Содержание:

ВВЕДЕНИЕ

При современном развитии информационных технологий не нуждается в дополнительных доказательствах тот тезис, что информация является наиболее ценным ресурсом для любой организации, действующей на современном рынке. Отсюда вытекает однозначность необходимости защиты информации.

По оценкам некоторых экспертов информационной безопасности, утечки конфиденциальной информации, причиной которых является использование открытых каналов, выдвигаются в настоящее время на первое место среди утечек по другим каналам.

Нарушители, находящиеся за периметром информационной системы организации, стремятся получить несанкционированный доступ к информации, подлежащей защите, кроме того, существуют недобросовестные сотрудники организации, которые могут использовать свои возможности по доступу к информации с целью ее разглашения третьим лицам по корыстным чаще всего мотивам.

Но даже в случае примирения различных средств и методов защиты данных, система защиты информации не может быть полностью эффективной и есть шанс пропустить утечку информации, поскольку не все каналы могут качественно контролироваться.

В рамках этого тезиса делаем вывод, что для реализации эффективной системы защиты данных нужно брать под контроль каналы утечки информации различного рода. Доступность контроля каналов утечек информации поддерживают системы класса DLP (Data Leak Prevention).

Использование подобных DLP-систем позволит уменьшить риски утечки данных, а также даст возможность подробно расследовать инциденты ИБ в случае их возникновения.

Вопросу использования такой системы и посвящена эта работа. Внедрение DLP можно назвать достаточно сложным проектом, связанным с немалыми стоимостными и трудовыми затратами.

Объектом исследования в работе определена защита информации. Предметом исследования является безопасность данных ООО «Московская пивоваренная компания».

Цель курсовой работы: Выбрать программные средства для защиты корпоративной сети ООО «Московская пивоваренная компания».

Задачи курсовой работы:

1. Провести классификацию и выполнить анализ основных методов и средств защиты информации в сетях;

2. Рассмотреть основные технологии защиты информации в сетях;

3. Провести анализ существующей системы защиты информации в ООО «Московская пивоваренная компания»;

4. Выбрать программные средства для защиты сети компании.

В этой работе понятие защиты от потери данных рассмотрено с точки зрения обеспечения ИБ (информационной безопасности) и ЗИ (защиты информации).

1.ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ

1.1. Задачи и принципы обеспечения информационной безопасности

Разработка автоматизированных систем (АС) различной сложности так или иначе связана с решением некоторых задач, которые в первую очередь связаны с проектированием механизмов защиты данных от их потери в результате несанкционированного доступа (НДС) в подобных системах. Самыми обобщенными задачами можно назвать [26]:

• Реализацию безопасности информационных ресурсов как в уже существующих представлениях, так и в новых формах представления данных: мультимедиа, гипертекст и т.п. В системном плане это можно понимать, как необходимость

обеспечения безопасности при помощи технологий защиты на уровне информационных ресурсов, а не отдельных документов, сообщений или файлов;

• Реализация защищенности всей информационной структуры (перекрёстная идентификация/аутентификация составляющих информационного пространства). Активное развитие компьютерных технологий требует осуществления более эффективной защиты в случае удаленного доступа к данным, а также при взаимодействии пользователей, находящихся как внутри компьютерной сети, так и внутри общедоступных сетей. И это взаимодействие может быть реализовано в различных аппаратных и операционных средах;

• Обеспечение защиты от автоматических методов и средств вторжения. В ходе использования уже созданных АС было выявлено, что сегодня от защиты требуются совершенно другие функции, а именно – обеспечение безопасности ИС и процессов самой АС от ассоциированного разрушающего воздействия вредоносных систем. Подобная проблема позволяет убрать сложившийся стереотип реализации защищенности данных в АС, который подразумевает, что проблема безопасности может решатся лишь разграничением доступа.

Интеграция процедур защиты информации в информационный процесс в АС в качестве обязательного его элемента.

Таким образом, главные направления улучшения механизмов защиты данных от НСД в АС следуют из основных направлений развития технологий защиты информационных ресурсов в целом, с учетом особых свойств работы конкретной АС и требований, которые могут предъявляться к такого рода системам [30].

Важно помнить, что любая успешно реализованная угроза ИБ так или иначе использует отдельные особенности построения и функционирования АС, либо недостатки ее механизмов защиты.

Эти особенности исследуются уже достаточно давно и получили название «уязвимостей информационного процесса» или «уязвимостей механизма защиты». Все способы осуществления информационных атак базируются на такого рода уязвимостях, которые как бы провоцируют появление средств нападения. Таким образом, противостояние угроз и механизмов защиты напоминает систему с обратной связью: новые виды атак приводят к появлению новых способов защиты, а недостатки в механизмах защиты приводят к появлению новых средств их преодоления и т.д.

Выход из подобной ситуации возможен двумя путями [21]:

1) создание высокоэффективных и надежных средств защиты от каждого типа атак;

2) устранение уязвимостей АС, служащих источниками успешной реализации угроз информационной безопасности.

В соответствии с этим, возможно два пути обеспечения защищенности информации в АС [23]:

1) применение в них достаточно универсальных средств защиты от достаточно широкого круга угроз информационной безопасности;

2) изначальная разработка АС как защищенной, устранение в ее архитектуре уязвимостей, являющихся причинами успешной реализации угроз. При этом СЗИ, реализуя механизмы защиты от конкретных видов угроз, не зависят напрямую от назначения АС и не требуют модификации по мере ее развития.

Трудности реализации указанных направлений очевидны: для создания эффективного механизма защиты информации необходимо проанализировать все типы угроз информационной безопасности и выработать эффективные способы противодействия угрозам каждого типа.

Критерий оптимального управления СЗИ НСД в АС должен иметь комплексный характер, что приводит к многокритериальным задачам оптимального управления [11] механизмами защиты. Это обусловлено конфликтным характером использования ресурсов АС механизмами обработки и механизмами защиты информации.

