, роли и местоположения)
- срабатывание правил политик безопасности и оповещений в режиме реального времени при наступлении заданных событий (например, в случае попытки просмотра таблицы с критической информацией)

Предотвращение внедрения вредоносного SQL-кода.

Предотвращение атак должно производиться с помощью правил политик безопасности, контроль которых производится в реальном времени:

Политики доступа, позволяющие выявлять аномальные действия на основе сравнения с установленным «базовым» состоянием. Например, SQL атака обычно состоит из команд, направленных на получение доступа к базе данных, при этом используемые SQL-команды нетипичны для бизнес-приложений и бизнес-процессов компании.

Политики исключительных ситуаций, основанные на пороговых значениях (например, предельное число неудачных входов в базу данных или SQL ошибок). Анализ SQL ошибок может показать, что злоумышленник пытается найти имена таблиц с критическими данными, используя команды с необходимыми параметрами (например, “Credit_Card_Num” или “CC_Num"). При этом в случае перебора имен существующих таблиц, SQL ошибка не будет сформирована. Нужно выявлять такие события.

Политики исключительных ситуаций, основанные на специфических SQL ошибках (например, «ORA-00903:Invalidtablename» или «ORA-00942: Tableorviewdoesnotexist»). Анализ таких ошибок позволит выявить и пресечь атаки злоумышленников.

Политики выгрузки информации, обеспечивающие анализ всех выгружаемых данных. Могут отслеживаться как все выгрузки критических

данных (например, все запросы номеров кредитных карт), так и анализ количества выгружаемых данных (например, разовая выгрузка большого объема данных).

2.2 Аудит и отчетность

Для обеспечения проактивного контроля, анализ и фильтрация данных аудита должна производится в режиме реального времени. Должны формироваться отчеты. Они должны избавить от необходимости вручную разбирать и анализировать огромные неконсолидированные журналы событий. Обеспечивая полную прозрачность всех активностей СУБД (доступы к критическим таблицам, изменение привилегий, структуры данных, доступы во внерабочее время или из неавторизованных приложений и пр.), отчеты будут служить доказательством соответствия требованиям стандартов.

В идеале, нужно отслеживать и фиксировать активности всех пользователей, работающих с данными, в том числе привилегированных пользователей, пользователей бизнес-приложений, администраторов баз данных (DBA), напрямую работающих с данными, разработчиков, а также системных процессов.

Степень детализации собираемой информации зависит от требований по безопасности, установленных в компании.

С помощью отчетов нужно отслеживать:

- различные исключения, например, ошибки SQL или неудачные попытки входа в бизнес-системы
- команды, изменяющие структуры баз данных - DDL (create, drop, alter)
- запросы на выборку данных (select)
- команды DML (insert, update, delete), включая команды со связанными переменными(bind variables)

– команды DCL (grant, revoke), управляющие учетными записями, их ролями и правами доступа

– хранимые процедуры, созданные на языках, специфичных для платформы СУБД (PL/SQL у Oracle) Правила аудита могут применяться к отдельным объектам баз данных (например, к столбцам). Нужно собирать информацию о:

– доступах к данным: вся клиент-серверная информация (IP адреса, протоколы, учетные записи операционных систем и пр.); информация о сессиях СУБД (время, имена баз данных), бизнес-приложениях, а также SQL-параметры (операторы, команды, объекты, поля, значения и пр.)

– исключениях: все исключения и связанная с ними информация от СУБД

– нарушениях политик безопасности: информация о том, почему сработала политика - на какое действие какого пользователя

– отправленных оповещениях: информация обо всех оповещениях

– Политики безопасности могут быть применены к любому объекту, в том числе к пользователям, рабочим станциям, приложениям, параметрам доступа (например, время, используемые команды, объекты доступа) и пр. Формируемые политики можно применять также для связанных элементов (например, имя и номер кредитной карты), которые объединяются в единый набор и рассматриваются как единое целое.

2.3 Программное обеспечение Защита +

Защита + - наиболее широко используемое решение для контроля критических данных и предотвращения утечек информации.

