МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Кафедра мировой экономики и менеджмента**

**КУРСОВАЯ РАБОТА**

**Обеспечение информационной безопасности на предприятии в сфере торговли**

Работу выполнила \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_К.А.Аксанычева

Факультет экономический курс третий

Направление/специальность 38.05.01 Экономическая безопасность

Научный

руководитель

Доцент, канд.экон.н\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ю.А.Чепурко

Нормоконтролер

Доцент, канд.экон.н\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ю.А.Чепурко

Краснодар 2018

Содержание

[Введение 3](#_Toc512960677)

[1. Теоретические аспекты обеспечения информационной безопасности организации 5](#_Toc512960678)

[1.1.Основы обеспечения информационной безопасности 5](#_Toc512960679)

[1.2. Риски информационной безопасности 8](#_Toc512960680)

[1.3.Система обеспечения информационной безопасности организации 11](#_Toc512960681)

[2. Анализ обеспечение информационной безопасности предприятий торговли, торговых сетей и их инфраструктуры 16](#_Toc512960682)

[2.1.Структура, функции информационной системы предприятия 16](#_Toc512960683)

[2.2. Сервисы информационной системы предприятия 17](#_Toc512960684)

[2.3.Современное состояние информационной безопасности 20](#_Toc512960685)

[3.Совершенствование информационной безопасности предприятий торговли 22](#_Toc512960686)

[3.1.Реализация информационной безопасности 22](#_Toc512960687)

[3.2.Проблемы информационной безопасности торговых предприятий 26](#_Toc512960688)

[3.3.Меры по усовершенствованию информационной безопасности предприятий торговли 27](#_Toc512960689)

[Заключение 30](#_Toc512960690)

[Список использованной литературы 33](#_Toc512960691)

# Введение

Общеизвестно, что введение компьютеров в различные сферы деятельности человека привело к тому, что объемы хранимой в электронном виде информации увеличились до объемов, которые трудно осознать. Эти процессы были, вне всякого сомнения, оправданы, ведь в электронном виде информацию хранить проще, большие объемы данных можно быстро копировать, переписывать, передавать на большие расстояния. Однако есть в подключении компьютера к глобальным сетям и отрицательные стороны – ведь при отсутствии должной степени защиты ваша информация может пострадать от атак через сеть или Интернет.

Потеря коммерческой информации или ее раскрытие злоумышленниками или конкурентами, скорее всего, приведет к убыткам на рынке. Так, кража информации может понизить репутацию фирмы, а что касается подмены информации, то она и вовсе может привести к разорению, не говоря уже о доверии клиентов.

Но проблемы информационной безопасности ныне волнуют не только предпринимателей. Каждый, кто хоть немного знаком с компьютером и сетью интернет знает, насколько неприятно, когда твоя информация попадает в чужие руки. И не важно, будь то письма электронной почты, которые вместо того что бы отправляться одному адресату рассылают копии еще на несколько адресов, или информация набираемая вами в текстовых редакторах. Потеря конфиденциальности – серьезный психологический удар.

Интересно обратить внимание на следующую статистику, отображающую то, какие же можно назвать первоочередные причины повреждения, хищения или утраты информации:

- Вследствие неумышленных ошибок, сделанных самим человеком – владельцев информации – 52 процента случаев;

- Вследствие умышленных действий – 10 процентов;

- Вследствие перегрева носителей и пожаров – 15 процентов;

- Вследствие повреждения водой, попавшей извне или конденсата внутри – около 10 процентов случаев;

- Оставшиеся проценты – тем или иным образом связанные с действиями злоумышленников в сети.

Все вышесказанное обуславливает актуальность темы исследования.

Объект исследования – информационная безопасность.

Предмет исследования – информационная безопасность предприятий в сфере торговли.

Цель исследования – изучить особенности информационной безопасности в сфере торговли.

Для достижения поставленной цели необходимо решение следующих задач:

- выявить угрозы информационной безопасности,

- рассмотреть систему обеспечения информационной безопасности,

- провести анализ обеспечения информационной безопасности в сфере торговли,

- исследовать проблемы информационной безопасности предприятий торговли,

- разработать меры по усовершенствованию информационной безопасности предприятий торговли.

Структура работы представлена введением, тремя главами, заключением и списком использованной литературы.

# 1 Теоретические аспекты обеспечения информационной безопасности организации

# 1.1 Основы обеспечения информационной безопасности

Конфиденциальная для бизнеса информация входит в сферу повышенного интереса конкурирующих компаний. Для недобросовестных конкурентов, коррупционеров и других злоумышленников особый интерес представляет информация о составе менеджмента предприятий, их статусе и деятельности фирмы. Доступ к конфиденциальной информации и ее изменение могут нанести существенный урон финансовому положению компании [2].

При этом информационная утечка может быть даже частичной. В некоторых случаях даже обеспечение хищения 1/5 конфиденциальной информации может иметь критические последствия для финансовой безопасности. Причиной утечки информации, если отсутствует должное обеспечение информационной безопасности организации, могут быть различные случайности, вызванные неопытностью сотрудников.

Для разработки концепции обеспечения информационной безопасности (ИБ) под информацией понимают сведения, которые доступны для сбора, хранения, обработки (редактирования, преобразования), использования и передачи различными способами, в том числе в компьютерных сетях и других информационных системах.

Такие сведения обладают высокой ценностью и могут стать объектами посягательств со стороны третьих лиц. Стремление оградить информацию от угроз лежит в основе создания систем информационной безопасности.