В этих условиях решение задач организации оптимального управления СЗИ НСД в АС напрямую связано с обоснованием возможностей по использованию ресурсов АС и, как следствие, необходимостью обоснования требований к характеристикам СЗИ. В настоящее время содержание требований к СЗИ НСД и порядок их задания определяется действующими документами ФСТЭК (Федеральная служба по техническому и экспортному контролю) РФ, которые задают только качественные требования к СЗИ по составу реализуемых ими защитных функций [4].

Это обусловливает необходимость дополнения существующих качественных требований по защите информации количественными, что, в свою очередь, приводит к необходимости перехода от сложившейся практики организационного

характера управления СЗИ НСД к организационно-технологическому. Подобный переход может быть обеспечен средствами поддержки принятия управленческих решений на основе комплексной оценки качества функционирования СЗИ НСД в соответствии с математическими моделями процесса ее функционирования [13]. Такие средства являются обязательной составной частью комплексов СЗИ.

Система законодательства РФ в области информационной безопасности и защиты информации состоит из законов, подзаконных актов (указов и распоряжений Президента Российской Федерации и постановлений и распоряжений Правительства Российской Федерации, нормативных правовых актов федеральных органов исполнительной власти), а также ряда различных международных договоров Российской Федерации, которые, в соответствии с Конституцией Российской Федерации, являются составной частью ее правовой системы.

Основным законом, определяющим отношения в информационной сфере (в том числе связанные с защитой информации), является Федеральный закон «Об информации, информационных технологиях и защите информации», принятый в 2006 году.

1.2. Описание основных угроз безопасности данных

Под угрозой понимается, как правило, событие или действие, которое может произойти или уже произошло, и реализация которого может принести ущерб информационным активам компании в той или иной форме. При описании угроз, как правило, описываются их признаки и классифицируются объекты, к которым эти угрозы могут быть применены.

Такая классификация необходима по той причине, что громадное многообразие влияющих факторов различного рода на систему защиты информации формирует крайне подверженную изменениям и влияниям среду защиты информации, где каждый фактор описать невозможно, также как и невозможно определенно спрогнозировать ее влияние на всю систему в целом. Поэтому классификацию угроз проводят по классам угроз, а в каждом классе отдельные угрозы могут быть описаны более конкретно и полно.

Классификация всех возможных угроз информационной безопасности АС может быть проведена по ряду признаков (рисунок 1). В зависимости от рассматриваемой

предметной области в каждом конкретном случае классификация может быть дополнена. Рассмотрим классификацию угроз информационной безопасности по базовым признакам [7].

- по природе возникновения;
- по степени преднамеренности проявления;
- по непосредственному источнику угроз;
- по положению источника угроз;
- по степени зависимости от активности АС;
- по степени воздействия на АС;
- по способу доступа к ресурсам АС;
- по текущему месту расположения информации, хранимой и обрабатываемой в АС.

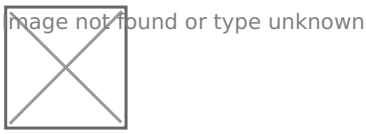

Рисунок 1 – Классификация угроз информационной безопасности [36]

Под угрозой понимается потенциально существующая опасность случайного или преднамеренного нанесения ущерба охраняемому объекту.

Вероятные угрозы охраняемому объекту можно разделить на 2 типа: внешние и внутренние угрозы.

Внешние угрозы [9]:

- физический ущерб объекту или его отдельным элементам как результат терроризма, хулиганства, вандализма;
- хищения силами организованной преступной группы;
- вооруженное ограбление силами организованной преступной группы;
- захват террористическими группировками.

Внутренние угрозы:

- хищения работниками;
- хищения охранниками;
- некомпетентное использование, настройка или неправомерное отключение средств и систем защиты;

- неумышленное изменение технологического процесса, внедрение и использование нерегламентированных технических средств, компьютерных программ.

Независимо от определения конкретного вида или класса угроз система защиты информации должна удовлетворять требованиям тех лиц, которые ее эксплуатируют, а также должна обеспечивать общие свойства информации и систем ее обработки [8].

На основании проведенного компанией InfoWatch исследования утечек можно выделить следующие наиболее актуальные каналы утечки информации[10].

В 2017 году Аналитическим центром InfoWatch был зарегистрирован 2131 случай утечки конфиденциальной информации (см. Рисунок 2).

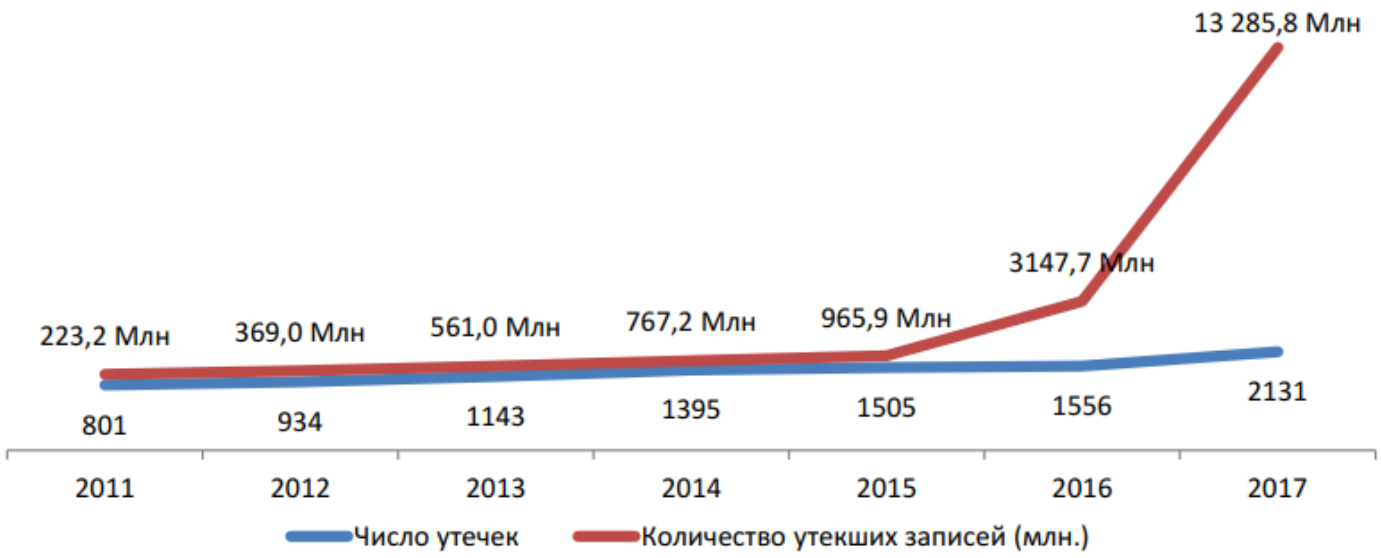

Рисунок 2 Число утечек информации и объем данных (записей), скомпрометированных в результате утечек. 2011 - 2017 гг.