Продукты Защита + пресекают попытки несанкционированного доступа и подозрительные действия привилегированных пользователей, пользователей бизнес-приложений, бизнес-систем собственной разработки, а также потенциальных мошенников.

Защита + – комплексное решение для контроля баз данных и бизнес-приложений. Защита + поддерживает все наиболее распространенные платформы СУБД и бизнес-приложения, работающие на основе крупнейших операционных система и серверов приложений.

Информация о состоянии контролируемых объектов агрегируется и нормализуется в едином хранилище данных аудита Защита +. Такой метод позволяет организовать единую систему контроля, которая обеспечивает формирование единой отчетности, расследование инцидентов и управление доступами.

Управление настройками программно-аппаратного комплекса Защита + (политики, отчеты, процессы контроля соответствия и т.п.) производится из единой WEB-консоли.

Для хранения данных аудита Защита + использует запатентованные средства, эффективность которых намного выше, чем традиционных способов (хранение данных в простых файлах). Используемые средства позволяют значительно уменьшить затраты на хранение, при этом оставляя неизменной необходимую глубину аудита.

Способы сбора данных

Мониторинг трафика баз данных осуществляется одним из следующих способов:

– S-TAP (программный агент): единственный в своем классе решений, этот легковесный программный агент отслеживает сетевой и локальный трафик СУБД (разделяемая память, именованные каналы и пр.) на уровне операционной системы СУБД. S-TAP почти не оказывает влияния на быстродействие СУБД (обычно 2-4% процессорного времени), поскольку только передает данные на коллекторы Защита +. Анализ, корреляция, нормализация данных аудитов производится на коллекторах или агрегаторахЗащита +. Агенты S-TAP часто являются самым лучшим вариантом установки, так как они не требуют изменений в сетевой инфраструктуре для организации SPAN-портов в центрах обработки данных.

– SPAN порт или аппаратный агент: в этом случае Защита + разворачивается как сетевой монитор, анализирующий зеркальный сетевой трафик, получаемый через SPAN порты.

– S-TAP и SPAN порты: для достижения максимальной эффективности можно использовать комбинированный способ сбора данных.

Защита + состоит из набора программных модулей, установленных на стабильную версию операционной системы Linux на отдельных серверах.

С помощью политик безопасности и механизмов выявления аномалий в режиме реального времени выявляются и пресекаются все подозрительные активности, в том числе попытки неавторизованного доступа.

Решение отслеживает 100% транзакций СУБД, в том числе команды DDL, DML, SELECT, DCL, хранимые процедуры, различные исключения безопасности, XML-команды, а также все другие активности пользователей (включая локальные доступы к СУБД).

Защита + практически не оказывает влияние на работу СУБД и не требует

никаких изменений в СУБД. В работе Защита + не использует штатные средства СУБД, тем самым обеспечивая независимость и достоверность собираемой информации.

Защита + – гибкое кроссплатформенное решение, которое может быть развернуто в течение нескольких дней. Решение не оказывает влияния на быстродействие баз данных и информационных систем, а также не требует их изменения при внедрении.

ГЛАВА 3. ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ

3.1. Экономическая часть

Экономическая эффективность информационной системы – это количественное выражение комплекса положительных влияний, оказываемого эксплуатацией компьютеров и других технических средств информационной системы на управляемый объект, в том числе и на организацию структуры управления, повышение качества управленческих работ на облегчение труда трудовых затрат, а так же качественными изменениями в организации учетного процесса, получаемые в результате применения средств высоких технологий и более рациональных методов труда, влияющих положительно на учетную и финансовую деятельность предприятия.

В данной части дипломного проекта произведём расчёт затрат на программно-аппаратные комплексы и заработные платы сотрудников отдела информационной безопасности.

3.2 Расчёт оборудования для совершенствования системы защиты информации

Себестоимость продукта (затрат) зависит напрямую от таких составляющих как размер заработной платы участников проекта, стоимости оборудования и программных средств, используемых для разработки продукта.

Данная подсистема разработана по заказу ОАО «РЖД» согласно специфике пожеланий данного учреждения и ориентирована на данное учреждение.

В таблице 3.2.1 произведём расчёт необходимого оборудования для совершенствования системы защиты информации.