В декабре 2017 года в России принята новая редакция Доктрины информационной безопасности. В документ ИБ определена как состояние защищенности национальных интересов в информационной сфере. Под национальными интересами в данном случае понимается совокупность интересов общества, личности и государства, каждая группа интересов необходима для стабильного функционирования социума.

Правоотношения, связанные с обеспечением информационной безопасности, регулируются федеральными законами «О государственной тайне», «Об информации», «О защите персональных данных» и другими. На базе основополагающих нормативных актов разрабатываются постановления правительства и ведомственные нормативные акты, посвященные частным вопросам защиты информации.

Информационная безопасность предполагает обеспечение защиты данных от хищений или изменений как случайного, так и умышленного характера. Система обеспечения информационной безопасности организации – эффективный инструмент защиты интересов собственников и пользователей информации.

Следует отметить, что ущерб может быть нанесен не только несанкционированным доступом к информации. Он может быть получен в результате поломки коммуникационного или информационного оборудования. Особенно актуальна эффективная организация обеспечения безопасности информационных банковских систем и учреждений открытого типа (учебные, социальные и др.) [8].

Для того чтобы наладить должное обеспечение защиты информации следует иметь четкое представление об основных понятиях, целях и роли информационной безопасности.

Термин «безопасность информации» описывает ситуацию, исключающую доступ для просмотра, модерации и уничтожения данных субъектами без наличия соответствующих прав. Это понятие включает обеспечение защиты от утечки и кражи информации с помощью современных технологий и инновационных устройств.

Защита информации включает полный комплекс мер по обеспечении целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Целостность – понятие, определяющее сохранность качества информации и ее свойств.

Конфиденциальность предполагает обеспечение секретности данных и доступа к определенной информации отдельным пользователям.

Доступность – качество информации, определяющее ее быстрое и точное нахождение конкретными пользователями.

Цель защиты информации – минимизация ущерба вследствие нарушения требований целостности, конфиденциальности и доступности [1].

Таким образом, под защитой информации будет пониматься комплекс правовых, административных, организационных и технических мер, направленных на предотвращение реальных или предполагаемых ИБ-угроз, а также на устранение последствий инцидентов. Непрерывность процесса защиты информации должна гарантировать борьбу с угрозами на всех этапах информационного цикла: в процессе сбора, хранения, обработки, использования и передачи информации.

Информационная безопасность в этом понимании становится одной из характеристик работоспособности системы. В каждый момент времени система должна обладать измеряемым уровнем защищенности, и обеспечение безопасности системы должно быть непрерывным процессом, которые осуществляется на всех временных отрезках в период жизни системы.

В теории информационной безопасности под субъектами ИБ понимают владельцев и пользователей информации, причем пользователей не только на постоянной основе (сотрудники), но и пользователей, которые обращаются к базам данных в единичных случаях, например, государственные органы, запрашивающие информацию. В ряде случаев, например, в банковских ИБ-стандартах к владельцам информации причисляют акционеров – юридических лиц, которым принадлежат определенные данные

Поддерживающая инфраструктура, с точки зрения основ ИБ, включает компьютеры, сети, телекоммуникационное оборудование, помещения, системы жизнеобеспечения, персонал. При анализе безопасности необходимо изучить все элементы систем, особое внимание уделив персоналу как носителю большинства внутренних угроз.

# 1.2 Риски информационной безопасности

Современные предприятия сталкиваются с самыми серьезными рисками для информационной безопасности.

Эти риски имеют как внутренние, так и внешние источники. Информационной безопасности предприятий угрожают:

- проникающие извне хакеры и вредоносные программы

- собственные злонамеренные сотрудники - инсайдеры

- собственные сотрудники - незлонамеренные нарушители

- стихийные бедствия (пожары, наводнения, аварии в энергосистемах и т.д.).

Главные цели атак на информационные системы предприятий:

- получение контроля над ценными ресурсами, например, кража финансовой информации или эксплуатация вычислительных ресурсов корпоративной сети

- ограничение деятельности предприятия по заказу недобросовестных конкурентов или политических оппонентов, например, путем вывода из строя информационной системы, разрушения связей с партнерами и т.д.[12]

Риски для информационной безопасности могут быть реализованы в самом разном виде: вредоносных программ, аппаратных и программных закладок, спам-рассылок, устройств для перехвата сигналов связи, регламентов, допускающих несанкционированный доступ инсайдеров и др.

Различчные методы для нанесения вреда информационной безопасности становятся всё более таргетированными (нацеленными на конкретную отрасль и даже предприятие). Так, в 2010 году была обнаружена специализированная вредоносная программа, атакующая автоматизированные системы оперативного диспетчерского управления производством, – компьютерный червь Stuxnet. Существуют целые классы вредоносных программ, специфичных для отдельных областей экономики, например, троянцы-банкеры.

Успешная компьютерная атака на предприятие может вести к самым неприятным последствиям - финансовому ущербу, снижению репутации и преследованию регуляторных органов.

Наиболее распространенные виды угроз:

1. Неблагоприятная для предприятия экономическая политика государства. Регулирование экономики государством с помощью манипуляций (определение валютного курса, учетная ставка, таможенные тарифы и налоги) является причиной многих противоречий на предприятиях в сфере производства, финансов и коммерции.

Большую опасность для обеспечения безопасности информации предприятия несут административные обязательства выхода на рынок, что приводит к насильственному сужению товарно-денежных отношений, нарушению законов со стороны государства и ограничению деятельности предприятия. Часто государство преувеличивает свою компетентность в финансовой и коммерческой сфере деятельности предприятия и необоснованно вмешивается в пространство информации этих сфер, а также посягает на собственность предприятия в различных формах [3].