Объем данных, скомпрометированных в результате утечек, составил более 13,3 млрд записей, — номера социального страхования, реквизиты пластиковых карт и иная критически важная информация.

Количественные показатели утечек в 2017 году вновь показали взрывную положительную динамику. Если в 2016 году прирост числа утечек к предыдущему году составил 3,4%, то в 2017 году число утечек выросло на 36,9%. Впервые за все время наблюдений мы зафиксировали четырехкратное увеличение объема данных (записей), скомпрометированных в результате утечек, и существенный (более, чем

в три раза) рост объема скомпрометированных данных (записей) в расчете на одну утечку («мощность» утечки) см. Рисунок 3.

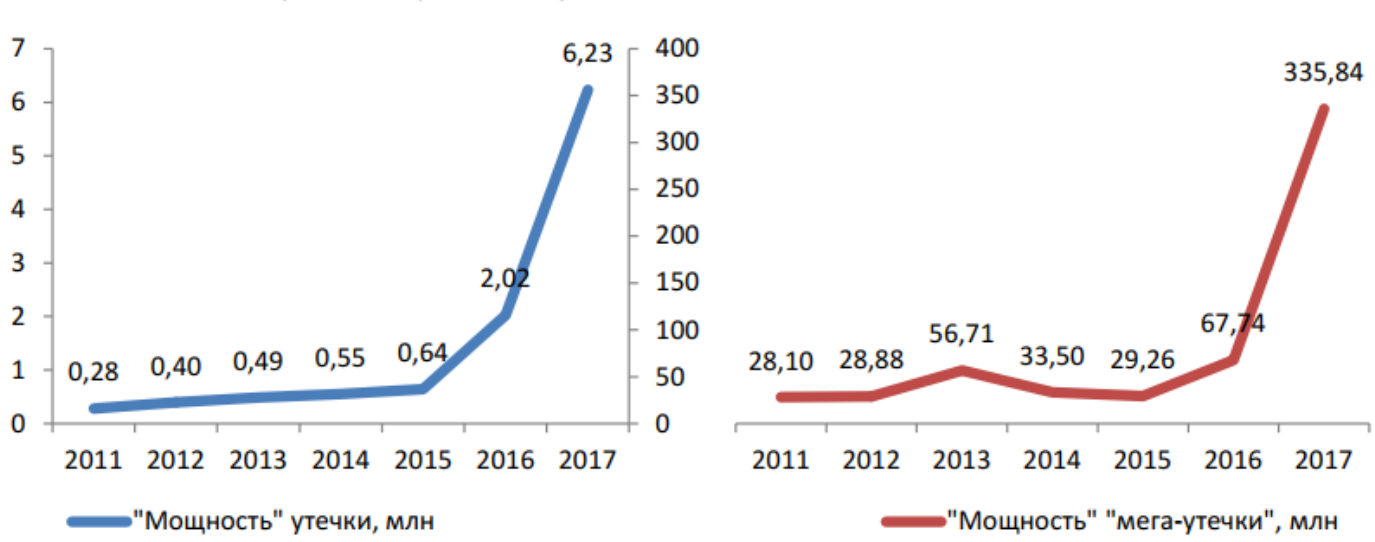

Рисунок 3 «Мощность» (объем скомпрометированных данных (записей) в расчете на одну утечку) для утечек вообще и «мега-утечек». 2011 -2017 гг.

В среднем, на одну «внешнюю» утечку приходится 8,23 млн скомпрометированных данных (записей). Для сравнения — в результате одной утечки данных по вине или неосторожности внутреннего нарушителя было скомпрометировано в среднем 4,2 млн данных (записей). По вине внешнего злоумышленника за год было скомпрометировано 6,6 млрд данных (записей) — это составляет 58,3% от совокупного объема скомпрометированных в 2017 году данных (записей). Внешние атаки спровоцировали 18 из 39 зафиксированных «мега-утечек».

При реализации полного анализа рисков нужно решать ряд непростых задач. Процесс оценивания рисков разделяется на несколько этапов:

• Определение ресурса и оценивание его количественных показателей или выявление потенциального негативного воздействия на бизнес;

• Оценка угроз;

• Оценка уязвимостей;

• Оценка уже внедренных и предполагаемых средств обеспечения ИБ;

• Оценка рисков.

На базе оценивания рисков определяются средства, поддерживающие режим информационной безопасности. Ресурсы, имеющие значение для бизнеса и подверженные уязвимости, входят в группу риска, если по отношению к ним возможна какая-либо угроза. При оценивании рисков берется во внимание возможное негативное влияние от нежелательных происшествий и параметры значимости выбранных уязвимостей, а также угроз для них.

Ресурсы зачастую подразделяются на несколько классов: физические, программные и данные. Для любого класса существует своя методика оценки ценности элементов. Чтобы оценить ценность ресурсов, выбирается подходящая система критериев. Помимо критериев, учитывающих финансовые потери, в компании могут присутствовать критерии, показывающие:

• Ущерб репутации компании;

• Проблемы, связанные с нарушением действующих законов;

• Ущерб здоровья персонала;

• Ущерб от разглашения конфиденциальных и персональных данных;

• Проблемы, связанные с невозможностью выполнения взятых обязательств;

• Ущерб от реорганизации компании или деятельности.

Могут применяться и другие критерии в зависимости от направленности организации. Так, в правительственных учреждениях могут использоваться критерии, отражающие сферы национальной безопасности и международных отношений.