Таблица 3.2.1 - Стоимость оборудования системы защиты информации

№	Наименование	Количество	Стоимость
1	2	3	4
1	Генератор шума «Барон»	1	42500.00 руб.
2	Фильтр сетевой помехоподавляющий ФП-10	1	40900.00 руб.
3	Индикаторов поля «ЛИДЕР 3G»	1	17890.00 руб.
4	Система видеонаблюдения и аудиорегистрации «Видеолокатор»	1	58000.00 руб.
5	Защитная пленка	4	10000.00 руб.
6	Жалюзи	4	12000.00 руб.
7	Декоративные экраны на батареи	3	3300.00 руб.
8	Экранирование		70000.00 руб.
	Итого:		238480.00 руб.

Вывод: стоимость необходимого оборудования для комплексной защиты информации комнаты переговоров составит 238480.00 рублей.

3.3 Анализ экономической целесообразности внедрения подсистемы «Защита +»

В первую очередь для экономической целесообразности внедрения подсистемы Защита +. Покупка программного обеспечение Защита + 20000,00 рублей.

Затраты на оплату труда программистарасчитаем по формуле 3.3.1:

$$ЗП = ЗМП \cdot 1, \text{ (ф. 3.3.1)}$$

Где QM – средний месячный оклад программиста;

1 – месяц.

QП =15000·1 = 15000 руб.

Среднемесячные затраты труда программиста с учетом премийрасчитаем по формуле 3.3.2:

QППР = QП·(1+КПР) ,(ф. 3.3.2)

Где КПР – коэффициент премий (10-30%).

QППР = 15000·(1+0,2) = 18000 руб.

Среднемесячные затраты на оплату труда программиста с учетом отчислений на социальные нужды расчитаем по формуле 3.3.3

QПСС = QПУР·(1+КСС), (ф. 3.3.3)

Где КСС – коэффициент отчислений на социальные нужды (единый социальный налог 30,2%).

QПСС= 18000·(1+0,302) =23436 руб.

Число рабочих часов в году определяется по формуле 3.3.4:

$$n_P = (N - N_П - N_B) \cdot N_{CM} - N_П \cdot 1, \text{ (ф. 3.3.4)}$$

гдеN – общее число дней в году;

NП – число праздничных дней в году;

NB – число выходных дней в году;

NCM – продолжительность смены;

1 – величина сокращений предпраздничных рабочих дней;

$$n_P = (365 - 10 - 104) \cdot 8 - 10 \cdot 1 = 1998 \quad \text{час}$$

Средняя часовая оплата труда программиста (разработчика) расчитывается по формуле 3.3.5

$$C_{РАЗР} = \frac{ФЗР_{СН}}{n_Р} \quad \text{(ф. 3.3.5)}$$

$$C_{разр} = \frac{299232,00}{1998} = 149,77 \text{ руб/ч}$$

Где ФЗРСН – годовой фонд заработной платы с учетом отчислений.

Время профилактики: ежедневно – 0,5 часа, ежемесячно – 2 часа, ежегодно – 16 часов.

Годовые текущие затраты на эксплуатацию ПК определяются по формуле 3.3.6

$$З_{ГПК} = З_{ГАМ} + З_{ГЭЛ} \quad \text{(ф. 3.3.6)}$$

$$З_{ГПК} = 4166,67 + 1337,85 = 5504,52$$

Где ЗГАМ – годовые отчисления на амортизацию;

ЗГЭЛ – годовые затраты на электроэнергию для ПК.