Серьезную угрозу для обеспечения безопасности информации предприятия несут политические действия, направленные на ограничение или прекращение экономических связей. Санкции в экономике вызывают у обеих сторон недоверие к дальнейшей деятельности и подрывают коммерческие взаимоотношения. Все это ведет к дестабилизации экономических отношений, и не только на уровне государства.

2. Действия иных хозяйствующих субъектов. В данном случае риск обеспечению безопасности информации несет нездоровая конкуренция. Нездоровая или недобросовестная конкуренция имеет несколько понятий и по нормам международного права разделяется на три вида:

- Когда деятельность одной коммерческой структуры пытаются представить потребителю под видом другой;

- Дискредитирование репутации коммерческого предприятия путем распространения ложной информации;

- Неправомерное и некорректное использование торговых обозначений, вводящих потребителя в заблуждение.

В западных странах существуют законодательные акты по ведению недобросовестной конкуренции, фирменным наименованиям, товарным обозначениям и препятствованию обеспечению безопасности информации, нарушение которых ведет к определенной юридической ответственности. Также к ответственности приводят следующие неправомерные действия:

- Подкуп или переманивание потребителей со стороны конкурента;

- Порядок обеспечения информационной безопасности организации нарушается путем разглашения коммерческих тайн, а также выяснения информации с помощью шпионажа, подкупа;

- Преднамеренное снижение цен для подавления конкуренции;

- Копирование товаров, рекламы, услуг и других форм коммерческой деятельности и информации конкурента.

Следующей формой недобросовестной конкуренции, направленной на препятствование обеспечению безопасности информации, считается физическое подавление в виде посягательства на жизнь и здоровье служащего компании.  В эту категорию входит:

- Организация разбойных нападений на производственные, складские помещения и офисы с целью ограбления;

- Уничтожение, порча имущества и материальных ценностей путем взрыва, поджога или разрушения;

- Захват сотрудников в заложники или физическое устранение.

3. Кризисные явления в мировой экономике.  Кризисы имеют особенность перетекать из одной страны в другую, используя каналы внешних экономических связей. Они также наносят ущерб обеспечению безопасности информации. Это следует учесть, определяя методы и средства обеспечения информационной безопасности организации [3].

Поэтапное интегрирование России в международную экономику способствует зависимости коммерческих предприятий страны от различных процессов, происходящих в мировой экономике (падение и рост цен на энергоносители, структурная перестройка и другие факторы). По степени внедрения национальной экономики в мировую экономическую структуру усиливается ее подверженность внешним факторам. Поэтому, современное производство в стремлении к увеличению прибыли, улучшению деятельности путем модернизации, повышению уровня обеспечения безопасности информации, стабильности обязательно должно обращать внимание на динамику потребительского спроса, политику государства и центральных банков, развитие научно-технического прогресса, на отношение конкурентов, мировую политику и хозяйственную деятельность.

Таким образом, компьютеризация экономики и распространение электронных финансовых транзакций приводят к росту угроз информационной безопасности предприятий. Для обеспечения приемлемого уровня информационной безопасности, вопросам защиты необходимо уделять достаточное внимание. Корпоративные компьютерные системы – это сложные информационные структуры, и поэтому для выполнения проектов по обеспечению их безопасности во многих случаях привлекаются сторонние специализированные компании.

# 1.3 Система обеспечения информационной безопасности организации

Система информационной безопасности для компании – юридического лица включает три группы основных понятий: целостность, доступность и конфиденциальность. Под каждым скрываются концепции с множеством характеристик.

Под целостностью понимается устойчивость баз данных, иных информационных массивов к случайному или намеренному разрушению, внесению несанкционированных изменений. Понятие целостности может рассматриваться как:

- статическое, выражающееся в неизменности, аутентичности информационных объектов тем объектам, которые создавались по конкретному техническому заданию и содержат объемы информации, необходимые пользователям для основной деятельности, в нужной комплектации и последовательности;

- динамическое, подразумевающее корректное выполнение сложных действий или транзакций, не причиняющее вреда сохранности информации [1].

Для контроля динамической целостности используют специальные технические средства, которые анализируют поток информации, например, финансовые, и выявляют случаи кражи, дублирования, перенаправления, изменения порядка сообщений. Целостность в качестве основной характеристики требуется тогда, когда на основе поступающей или имеющейся информации принимаются решения о совершении действий. Нарушение порядка расположения команд или последовательности действий может нанести большой ущерб в случае описания технологических процессов, программных кодов и в других аналогичных ситуациях.

Доступность – это свойство, которое позволяет осуществлять доступ авторизированных субъектов к данным, представляющим для них интерес, или обмениваться этими данными. Отказ системы предоставлять информацию становится проблемой для любой организации или групп пользователей. В качестве примера можно привести недоступность сайтов госуслуг в случае системного сбоя, что лишает множество пользователей возможности получить необходимые услуги или сведения.

Конфиденциальность означает свойство информации быть доступной тем пользователям: субъектам и процессам, которым допуск разрешен изначально. Большинство компаний и организаций воспринимают конфиденциальность как ключевой элемент ИБ, однако на практике реализовать ее в полной мере трудно. Не все данные о существующих каналах утечки сведений доступны авторам концепций ИБ, и многие технические средства защиты, в том числе криптографические, нельзя приобрести свободно, в ряде случаев оборот ограничен.