Также важно идентифицировать уязвимости – слабые места в системе защиты, которые становятся причиной реализации угроз.

Чтобы конкретизировать вероятность реализации угрозы, исследуется некоторый отрезок времени, в течение которого происходит защита ресурса. Возможность того, что угроза будет реализована, выражается следующими факторами:

• Привлекательность ресурса (параметр учитывается при рассмотрении угрозы умышленного воздействия со стороны людей);

• Использование ресурса для получения дохода (параметр учитывается при рассмотрении угрозы умышленного воздействия со стороны людей);

• Использования уязвимости для совершения атаки.

Сегодня известно большое количество методов оценивания угроз. Уже разработано множество методик анализа рисков.

1.3. Методы и средства обеспечения защиты информации

1. Организационно-правовые методы и средства [4]. Организационные меры по обеспечению информационной безопасности являются основной всех мероприятий по построению системы защиты информации. От того, насколько полно и качественно руководством предприятия построена организационная работа по защите информации, зависит эффективность системы защиты информации в целом, так как правильная постановка задачи на обеспечение мер по защите информации и грамотное распределение обязанностей между исполнителями – это фундамент построения любой системы.

Место и роль организационных мероприятий в общей системе

2. Аппаратно-программные методы и средства. Программно-аппаратные комплексы защиты информации предназначены для решения следующей совокупности задач защиты конфиденциальной информации, обрабатываемой в корпоративных приложениях [4]:

- реализация защищенной обработки на одном компьютере данных различной категории конфиденциальности с предотвращением хищения, раскрытия конфиденциальности при хищении и несанкционированной модификации конфиденциальных данных;
- реализация защиты системных ресурсов компьютеров в составе АС предприятия;
- реализация защищенного подключения компьютеров к локальной и внешней сети;
- реализация коллективного доступа сотрудников предприятия к защищаемым ресурсам АС предприятия;
- реализация эффективного инструментария администратора безопасности (АРМа администратора АС предприятия).

Одним из видов программно-аппаратных комплексов для предотвращения потерь данных являются DLP-системы.

DLP-системы - система предотвращения утечек важной информации из информационной системы под влиянием внешних факторов, а также программные или программно-аппаратные устройства или комплексы для обеспечения защиты от таких утечек. Такие системы формируются в результате анализа информационных потоков, пересекающих границу защищаемой информационной системы.

При обнаружении в таком потоке информации, которая определена как конфиденциальная, производится срабатывание активной компоненты системы и такая передача блокируется.

При этом могут подвергаться анализу такие каналы утечек, как [32]:

- электронная почта (общая и корпоративная);
- ftp-доступ к удаленным ресурсам;
- мгновенные сообщения интернет-мессенджеров;
- передача информации для печати;
- информация при передаче на внешние накопители (USB- флешки, различного рода диски);
- соединения внутри сети.

Основными преимуществом DLP-систем перед системами с аналогичными задачами являются возможность контроля над всеми типами и видами каналов утечки, постоянно используемым и повседневной деятельности предприятия, возможность обнаружения конфиденциальной информации независимо от вида ее представления по ее содержимому, возможность блокировки любого канала утечки информации и сигнализация об этом администратору безопасности, а также предельная автоматизация правил и процедур обработки информации в соответствии с действующей в организации политикой безопасности.

DLP – достаточно сложное программное или программно-аппаратное решение, которое позволяет не только блокировать факт передачи информации, но и осуществлять распознавание подготовки пользователя к такому действию [12]. На основании анализа таких ситуаций система строит отчеты и в случае утечки информации они могут стать основной для расследования и поиска виновных.

Таким образом, DLP система в первую очередь необходима для анализа трафика, а также его блокировки в случае обнаружения передачи конфиденциальной информации. Степень защиты информации, перечень каналов, порядок реагирования системы настраивается в ходе управления системой. Как правило, в едином интерфейсе управления системой могут быть объединены события по данным из трех областей – это информация, передаваемая по каналам внутренней сети во внешнюю сеть, данные, которые постоянно хранятся в хранилищах информации предприятия, а также данные, с которыми работают пользователи на своих рабочих местах. Следовательно, для полноценного использования DLP системы необходима установка трех различных компонент – в каналах передачи данных, на северах, на станциях пользователей [14].

3. Инженерно-технические методы и средства. Инженерно-техническая защита информации должна быть встроена в общую систему информационной безопасности компании и, в свою очередь, включать в себя физическую защиту информации, контроль доступа, аутентификацию, технические средства разграничения доступа.

Для предотвращения работы с ресурсами ИС посторонних лиц важно обеспечить распознавание каждого допустимого пользователя (или групп пользователей). Для подобной идентификации можно применять устройства различного рода: магнитные карты, ключи, дискеты и т.д.

Аутентификация (подтверждение подлинности) сотрудника может быть осуществлена при помощи [19]:

• Проверки специального устройства (карты, ключа и т.д.), либо знания пароля;

• Проверки уникальных физических характеристик и параметров каждого пользователя при использовании биометрических устройств.

Области ответственности и задачи для каждого конкретного технического средства обычно устанавливаются исходя из его технических характеристик, описанных в документации по каждому средству.

Технические средства разграничения доступа в идеале должны составлять одну большую единую систему контроля доступа [20]:

• На подконтрольную территорию в целом;

• К компонентам информационной системы и элементам системы защиты данных;

• К информационным ресурсам (носителям информации, документам, архивам, справкам и т.д.);

• К активным ресурсам (задачам и прикладным программам);

• К самой операционной системе, программам и программным средствам защиты.

2.АНАЛИЗ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ООО «МОСКОВСКАЯ ПИВОВАРЕННАЯ КОМПАНИЯ»

2.1.Краткая характеристика компании и используемых средств защиты информации

Московская Пивоваренная Компания вышла на российский рынок напитков с продуктами собственного производства в сентябре 2008 года. В состав компании входят самый современный пивоваренный завод в России, а также собственные дистрибьюторский и логистический центры, расположенные в семи километрах от МКАД (г. Мытищи) в экологически чистом районе. Партнерами проекта выступили Сбербанк России и инвестиционный фонд Detroit Investments, общий объем инвестиций составил более 300 миллионов долларов.