Сумма годовых амортизационных отчислений определяется по формуле 3.3.7

$$З_{ГАМ} = Ц_{ПК} \cdot Н_А \quad \text{(ф. 3.3.7)}$$

Где ЦПК – балансовая стоимость ПК;

На – норма амортизационных отчислений за мес.

$$Н_А = \frac{1}{Т_{ЭКС}^{ПК}} \cdot 100 \,,$$

$$H_A = (\frac{1}{6} \cdot 100) = 16.67\%$$

Балансовая стоимость ПК расчитывается по формуле 3.3.8

$$Ц_{ПК} = Ц_Р \cdot (1 + К_{УН}) \quad \text{(ф. 3.3.8)}$$

гдеЦР – рыночная стоимость ПК (в среднем 50000);

КУН – коэффициент, учитывающий затраты на установку и наладку (5%);

ЦПК=50000·(1+0,05)=52500 руб.

$$З_{ГАМ} = Ц_{ПК} \cdot H_A,$$

$$З_{ГАМ} = 52500 * 0,1667 = 8751,75 \text{ рублей.}$$

Затраты на электроэнергию, потребляемую ПК определяются по формуле 3.3.9:

$$З_{ГЭЛ} = P_{ЧПК} \cdot T_{ГПК} \cdot Ц_{ЭЛ} \cdot A, \quad \text{(ф. 3.3.9)}$$

$$З_{ГЭЛ} = 0,5 \cdot 1982 \cdot 1,5 \cdot 0,9 = 1337,85 \text{ рублей.}$$

гдеРЧПК – установочная мощность ПК;

ТГПК – годовой фонд полезного времени работы машины;

ЦЭЛ – стоимость 1кВт/час. электроэнергии (Цэл=1,5 руб.);

А – коэффициент интенсивного использования ПК (0,9-1);

Затраты на аренду рабочего места рассчитывается по формуле 3.3.10

$$А_{ЗД} = S \cdot D_{ЗД} \cdot К_{АЗД} \quad (3.3.10)$$

$$А_{ЗД} = 6 \cdot 6000 \cdot 0,40 = 14400 \text{ рублей.}$$

где S – площадь одного рабочего места (6-10 м2);

DЗД– стоимость 1 м2 помещения с учетом коммунальных расходов (8-

14 тыс. руб./ м2);

КАЗД – коэффициент амортизации здания.

$$К_{АЗД} = \frac{1}{Т_{ЭКС}^{ЗД}} \cdot 100,$$

$$К_{АЗД} = \frac{1}{251} \cdot 100 = 0,40$$

.

Расходные материалы

Затраты на расходные материалы приведены в таблице 3.3.1.

Таблица 3.3.1- Расходные материалы

Статьи затрат	Стоимость за единицу, руб./шт., руб./час	Количество, шт./час., комплект	Общая стоимость, руб.
1	2	3	4
Диски CD-RW	75	1	75
Бумага формата А4	365	1	365
Картридж	2500	0,1	250
Канцелярские товары	500	0	0
Итого (ZPM):	690 руб.		

Общие внедрение на разработку программного продукта

Общие затраты на внедрения программного продукта пиведены в таблице 3.3.2.

Таблица 3.3.2 – Общие затраты

Статьи затрат	Условное обозначение	Числовое значение
Общие затраты на внедрение		236 000 руб..
Аренда рабочего места	АЗД	14400 руб.
Расходные материалы	ЗРМ	690 руб.
ИТОГО (СОБЩ):		251090 руб.

При расчете ожидаемого эффекта от внедрения проекта следует учесть тот факт, что ни время функционирования компьютера на рабочем месте, ни время работы оператора ПК не изменились. Данные затраты фирмы являются постоянным фактором оператор ПК получает оклад от проведённого времени на рабочем времени, компьютер работает все рабочее время. Таким образом, метод АВС, в своем классическом варианте несколько обессмысливается.

Оценка возможных производственных потерь

Ожидаемым результатом может быть эффективность обработки и хранения данных для последующего оперативного использования, эффект предоставления информации, который согласитесь, трудно измерить в конкретном денежном исчислении. Это можно оценить в зависимости от того, какой бы ущерб нанесла ошибка в производственном процессе и затраты на устранение её последствий. Бесспорен тот факт, что ручная работа существенно усложняет и тормозит производственный процесс и тут можно сказать о том, что такой подход при современных темпах производства и совершенствования высоких компьютерных технологий, просто пагубен.

Необходимо сразу сказать о том, что оценку производственных потерь невозможно просчитать и измерить в денежном эквиваленте до возникновения ошибки. Только в этом случае можно просчитать стоимость ошибки, ведущей к затратам направленным на ликвидацию последствий. Финансовые затраты на ликвидацию потерь от бесхозяйственной

деятельности руководителей и персонала при использовании недостоверной информации могут измеряться суммами различного порядка.