Равные свойства ИБ имеют разную ценность для пользователей, отсюда – две крайние категории при разработке концепций защиты данных. Для компаний или организаций, связанных с государственной тайной, ключевым параметром станет конфиденциальность, для публичных сервисов или образовательных учреждений наиболее важный параметр – доступность [10].

Объекты защиты в концепциях ИБ

Различие в субъектах порождает различия в объектах защиты. Основные группы объектов защиты:

- информационные ресурсы всех видов (под ресурсом понимается материальный объект: жесткий диск, иной носитель, документ с данными и реквизитами, которые помогают его идентифицировать и отнести к определенной группе субъектов);

- права граждан, организаций и государства на доступ к информации, возможность получить ее в рамках закона; доступ может быть ограничен только нормативно-правовыми актами, недопустима организация любых барьеров, нарушающих права человека;

- система создания, использования и распространения данных (системы и технологии, архивы, библиотеки, нормативные документы);

- система формирования общественного сознания (СМИ, интернет-ресурсы, социальные институты, образовательные учреждения).

Каждый объект предполагает особую систему мер защиты от угроз ИБ и общественному порядку. Обеспечение информационной безопасности в каждом случае должно базироваться на системном подходе, учитывающем специфику объекта.

Категории и носители информации

Российская правовая система, правоприменительная практика и сложившиеся общественные отношения классифицируют информацию по критериям доступности. Это позволяет уточнить существенные параметры, необходимые для обеспечения информационной безопасности:

- информация, доступ к которой ограничен на основании требований законов (государственная тайна, коммерческая тайна, персональные данные);

- сведения в открытом доступе;

- общедоступная информация, которая предоставляется на определенных условиях: платная информация или данные, для пользования которыми требуется оформить допуск, например, библиотечный билет;

- опасная, вредная, ложная и иные типы информации, оборот и распространение которой ограничены или требованиями законов, или корпоративными стандартами.

Средства защиты информации

Для целей разработки концепций ИБ-защиты средства защиты информации принято делить на нормативные (неформальные) и технические (формальные).

Неформальные средства защиты – это документы, правила, мероприятия, формальные – это специальные технические средства и программное обеспечение.

Формальные средства защиты информации:

- Физические средства защиты. Это механические, электрические, электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним.

- Аппаратные средства защиты. Это электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы.

- Программные средства – это простые и системные, комплексные программы, предназначенные для решения частных и комплексных задач, связанных с обеспечением ИБ.

- Специфические средства защиты. Это различные криптографические алгоритмы, позволяющие шифровать информацию на диске и перенаправляемую по внешним каналам связи.

Неформальные средства защиты:

- Нормативные средства. Эта категория средств обеспечения информационной безопасности представлена законодательными актами и нормативно-распорядительными документами, которые действуют на уровне организации.

- Организационные и административные меры. Это и архитектурно-планировочные решения, позволяющие защитить переговорные комнаты и кабинеты руководства от прослушивания, и установление различных уровней доступа к информации.

- Морально-этические меры. Они определяют личное отношение человека к конфиденциальной информации или информации, ограниченной в обороте.

# 2 Анализ обеспечение информационной безопасности предприятий торговли, торговых сетей и их инфраструктуры

# 2.1 Структура, функции информационной системы предприятия

Информационная система является средством информационного обеспечения процесса управления.

Единая информационная система управления предприятием ориентируется на достижение цели: удовлетворения потребностей в информации руководителей всех уровней и звеньев системы управления предприятием в установленные сроки для подготовки, принятия и реализации решений.

Современная информационная система предприятия является автоматизированной, человеко-машинной системой, в которой творческие способности менеджера дополняются возможностями электронно-вычислительной техники, математического моделирования и прогнозирования [2].

Информационная система управления предприятия должна обеспечить (функции):

1. Полноту информации для каждого звена системы управления. Полнота определяется как отношение информации, полученной к запрошенной или необходимой для управления;

2. Полезность и ценность информации. Информационные потоки в системе управления должны направляться по конкретным адресам – конкретным руководителям, специалистам и служащим управленческого аппарата;

3. Точность и достоверность информации – принятие решений на недостаточно точных или недостоверных данных увеличивает риск допущения ошибок, принять неверное решение;

4. Своевременность поступления информации – если информация не поступает вовремя, то орган управления будет бездействовать как раз в тот момент, когда объект управления особенно нуждается в управляющем действии;

5. Агрегируемость информации – рациональное распределение информации по уровням иерархии управления. На высшие уровни управления должна поступать более обобщенная информация, на нижние – более детализированная;

6. Актуальность информации – при принятии решений важно учитывать возраст информации и ее актуальность для конкретных управленческих задач;

7. Экономичность и эффективность обработки информации. Эффективность информационной подсистемы можно оценить, сопоставляю результаты управления с затратами на сбор, накопление, обработку, преобразование и передачу информации [11].

Кроме того, автоматизированная информационная система должна удовлетворять ряд таких технических требований, как:

- надежная защита от несанкционированного доступа к данным;

- регистрация действий персонала;

- удобный пользовательский интерфейс рабочих мест;

- возможность развития системы;

- возможность проведения конвертации данных из использовавшихся ранее в новую систему;

- высокая надежность работы.

Информационная система управления включает субъекты коммуникации, каналы и носители информации, а так же технические средства информационной работы.

# 2.2 Сервисы информационной системы предприятия

Системы управления IT компании или организации являются сложными по своей природе, потому что требуют согласования позиций многих сторон и учета их интересов (спонсоры создания инф. системы, разработчики, конечные пользователи).