В состав компании входит самый современный пивоваренный завод в России, а также собственные дистрибьюторский и логистический центры.

Организация режима информационной безопасности и эксплуатация СЗИ ИС ООО «Московская пивоваренная компания» осуществляется группой по защите информации, которая организационной входит в отдел информационных технологий. Организационная структура группы представлена на рисунке 4:

Image not found or type unknown

Рисунок 4 – Структура группы по защите информации

Также в компании применяется антивирусная защита - на ПК пользователей и серверах инсталлирован программный продукт Kaspersky Enterprise Space Security.

В компании применяется ЭДО с использованием СЭД Docsvision.

В состав установленного программного комплекса защиты от утечек данных входят Zgate — сетевая DLP-система для защиты от утечек корпоративных данных, Zlock — система, позволяющая предотвратить утечки конфиденциальных дынных через периферийные устройства, а также Zdisk – механизм защиты от НСД для ПК пользователей.

Средствами SecurIT и TrendMicroDLP реализованы функции определения, контроля и обеспечения безопасности всех конфиденциальных данных в состоянии хранения, обработки и передачи.

2.2.Выделение информационных активов компании и определение уязвимостей

Функции организации и обеспечения ИБ в ООО «Московская пивоваренная компания» сейчас выполняются сотрудниками IT-отдела по поручению начальника данного отдела. Ими же реализуется анализ рисков ИБ с последующим докладом руководителю ООО «Московская пивоваренная компания» через начальника отдела ИТ.

Из всего этого следует, что в настоящее время в ООО «Московская пивоваренная компания» нет продуманной стратегии по анализу рисков ИБ, анализ реализован лишь частично, фрагментарно и выполняется неподготовленным сотрудником. Оценка рисков в рамках проведения анализа реализована в виде составления списка самых опасных угроз, которые могут быть угрозой целостности информационных активов компании в настоящее время.

В компании имеется информация конфиденциального характера, которая также сведения ограниченного распространения (коммерческая тайна, служебная тайна, персональные данные), и открытые сведения.

Необходимо защитить:

• Всю конфиденциальную информацию и информационные ресурсы, независимо от их представления и местонахождения внутри информационной среды компании;

• Данные, составляющие коммерческую тайну, доступ к которым ограничен владельцем информации в рамках закона ФЗ "О коммерческой тайне";

• Служебные данные, доступ к которым ограничен органами государственной власти в рамках ГК РФ;

• Данные о частной жизни граждан, по которым можно определить их личность (персональные данные), доступ к которым ограничен в рамках ФЗ "О персональных данных";

• Открытые данные, необходимые для стабильного функционирования компании.

Перечень сведений конфиденциального характера ООО «Московская пивоваренная компания» приведен в таблице 1.

Таблица 1 - Перечень сведений конфиденциального характера ООО «Московская пивоваренная компания»

№ п/п	Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, №№ статей
	Сведения о программном обеспечении, принципах построения, структуре и составе оборудования корпоративной информационной системы ООО «Московская пивоваренная компания»	Коммерческая тайна	Указ Президента РФ от 6 марта 1997 года № 188, ФЗ РФ от 29 июля 2004 г. N 98-ФЗ О коммерческой тайне, ФЗ РФ от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
	Входящая и исходящая корреспонденция (в том числе в электронном виде)	Коммерческая тайна	ФЗ РФ от 29 июля 2004 г. N 98-ФЗ О коммерческой тайне
	Персональная информация о сотрудниках	КТ	З РФ от 27 июля 2006 г. N 152-ФЗ "О персональных данных"

Бухгалтерские и финансовые сведения, в том числе документы по установленным формам отчетности о финансово-хозяйственной деятельности	КТ	ФЗ РФ от 29 июля 2004 г. N 98-ФЗ О коммерческой тайне
Сведения, раскрывающие систему организации и состояние сохранности коммерческой тайны в Компании, методы и способы защиты конфиденциальной информации от утечки, утери или искажения	Коммерческая тайна	ФЗ РФ от 29 июля 2004 г. N 98-ФЗ О коммерческой тайне
Система ООО «Московская пивоваренная компания» и разграничения доступа в КИС, идентификаторы и пароли, используемые сотрудниками компании для доступа к информации	КТ	ФЗ РФ от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Активы, имеющие наибольшую ценность и поэтому выбранные в качестве объекта защиты информации, приведены в таблице 2.

Таблица 2 - Результаты ранжирования активов

Наименование актива	Ценность актива (ранг)

Предварительные результаты торгов обоих типов	5
Информация о тендерном предложении до его раскрытия публике	5
Персональные данные сотрудников	4
Финансовая и бухгалтерская отчетность	4
Сведения об арендаторах	3
Сведения о заключаемых договорах	3
Входящая и исходящая корреспонденция	2

Ранги информационным активам присвоены в результате анализа возможных последствий нарушения их целостности или получения к ним несанкционированного доступа третьих лиц.

Таким образом, можно выделить следующие активы, имеющие наибольшую ценность:

- Предварительные результаты торгов обоих типов
- Информация о тендерном предложении до его раскрытия публике
- Персональные данные сотрудников
- Финансовая и бухгалтерская отчетность
- Сведения об арендаторах
- Сведения о заключаемых договорах
- Входящая и исходящая корреспонденция

Оценка уязвимостей в рассматриваемой компании проводится на основании распоряжении руководителя ООО «Московская пивоваренная компания», а также в соответствии с заранее разработанным планом – один раз в 3 месяца.

Установлено, что внутренними нарушителями могут быть лица из следующих категорий персонала:

- технический персонал (уборщики, охранники и т.п. имеющие доступ в помещения, но не имеющие права доступа в ИС)
- рядовой сотрудник - пользователи ИС ООО «Московская пивоваренная компания»;
- руководящий состав - пользователи ИС ООО «Московская пивоваренная компания»;
- сотрудники, имеющие права администратора ИС ООО «Московская пивоваренная компания».