Заключение

В рамках данной дипломной работы были получены следующие результаты:

Проведен анализ предприятия на предмет выявления угроз.

Были определены основные угрозы безопасности информации во время проведения переговоров:

– подслушивание и несанкционированная запись речевой информации с помощью закладных устройств, систем лазерного подслушивания, стетоскопов, диктофонов;

– регистрация на неконтролируемой территории с помощью радиомикрофонов участниками, выполняющими агентурное задание;

– перехват электромагнитных излучений при работе звукозаписывающих устройств и электроприборов.

– Для данного строительного холдингавыявлены наиболее опасныетехнические каналы утечки информации: оптический, материально-вещественный, акустический, радиоэлектронный.

– Была рассмотрена действующая организация инженерно-технической защиты информации в конференц-зале.

– Изучены теоретические основы построения инженерно-технической защиты информации.

– Рассмотрен теоретический материал по инженерно-технической защите информации. Определены меры и средства по обеспечению инженерно-технической защиты информации.

– Разработаны меры по совершенствованию инженерно-технической защиты информации.

Были выделены рубежи защиты:

– дверь в конференц-зал;

– окна в помещение организации;

– система отопления;

- линии электросетей;
- человеческий фактор.

Для каждого рубежа предложены соответствующие технические меры и средства защиты.

В работе предложен ряд организационных мер для защиты данных в помещении для переговоров ОАО «РЖД»

Произведена оценка стоимости оборудования для совершенствования системы инженерно-технической защиты информации в конференц-зале.

Список используемой литературы

1. Торокин А.А. Инженерно-техническая защита информации [Текст] // М.: Гелиос АРВ, 200 5 958 с.
2. Защита от утечки информации по техническим каналам [Текст] //Бузов Г.А., Калинин С.В., Кондратьев А.В. – М.: Горячая линия – Телеком, 2002. – 414 с.
3. . Правовое обеспечение системы защиты информации на предприятии [Текст]: учеб.пособие // Демин В., Свалов В 2008 - 190 с.
4. Завгородний, И.В. Комплексная защита информации [Текст] // Логос, 2001г. — 370с.
5. Машкина, И.В. Курс лекций по инженерно-технической защите информации[Текст] // УГАТУ, 2007г — 450с.
6. Рембовский, А.М. Выявление технических каналов утечки информации [Текст] // Вестник МГТУ, 2003г.— 270с.
7. Хорев, А.А. Защита информации от утечки по техническим каналам. Технические каналы утечки информации [Текст]: учеб.пособие //А. А. Хорев; Гостехкомиссия России, 1998.- 320 с.
8. Хорев А. А. Способы и средства защиты информации[Текст]: учеб. пособие // М.: МО РФ, 2000
9. Защита информации в офисе [Текст]: учеб.пособие // И.К. Корнеев, Е.А. Степанов. – М.: Проспект, 2008. – 336 с.
10. Бузов Г.А. Специальная Техника [Текст]: журнал // № 5, 2005.
11. Хорев А.А. Специальная Техника [Текст]: журнал // № 5, 2009.-
12. Интернет-проект ООО «Научно-Производственный Центр Аналитика» [Электронный ресурс]: - Режим доступа: http://www.analitika.ru
13. Лаборатория ППШ. Противодействие промышленному шпионажу [Электронный ресурс]: - Режим доступа: http://www.pps.ru.
14. Научная электронная библиотека[Электронный ресурс]: - Режим доступа: http://www.elibrary.ru

15. Компания «Конфидент»[Электронный ресурс]: - Режим доступа:http://www.confident.ru/home/
16. ОАО «ФОРПОСТ» [Электронный ресурс]: - Режим доступа:http://forpost-dveri.ru.
17. Торгово-сервисная фирма[Электронный ресурс]: - Режим доступа: http://orientir74.blizko.ru/products/261869-antizhuchok_lider_3g
18. ООО НПП "СПО"[Электронный ресурс]: - Режим доступа: http://filtr-fp.ru/