Работа IT отдела как субъекта IT менеджмента, охватывает управление всеми компьютерными и коммуникационными ресурсами предприятия. Его основная задача заключается в создании и поддержании рабочего состояния прикладных систем и инфраструктуры, на которой эти системы выполняются. Информационное обслуживание заключается в предоставление информационных услуг (сервисов).

IT-сервис — это IT услуга, которую IT-подразделение (отдел, служба) или внешний провайдер предоставляет бизнес-подразделениям предприятия для поддержки их бизнес-процессов.

Примеры IT-сервисов: эл. почта, сетевая инфраструктура, системы хранения данных, бизнес-аппликации и т.д. Набор IT-сервисов для предприятия является индивидуальным: зависит от потребностей, отрасли, уровня и т.п.

В общем случае IT-сервис определяется по следующим параметрам:

- Функциональность (какую задачу выполняет, где применим)

- Время обслуживания (время, в течение которого IT-отдел поддерживает сервис, то есть несет ответственность за его непрерывное функционирование)

- Доступность (процент времени, когда сервис доступен)

- Надежность (определяется средним временем работы между двумя отказами)

- Производительность (возможность выдерживать некоторый уровень нагрузки)

- Конфиденциальность (вероятность несанкционированного доступа)

- Масштаб (размеры)

- Затраты (стоимость совокупности всех ресурсов, стоимость владения)

В современных условиях информационного развития общей методологической основой процессного подхода к IT-сервисам является подход ITIL / ITSM. Он основан на сборе и систематизации передовой практики управления службой IT в течение последних 20-ти лет.

Иными словами, речь идет об использовании типовых моделей бизнес-процессов службы IT. ITIL — Information Technology Infrastructure Library (Библиотека инфраструктуры информационных технологий) представляет собой некий набор всеобъемлющих, непротиворечивых и согласованных документов, которые созданы на основе знаний и опыта мировых организаций, и используются с целью управления обслуживанием информационных систем.

Библиотека ITIL была создана в результате принятия факта о том, что достижение предприятиями разных сфер деятельности своих корпоративных целей в значительной мере зависит от IT. Эта возрастающая со временем зависимость привела к росту потребности в IT-услугах, качество которых соответствовало бы целям конкретного бизнеса, требованиям и ожиданиям заказчика.

Со временем акцент переместился с разработки IT-приложений на менеджмент IT-услуг. Информационные системы только тогда способствуют достижению корпоративных целей, когда система доступна всем пользователям, и при возникновении ошибок и необходимости модификации поддержка может быть оказана службой сопровождения.

Суть создания ITIL состоит в том, чтобы повысить уровень эффективности информационных систем в процессе выполнения задач предприятия при увеличении организационных требований и снизить расходы на предоставление или модернизацию сервисов (услуг) информационных технологий [8].

На современном этапе развития информационных технологий ITIL — это, по сути, стандарт, который является популярным в бизнес-процессах любой развитой страны. Всего в стандарте указаны 40 функций, включая менеджмент изменений информационной системы, управление рабочими конфигурациями, запросами на обслуживание, планирование развития эксплуатационной и диспетчерской служб.

Непосредственно практическую ценность для управленческого аппарата любой организации ITIL представляет в том, что в нем соединяется весь накопленный опыт организации обслуживания информационных систем. Данный стандарт создает четкое представление относительно критериев разработки эффективной службы использования и концентрирует внимание на принципиально важных составляющих, которые нельзя упускать в процессе построения организационной структуры сервиса.

# 2.3 Современное состояние информационной безопасности

Коммерческие организации всегда считали затраты на обеспечение безопасности неизбежной и пустой тратой средств, а не своим первоочередным делом. Например, у входа в помещение даже небольшой компании вас встретит охранник или система ограничения и контроля доступа. А вот с защитой информации дела обстоят еще не так хорошо. Не все понимают, как можно потерять информацию и во что это выльется.

Урон, наносимый компьютерными преступлениями, можно сопоставить с доходами от незаконного оборота наркотиков и оружия. Только в США ежегодный ущерб, наносимый «электронными преступниками», составляет около 100 млрд долларов [5].

Количество компьютерных преступлений в кредитно-финансовой сфере постоянно возрастает. Например, онлайновые магазины фиксируют до 25% мошеннических платежных операций. Тем не менее, в Западных странах наблюдается активное развитие электронной коммерции — этого сверх рентабельного современного бизнеса.

Параллельно развитию этой сферы увеличиваются и доходы «виртуальных» мошенников. Последние уже не действуют в одиночку, а работают тщательно подготовленными, хорошо технически и программно вооруженными преступными группами при непосредственном участии самих банковских служащих.

Специалисты в области безопасности отмечают, что доля таких преступлений составляет около 70%.

О том, что сфера электронной коммерции вызывает повышенный интерес в криминальной среде, говорят данные одного из опросов, проведенного в 50 странах мира среди 1600 специалистов в области защиты информации. По итогам опроса выяснилось следующее:

- серверы, связанные с продажей продуктов или услуг через сеть Internet, подвергались нападениям приблизительно на 10% чаще, чем серверы, не используемые для проведения финансовых сделок;

- 22% фирм, занимающихся продажами через Web-серверы, имели потери информации, и только 13% компаний, не продающих продукты через Internet, столкнулись с этой же проблемой;

- 12% респондентов, имеющих электронные магазины, сообщили о краже данных и торговых секретов, и только 3 таких случая зафиксировано у компаний, не продающих продукты через систему Web [7].