Внешними нарушителями могут быть:

- сотрудники органов государственной власти, а также сотрудники государственных и частных предприятий и учреждений, имеющие непостоянный доступ к ИС ООО «Московская пивоваренная компания» с целью выполнения работ по обслуживанию, установке, настройке и администрированию технических и программных средств;
- посетители ООО «Московская пивоваренная компания» (обычные граждане, пришедшие в компанию);
- сотрудники как государственных, так и коммерческих организаций взаимодействующих по вопросам обеспечения жизнедеятельности ООО «Московская пивоваренная компания» (энерго-, водо-, теплоснабжения, аренды и т.п.);
- представители криминальных структур;
- представители недобросовестных коммерческих структур;
- представители террористических организаций;
- хакер, группа хакеров.

При анализе мотивов действий нарушителя установлено два основных мотива нарушений: безответственность (любопытство) и корыстный интерес (месть, получение финансовой выгоды, получение конкурентной выгоды, в том числе за счет использования данных).

При нарушениях, вызванных безответственностью, нарушитель целенаправленно или случайно производит какие-либо разрушающие действия, не связанные со злым умыслом, вследствие своей некомпетентности или небрежности.

При нарушениях, вызванных корыстным интересом, внутренний или внешний нарушитель - злоумышленник будет целенаправленно пытаться преодолеть систему защиты информации для доступа к данным, хранимым, передаваемым и обрабатываемым в ИС ООО «Московская пивоваренная компания».

При анализе квалификации нарушителей, установлено, что внутренние и внешние нарушители по своей квалификации и уровню знаний об ИС ООО «Московская пивоваренная компания» могут быть разделены следующим образом:

- не знает функциональные особенности и структуру и основные закономерности формирования в ней массивов данных и потоков запросов к ним, не умеет пользоваться штатными программными средствами;
- плохо знает функциональные особенности и структуру, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными программными средствами ИС ООО «Московская пивоваренная компания»;
- средние знания о функциональных особенностях и структуре ИС ООО «Московская пивоваренная компания», обладает высоким уровнем знаний сетевых и информационных технологий, имеет опыт работы со специализированными программными средствами и утилитами;
- хорошо знает функциональные особенности ИС ООО «Московская пивоваренная компания», обладает высоким уровнем знаний в области защиты информации, программирования, сетевых и информационных технологий и опытом работы с техническими и программными средствами ИС ООО «Московская пивоваренная компания»;
- отлично знает функциональные особенности и структуру ИС ООО «Московская пивоваренная компания», функции и механизм действия средств защиты, их сильные и слабые стороны, являлся разработчиком или принимал участие в реализации системы обеспечения информационной безопасности или других систем использующихся в ИС ООО «Московская пивоваренная компания».

По используемым методам и средствам несанкционированного получения информации внутренние и внешние нарушители могут быть разделены следующим образом:

- получение только случайного доступа к информации, не используя при этом каких-либо заранее определенных методов и средств получения информации;
- исследование, сбор информации об ИС ООО «Московская пивоваренная компания» и системе защиты информации;

- использование только штатных и разрешенных к использованию технических и программных средств, а также известных уязвимостей в обеспечении безопасности информации ;
- использование специальных программных (сканеры уязвимостей, взломщики паролей и т.п.) и/или технических средств получения информации, активное отслеживание модификаций существующих в ИС ООО «Московская пивоваренная компания» средств обработки и передачи информации, а также средств защиты информации, внедрение программных закладок и вирусов в ИС ООО «Московская пивоваренная компания», подключение к каналам передачи данных;
- использование агентурного метода получения информации.

1. **Выбор методов и средств защиты информации**

Полнота решения задач защиты информации подтверждается реализацией основополагающих требований (в том числе, сформулированных в действующих нормативных документах в области защиты информации) к достаточности (полноте) набора механизмов защиты, применительно к области использования КСЗИ, к корректности реализации механизмов защиты из состава КСЗИ, к решению задач защиты в общем виде (не применительно к конкретной угрозе или уязвимости системного или прикладного ПО.

Одним из видов программно-аппаратных комплексов для предотвращения потерь данных являются DLP-системы.

В последние годы внимание руководителей предприятий все больше концентрируется на защите от внутренних угроз; это явление находит отражение в современных стандартах и нормативных документах в области информационной безопасности. Кроме того, в последнее десятилетие стали массово выпускаться технические средства для защиты от внутренних угроз. К таким средствам относится, в частности, DLP - системы, которые являются программно - аппаратным комплексом средств, обеспечивающих защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента автоматизированной системы путем анализа и блокирования исходящего трафика. Существующие на данный момент DLP - системы обладают широкими функциональными возможностями и демонстрируют достаточно высокую эффективность при условии их грамотного применения. Принцип функционирования DLP - системы представлен на Рисунке 5.

Рисунок 5 Принцип функционирования DLP - системы

Эффективность работы любой DLP-системы зависит в первую очередь от качества выявления конфиденциальной информации в общем потоке данных. Для этого используется ряд различных технологий. Сравним их.

2.3.Выбор программного комплекса для внедрения в систему защиты информации

Каждая из предприятий- разработчиков систем защиты от утечек (DLP) предлагает, как правило, аналогичную структуру системы, отличающуюся только в деталях. Основными модулями такой системы являются [17]:

- контролирующие модули для каждого канала, по которому возможна утечка;
- агентские модули, устанавливаемые на рабочих местах конечных пользователей;
- управляющее звено с панелью управления для администратора системы.

Контролирующие модули, проводя анализ всей информации, проходящей по каналам за периметр информационной системы организации, определяют данные, которые подлежат защите, проводя ее классификацию и распределение, и передают данную информацию для принятия решения на сервер DLP. Такие модули могут устанавливаться как для исходящей, так и входящей информации.

Модули контроля для обнаружения данных, хранимых в сетевых ресурсах, производят специальные процессы обнаружения, которые могут различаться способами определения конфиденциальной информации. Это может быть как сканирование трафика, так и запуск отдельных программных модулей на серверах или рабочих станциях.

Модули контроля на рабочих станциях также действуют в соответствии с определенной ранее политикой безопасности, проводя анализ действий пользователей с защищаемой информацией, и производят отправку обнаруженных инцидентов на сервер правления DLP.