Эти показатели продолжают расти, но на самом деле цифры не точные. Реально они могут превышать приведенные данные на порядок. Ведь многие потери не обнаруживаются или о них не сообщают. Поэтому, например, в нашей стране, начиная с 1997 года, ежегодно раскрывается всего лишь 10% компьютерных преступлений.

# 3 Совершенствование информационной безопасности предприятий торговли

# 3.1 Реализация информационной безопасности

Современные тенденции развития торговли в России приводят к укрупнению компаний за счет увеличения численности предприятий в их составе, консолидации активов различных операторов, проведения сделок слияний и поглощений, создания сетевых распределительных центров.

В результате растут требования к информационным технологиям и их значимость в организации торговли. Обработка информационных потоков в любой компании требует высоких темпов и абсолютной точности.

Управление современным магазином, предприятием оптовой торговли и торговой сетью предполагает использование автоматизированных систем комплексного торгового, складского и бухгалтерского учета. Сегодня руководители принимают управленческие решения, основываясь на данных, полученных из информационных систем. Таким образом, какова бы ни была структура фирмы, ведение учета договоров, движения товарно-материальных ценностей, денежных средств и бухгалтерского учета должны осуществляться в едином информационном пространстве.

В целях автоматизации управления торговым процессом на предприятии создается информационная система, которая может включать:

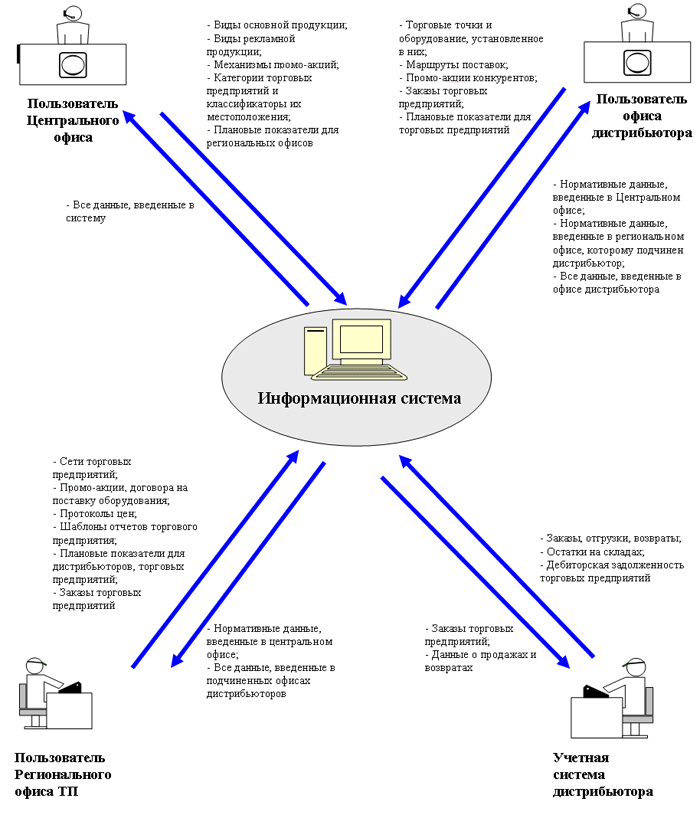


Рисунок 1 - Основные информационные потоки, циркулирующие в системе управления сетевой компании

- внутреннюю систему учета и отчетности (содержит данные об объеме, структуре и скорости товарного производства и обращения, издержках и потерях предприятия, валовых доходах, чистой прибыли, рентабельности и т.д.);

- систему маркетинговой информации (позволяет отслеживать текущее состояние, тенденции и перспективы развития рынка). Данную информационную систему можно определить и как разведывательную, т.к. она обеспечивает сбор, обработку и анализ данных о деятельности конкурентов.

Данные в информационную систему поступают от персонала компании и из офисных систем дистрибьюторов. В дальнейшем они используются для оперативного управления предприятием, контроля и анализа деятельности компании в целом, региональных представительств и дистрибьюторов. Потребителями данных информационной сети являются менеджеры и руководители компании, и фирм- дистрибьюторов. На рисунках 1 и 2 приведены основные информационные потоки, циркулирующие в системе управления торговым предприятием (торговой сетью), показаны их основные источники и потребители.

Руководителю предприятия, финансовому директору, главному бухгалтеру, старшим менеджерам для принятия стратегических управленческих решений крайне необходимо представлять полную картину состояния предприятия и тенденций его развития (рисунок 1).

На рабочих местах в бухгалтерии, в торговом зале, на складе работники имеют дело лишь с отдельными фрагментами общего информационного потока. Их задачи и функции, как правило, сводятся к оформлению и учету прихода и расхода товаров, выписке счетов, работе на кассовом аппарате и т.д. (рисунок 2).

Учитывая риски торговых предприятий и уязвимость информационных систем, представляется безответственным такой подход, при котором компания реагирует на события после того, как они происходят. Отсюда следует, что в компании должна быть создана система информационной безопасности. Она является одним из основных элементов системы управления.

Остановка работы информационной системы может вызвать необратимые последствия для бизнеса.

Исходными данными создания эффективной системы информационной безопасности должны быть четкие представления о ее целях и структуре, о видах угроз и их источниках, о возможных мерах противодействия.