Программы-агенты на рабочих станциях и серверах контролируют соблюдение правил обработки конфиденциальной информации.

Сервер управления проводит анализ от всех выше перечисленных модулей, формирует отчеты по итогам их работы с помощью консоли управления.

Таким образом, DLP эффективно обеспечивает защиту информации от намеренного несанкционированного распространения, как сотрудниками, так и посторонними лицами, имеющими какие-то права доступа в систему.

Для того чтобы система DLP имела возможность различать информацию разных категорий, необходимо эти правила установить и передать в систему. Современные системы защиты от утечек имеют сформированный словарь данных и свод правил на обнаружение данных различного типа и перечень действий при таком обнаружении. Однако это не отменяет необходимость тонкой настройки системы с учетом особенностей данных, обрабатываемых в конкретной организации. Проект внедрения DLP является организационно-техническим мероприятием и содержит некоторые стандартизированные процедуры, описание которых приведено в таблице 3.

Таблица 3 - Логическая схема эксплуатации системы DLP [34]

Процедура	Обучение системы принципам классификации информации	Ввод правил реагирования	Выполнение системой DLP операций контроля	Обработка инцидентов

Описание процедуры	Формирование систем принципов и правил определения конфиденциальной информации	Настройка методов реагирования в зависимости от категории обнаруженной информации	Система контролирует, анализирует информацию, в том числе действия пользователей, сопоставляя с определенными правилами и стандартами. В случае определения их нарушения формируется и передается инцидент.	Обработка инцидентов проводится в автоматическом или ручном режимах. В первом случае система блокирует канал передачи данных, во втором – решение принимается офицером безопасности.
Описание ролей участников процесса со стороны подразделений организации	Лица, владеющие информационными ресурсами, оказывают помощь в их классификации и определении мест хранения	Служба информационной безопасности разрабатывает и по мере необходимости уточняет правила определения инцидентов	Офицеры безопасности получают сообщения о сформированных инцидентах	Сотрудники службы информационной безопасности реагируют на сформированные инциденты и рекомендуют способы их исправления

Лица, руководящие информационными ресурсами, называются владельцами информационных ресурсов. Это лица, которые могут определить ценность информации и необходимость ее защиты. Как правило, это руководители подразделений организации.

Вполне возможно возникновение ситуации, когда информационные ресурсы в организации не определены, поэтому в DLP уже существует стандартный набор

правил определения защищаемой информации и правил формирования инцидентов.

Кроме того, как правило, DLP имеет возможность самообучения на основании ввода образцов защищаемой информации с указанием их категорий, вводом образцов баз данных, вводом шаблонов конфиденциальной информации, вводом характерных словосочетаний и фраз в качестве масок определения информации, а также определением исключений.

В настоящее время на рынке представлено большое количество DLP-систем.

Рассмотрим для сравнения некоторые из них, а именно:

Российские:

- Zecurion DLP [41].
- Дозор Джет 4.0.24 [42].

Зарубежные:

- Symantec Data Loss Prevention [40],
- McAfee DLP Endpoint.

Сравнить продукты можно по нескольким критериям:

- позиционирование системы на рынке.
- системные требования.
- используемые технологии детектирования.
- контролируемые каналы передачи данных.
- возможности контроля подключаемых внешних устройств.
- управление системой и обработка инцидентов.
- отчетность.

Для того, чтобы выбрать DLP систему для внедрения на предприятии, будем использовать метода анализ иерархий [22].

Данный метод является математическим инструментом, позволяющим применить системный подход к многокритериальным проблемам принятия решений. Этот метод позволяет в интерактивном режиме определить, какой вариант решения проблемы наиболее согласуется с теми требованиями, которые определены к ее решению.

Целью сравнения в данном случае является выбор наиболее соответствующей DLP системы для предотвращения утечек в информационной системе организации. Для этого сравним три из четырех рассмотренных ранее систем защиты от утечек информации, а именно Zecurion DLP, Symantec DLP, McAfee DLP по десяти независимым характеристикам (три канала утечек, шесть методов предотвращения утечек информации, а также наличие сертификации) [34].

К каналам утечки информации отнесены:

- Электронная почта;
- Интернет-мессенджеры;
- Внешние носители информации;
- Ftp-доступ к удаленным ресурсам;
- Передача данных на печать;
- Клиенты файлообменных сетей.

К методам предотвращения утечек информации относятся:

- разграничения прав доступа пользователей;
- контроль управления подключением внешних устройств;
- обеспечение закрытости программной среды для пользователей и процессов;
- Разделение файловых объектов и процессов между пользователями;
- Контроль доступа к буферу обмена для процессов и пользователей;
- Криптографическая защита данных с использованием аппаратных средств и подключения защищенных баз данных;

Для определения приоритетов составляются матрицы попарных сравнений (таблица 4). Экспертные данные сформулированы на основании выше изложенной информации (характеристиках сравниваемых DLP-систем и представлениях об объекте защиты). Сравнения проводились по шкале значимости от 1 до 9 (1 - одинаковая значимость, 3 - незначительное превосходство и т. д., обратные величины - если сравниваемый объект уступает в данной характеристике).

Таблица 4 - Матрица попарных сравнений

	Канал 1	**Канал 2**	**Канал 3**	**Метод 1**	**Метод 2**	**Метод 3**	**Метод 4**	**Метод 5**	**Метод 6**	**Серт.**

Канал 1	1	1/3	1/5	1	1	1	1	1	1	1/3
Канал 2	3	1	1/3	1	1	1	1	1	1	1/3
Канал 3	5	3	1	1	1	1	1	1	1	1/3
Метод 1	1	1	1	1	1/9	1/7	1/7	1/7	1/7	1/3
Метод 2	1	1	1	9	1	5	3	1	3	1/3
Метод 3	1	1	1	7	1/5	1	1	1/5	1/7	1/3
Метод 4	1	1	1	7	1/3	1	1	1/5	1/7	1/3
Метод 5	1	1	1	7	1	5	5	1	1/3	1/3
Метод 6	1	1	1	7	1/3	7	7	3	1	1/3
Серт.	3	3	3	3	3	3	3	3	3	1

Для каждой из матриц N определяется нормализованный вектор локальных приоритетов, со следующими компонентами:

(1)

где *n* размерность матрицы — *a*j элемент -i-ой строки матрицы. Таким образом, матрице *N* сопоставляется вектор *a.*

Нормирование компонент осуществляется путем деления каждой компоненты вектора *a* на сумму всех компонент этого вектора:

(2)

Далее считаются приоритеты для сравнения альтернатив по всем критериям (таблица 5).