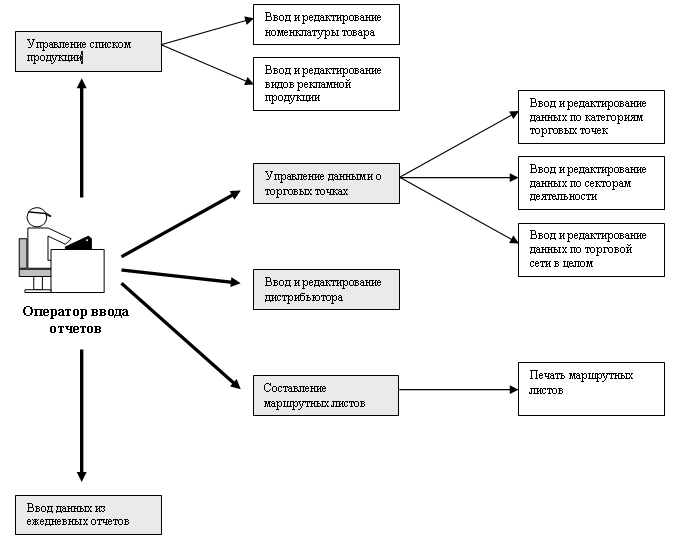


Рисунок 2 - Система обмена данными для сотрудников различных подразделений торгового предприятия или торговой сети

Внешние риски для ИБ чаще всего исходят от конкурентов, криминальных группировок, коррупционеров в составе правовых и административных органов власти.

Внутренние риски для ИБ представляют наибольшую опасность. Они могут исходить от некомпетентных руководителей, недобросовестного и малоквалифицированного персонала,. Отдельные сотрудники с высоким уровнем самооценки, из-за неудовлетворенности своих амбиций (уровень зарплаты, отношения с руководством, коллегами и пр.) могут инициативно выдать коммерческую информацию конкурентам, попытаться уничтожить важную информацию или пассивные носители, например, внести компьютерный вирус.

Проблема принятия мер по обеспечению информационной безопасности на предприятиях в сфере торговли актуальна. Мало предприятий, которых будут устраивать убытки. Руководители компаний должны осознать важность информационной безопасности, научиться предвидеть будущие тенденции и управлять ими. Эффективная работа систем безопасности должна стать первоочередной задачей для всего предприятия в целом.

Реализация программы защиты информации должна осуществляться на основе комплексного использования систем и средств безопасности исходя из предпосылки, что невозможно обеспечить требуемый уровень защищенности только с помощью одного отдельного средства или мероприятия, или их простой совокупности. Необходимо их системное согласование. В этом случае реализация любой угрозы может воздействовать на защищаемый объект только в случае преодоления всех уровней защиты.

# 3.2 Проблемы информационной безопасности торговых предприятий

Современное толкование понятий информационной безопасности и защищенности конфиденциальной информации во все большей степени находит свое отражение в комплексном, системном подходе к созданию системы защиты данных, необходимой для создания условий принятия обоснованного управленческого решения во всех сферах деятельности государства.

По данным экспертов, количество выявленных ИТ- преступлений в РФ удваивается ежегодно. В настоящее время особый статус приобретает проблема информационной безопасности в экономической сфере, что обусловлено, прежде всего, недостаточностью уровня развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг.

Отягощающим фактором является высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий, касающихся аппаратно-программных средств и средств связи. Потому стратегическими целями о области информационной безопасности в экономической сфере являются минимизация уровня негативного воздействия дестабилизирующих факторов, связанных с недостаточностью развития отечественной отрасли информационных технологий и средств вычислительной техники, разработка конкурентоспособных средств обеспечения информационной безопасности, а также повышение качества услуг в сфере обеспечения информационной безопасности.

Аналитический центр InfoWatch опубликовал данные по утечке данных в России за последний год. Согласно исследованию, СМИ обнародовали 213 случаев утечек информации из российских госорганов и компаний, что составляет 14% от общемирового количества утечек. Самые частые случаи — это утечка платежной информации и персональных данных — 80%. В 68% случаев виновными оказываются сотрудники организаций, и только в 8% — руководство.

По сравнению с прошлыми годами количество утечек выросло на 89%. На сегодня Россия занимает второе после США место в списке стран, наиболее сильно страдающих от утечек информации.

# 3.3 Меры по усовершенствованию информационной безопасности предприятий торговли

Хоть и количество угроз постоянно растет, появляются все новые и новые вирусы, разработчики средств защиты информации тоже не стоят на месте. На каждую угрозу разрабатывается новое защитное ПО или совершенствуется уже имеющееся.

Среди средств информационной защиты можно выделить: Физические средства защиты информации. К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами. Большое распространение получили HID-карты для контроля доступа.

Например, при внедрении этой системы, пройти в серверную или другое важное подразделение компании могут лишь те, кому такой доступ предоставлен по протоколу. Базовые средства защиты электронной информации. Это незаменимый компонент обеспечения информационной безопасности компании. К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции. Корпоративные почтовые ящики обязательно должны быть оборудованы такими системами.

Кроме того, необходима организация дифференцированного доступа к информации и систематическая смена паролей.

Так же, резервное копирование данных. Это решение, подразумевающее хранение важной информации не только на конкретном компьютере, но и на других устройствах: внешнем носителе или сервере. В последнее время особенно актуальной стала услуга удаленного хранения различной информации в «облаке» дата-центров. Именно такое копирование способно защитить компанию в случае чрезвычайной ситуации, например, при изъятии сервера органами власти. Создать резервную копию и восстановить данные можно в любое удобное для пользователя время, в любой географической точке.

План аварийного восстановления данных. Крайняя мера защиты информации после потери данных. Такой план необходим каждой компании для того, чтобы в максимально сжатые сроки устранить риск простоя и обеспечить непрерывность бизнес-процессов. Если компания по каким-то причинам не может получить доступ к своим информационным ресурсам, наличие такого плана поможет сократить время на восстановление информационной системы и подготовки ее к работе. В нем обязательно должна быть предусмотрена возможность введения аварийного режима работы на период сбоя, а также все действия, которые должны быть предприняты после восстановления данных.

Итак, защита информации должна осуществляться комплексно, сразу по нескольким направлениям. Чем больше методов будет задействовано, тем меньше вероятность возникновения угроз и утечки, тем устойчивее положение компании на рынке.

# Заключение

Информационная безопасность предполагает обеспечение защиты данных от хищений или изменений как случайного, так и умышленного характера. Система обеспечения информационной безопасности организации – эффективный инструмент защиты интересов собственников и пользователей информации.

Следует отметить, что ущерб может быть нанесен не только несанкционированным доступом к информации. Он может быть получен в результате поломки коммуникационного или информационного оборудования. Особенно актуальна эффективная организация обеспечения безопасности информационных банковских систем и учреждений открытого типа (учебные, социальные и др.).

Термин «безопасность информации» описывает ситуацию, исключающую доступ для просмотра, модерации и уничтожения данных субъектами без наличия соответствующих прав. Это понятие включает обеспечение защиты от утечки и кражи информации с помощью современных технологий и инновационных устройств.

Современные предприятия сталкиваются с самыми серьезными рисками для информационной безопасности.

Эти риски имеют как внутренние, так и внешние источники. Информационной безопасности предприятий угрожают:

- проникающие извне хакеры и вредоносные программы

- собственные злонамеренные сотрудники - инсайдеры

- собственные сотрудники - незлонамеренные нарушители

- стихийные бедствия (пожары, наводнения, аварии в энергосистемах и т.д.).

Способы нанесения вреда информационной безопасности становятся всё более таргетированными (нацеленными на конкретную отрасль и даже предприятие).

Система информационной безопасности для компании – юридического лица включает три группы основных понятий: целостность, доступность и конфиденциальность. Под каждым скрываются концепции с множеством характеристик.

Под целостностью понимается устойчивость баз данных, иных информационных массивов к случайному или намеренному разрушению, внесению несанкционированных изменений.

Современная информационная система предприятия является автоматизированной, человеко-машинной системой, в которой творческие способности менеджера дополняются возможностями электронно-вычислительной техники, математического моделирования и прогнозирования.

Системы управления IT компании или организации являются сложными по своей природе, потому что требуют согласования позиций многих сторон и учета их интересов (спонсоры создания инф. системы, разработчики, конечные пользователи).

Современные тенденции развития торговли в России приводят к укрупнению компаний за счет увеличения численности предприятий в их составе, консолидации активов различных операторов, проведения сделок слияний и поглощений, создания сетевых распределительных центров. Современное толкование понятий информационной безопасности и защищенности конфиденциальной информации во все большей степени находит свое отражение в комплексном, системном подходе к созданию адекватной, упреждающей системы защиты данных, необходимой для создания условий принятия обоснованного управленческого решения во всех сферах деятельности государства.

По данным экспертов, количество выявленных ИТ- преступлений в РФ удваивается ежегодно. В настоящее время особый статус приобретает проблема информационной безопасности в экономической сфере, что обусловлено, прежде всего, недостаточностью уровня развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг.

На данный момент появляются все новые и новые вирусы. На каждый вирус разрабатывается новое защитное ПО или совершенствуется уже имеющееся.

Таким образом, можно сделать вывод, что защита информации должна осуществляться в совокупности по всем направлениям. И чем больше приемов и технологий будет задействовано, тем меньше вероятность возникновения угроз и утечки, тем устойчивее положение компании на рынке.

# Список использованных источников

1. Галатенко В. А. «Основы информационной безопасности». — «Интернет-Университет Информационных Технологий — ИНТУИТ.ру», 2014. — 280 с. Курс лекций
2. Галатенко В. А. Стандарты информационной безопасности. — ИНТУИТ.ру», 2014. 326 с., Курс лекций
3. Современные подходы к обеспечению информационной безопасности. Часть 2. Информационный бюллетень Microsoft. http://www.microsoft.com/Rus/Government/Newsletters/Issue22/Default.mspx
4. Александр Астахов. Разработка эффективных политик информационной безопасности. 30.01.2014. Журнал "Директор ИС", #01, 2014 год // Издательство "Открытые системы".
5. Елена Шашенкова. Свести простои к минимуму. 27.04.2018
6. Дидковский И. Защита вашей переписки. http://langos.lrn.ru/pubs/
7. Нишпель Маркус. Управление компонентами на базе правил. Журнал "LAN", №05, 2017 год // Издательство "Открытые системы".
8. Узварик А. Отказоустойчивые системы хранения. 05.07.2015. Журнал "LAN", №07, 2017 год // Издательство "Открытые системы".
9. Род Лаура. Средства защиты, которые не нужны? 25.10.2015 Еженедельник "Computerworld", №39, 2015 год // Издательство "Открытые системы".
10. Покровский П. Что дороже - ущерб или безопасность? 21.10.2016. Директор ИС, №10/2016
11. Коржов В. Информационная оборона. 27.10.2016 Открытые системы, №10/2016
12. Коржов В. Безопасность в КУБе. 29.11.2017 Computerworld, №44/2017