Таблица 5 - Приоритеты сравнения альтернатив по всем критериям

	Канал 1	Канал 2	Канал 3	Метод 1	Метод 2	Метод 3	Метод 4	Метод 5	Метод 6	Серти-Фика-ция
Zecurion DLP	0,08	0,33	0,26	0,33	0,14	0,08	0,08	0,33	0,09	0,08
Symantec DLP	0,46	0,33	0,1	0,33	0,72	0,46	0,46	0,33	0,45	0,18
McAfee DLP	0,46	0,33	0,64	0,33	0,14	0,46	0,46	0,33	0,45	0,73

Полученный вектор приоритетов для сравнения значимости критериев между собой приведен в таблице 6.

Таблица 6 - Приоритеты значимости критериев

Канал 1	Канал 2	Канал 3	Метод 1	Метод 2	Метод 3	Метод 4	Метод 5	Метод 6	Сертифика ция

0,059	0,077	0,1	0,02	0,13	0,057	0,059	0,116	0,139	0,23

Перемножив одну матрицу на другую, получаем итоговый вектор приоритетов для альтернатив (A - 0,17; B - 0,36; C - 0,46).

По результатам проведенных вычислений получаем значения общего ранжирования альтернатив:

A = 0,17; B =0,36; C = 0,46.

Таким образом, наиболее приемлемой альтернативой для оценивающего эксперта является DLP-система McAfee DLP.

На основании представленных характеристик для рассматриваемого предприятия наиболее подходит McAfee DLP.

ЗАКЛЮЧЕНИЕ

Безопасность в ИТ понимается как комплекс мер и воспринимается как единая система. Компьютерная безопасность может иметь разные аспекты, среди которых нет более или менее значимых, здесь важно все. Не получиться вот так взять и убрать часть каких-то мер, иначе система просто не заработает.

Компьютерная безопасность не так сильно отличается от безопасности в начальном значении. В реальных условиях вы никогда не увидите хорошую дверь с хорошим замком на деревянном полуразвалившемся сарае. Аналогично, как и автомобиль с дорогой качественной резиной, но нерабочими тормозами будет очень даже небезопасен. Примерная ситуация складывается и в компьютерной безопасности, где всегда нужно организовывать меры защиты в каждой точке соприкосновения с неспокойной средой. И любой ресурс в такой системе, ПК или сервер, должен быть защищён надлежащим образом. В безопасности должны находится и сами файлы, и вся сеть. Доступ к любым данным лучше всего организовать безопасный, и все сотрудники, которые имеют доступ к информации, становятся звеном в цепочке механизма, отвечающего за работу совокупной СБ.

Рассматриваемый проект описывает информационные активы предприятия и их уязвимости в момент возникновения различных угроз. Стало понятно, что в такие

моменты компания несет убытки, и не только в финансовом плане, а также в отношении репутации предприятия, что ставит под сомнение всю дальнейшую деятельность.

В качестве базового решения по поддержанию безопасности ИС от утечек данных принято решение о развертывании системы защиты от утечек (DLP).

Система безопасного хранения и перемещения конфиденциальных данных включает в себя следующие функции:

• Нахождение – Поиск конфиденциальных и персональных данных в любых местах, учет конфиденциальной информации и автоматизированное управление переносом или удалением данных;

• Отслеживание – Изучение характера применяемости конфиденциальных данных независимо от того, находится ли сотрудник в корпоративной сети или нет;

• Безопасность – Автоматическое принудительное выполнение правил безопасности для постоянной защиты конфиденциальных данных и недопущения их исчезновения из организации;

• Координация – Введение единой политики по всей компании, уведомление об инцидентах и минимизация последствий, подробный анализ контента — и все это выполняется на основе одной платформы.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Баранова Е.К. Информационная безопасность: учебное пособие. – М.: Инфра-М, 2016. – 324 с.
2. Баранова, Бабаш: Криптографические методы защиты информации. Лабораторный практикум. Учебное пособие, М. Кнорус, 2017 г. 254 с.
3. Бирюков А.А. Информационная безопасность. Защита и нападение. – М.: ДМК Пресс, 2016. – 474 с.
4. Бирюков А.А., Информационная безопасность. Защита и нападение, М., ДМК-Пресс, 2017 г., 434 с.
5. Бондарев В.В., Введение в информационную безопасность автоматизированных систем, М. , Издательство МГТУ им. Н.Э.Баумана, 2016 г., 252 с.

6. Борисов М.С., Романов О. В., Основы организационно-правовой защиты информации. Учебное пособие, М. Ленанд, 2018 г, 312 с.
7. Брюс Шнайер, Прикладная криптография. Протоколы, алгоритмы и исходный код на С, М., Вильямс, 2016 г, 1024 с.
8. Воронцова С.В., Обеспечение информационной безопасности в банковской сфере. Монография. - М.: Кнорус, 2015. – 160 с.
9. Вус М.А. Информатика: введение в информационную безопасность / М.А. Вус, В.С. Гусев, Д.В. Долгирев и др. - СПб., 2012. - 156 с.
10. Гашков С. Б., Применко Э. А., Черепнев М. А., Криптографические методы защиты информации, Академия, 2010 г., 304 с.
11. Глинская Е.В., Чичваркин Н.В. Информационная безопасность конструкций ЭВМ и систем. – М.: Инфра-М, 2016. – 118 с.
12. Глобальное исследование утечек информации за 2017 год. [Электронный ресурс] URL: https://www.infowatch.ru/report2017 (дата обращения: 02.08.2018).