Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №1

Разработка и внедрение политики безопасности

Консалтинговой компании

Студента: Дубалеко В.В.

ФИТ 3 курс 4 группа

Преподаватель: Берников В.О.

Минск 2020

**Оглавление**

[**Введение** 3](#_Toc33614616)

[**Обоснование актуальности** 4](#_Toc33614617)

[**Описание структуры организации** 5](#_Toc33614618)

[**Основные угрозы и их источники** 8](#_Toc33614619)

[**Оценка угроз, рисков и уязвимостей** 11](#_Toc33614620)

[**Условная численная шкала для оценки ущерба агентству от НСД** 13](#_Toc33614621)

[**Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам агентства** 14](#_Toc33614622)

[**Разработка мер защиты** 16](#_Toc33614623)

[**Вывод** 22](#_Toc33614624)

# **Введение**

Информационная безопасность – это состояние защищённости информационной среды, защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Информационная безопасность организации – состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.

Под информационной безопасностью подразумевается сохранение следующих характеристик:

Конфиденциальность: предоставление доступа к информации только тем, у кого есть право на доступ к ней;

Целостность**:** защита точности и полноты информации и методов обработки;

Доступность: обеспечение доступа к информации и связанным с ней ресурсам авторизированным пользователям по мере необходимости.

Информационная безопасность достигается путем внедрения совокупности необходимых средств защиты, в число которых могут входить политики, рекомендации, инструкции, организационные структуры и программные функции. Любая организация должна определить требования к безопасности. При оценке требований используются три основных показателя.

# **Обоснование актуальности**

На сегодняшний момент тяжело представить современный мир без тех технологий, которыми мы пользуемся. Каждая компания и организация использует различные технические устройства, многие процессы автоматизированы, множество систем работает по написанным программам, а человеку остаётся лишь контролировать процесс исполнения деятельности, и писать новые программы для большего ускорения процессов. С помощью современных программ, а также компьютерных технологий, люди достигли больших высот и преобразований почти во всех сферах жизни общества. Однако, это имеет свои уязвимые аспекты, во-первых, человек стал зависим от своих технологий, во-вторых, теперь уязвимость одной технологии может привести к полной уязвимости организации, и есть те, кто может этим воспользоваться в корыстных целях. Несомненно, обычный пользователь персонального компьютера в большинстве случаев не может обезопасить даже свой компьютер, именно поэтому появилась такая специальность как информационная безопасность, её главная цель – это обеспечение безопасности информации.

Вопрос информационной безопасности актуален не только в контексте защиты от оппонентов в корпоративных войнах – он не менее важен в условиях, когда сотрудники правоохранительных органов, не всегда на законных основаниях и не всегда с законными целями, получают конфиденциальную информацию граждан.

# **Описание структуры организации**

Разнообразие структур управления консалтинговыми фирмами объясняется их размерам, направлениям деятельности и особенностями организационных культур. Рассмотрим наиболее распространенные из них.  
Линейно-функциональная структура управления, в основу которой положен принцип единоначалия, является формализованной многоуровневой иерархией.  
Такой тип структуры в основном является наиболее эффективным в случаях:

* необходимость решения стабильных задач и выполнения повторяющихся процессов;
* относительно одинаковых обязанностей исполнителей и ограниченного количества информации, приказов и распоряжений.

Саму многоуровневую структуру можно представить в виде управленческой пирамиды. Рассмотрим более подробно уровне пирамиды:

Первый уровень - консультанты без рангов, которые в одиночку или бригадами выполняют работу для клиента.

Второй уровень - руководители операции, которые ответственны за бригаду или отдельных консультантов. Их главными функциями являются:

* планирование работы консультантов
* контроль за выполнением работы
* информирование руководства фирмы о ходе выполнения работ и труда каждого консультанта
* осуществление связи консультантов с руководством клиентской организации

Руководитель операций - консультант, имеет хорошую рекомендацию и трех-четырехлетний стаж работы в данной консультационной фирме.  
Наставник - ответственный за консультантов, работающих по одному на объектах, территориально расположенных недалеко друг от друга. В его функции входит обсуждение проблем и, в случае необходимости, их решение.

Третий уровень - совладельцы фирмы, которые несут формальную ответственность перед клиентом за работу, выполняемую консультантом или бригадами консультантов фирмы. Как правило, совладельцами также являются региональные вице-президенты, президент и исполнительный комитет. К основным функциям в роли совладельцев можно смело отнести:

* проведение предварительных переговоров о проблемах и работу, которую необходимо выполнить
* подготовка контракта
* формирование бригады консультантов
* общее наблюдение за ходом работы
* решение конфликтных ситуаций, возникающих между консультантами и клиентом
* корректировка отчета о проделанной работе и передача его руководству компании клиента.

Ответственные за операции могут возглавлять отдел или специализированное отделение компании. Они отчитываются перед высшим руководством о развитии специализированных отделов или департаментов, за которые они отвечают. Наверху пирамиды находится директор-распорядитель (председатель исполнительного комитета). Также к высшему руководству компании принадлежат президент и председатель исполнительного комитета Характерной чертой консультационных фирм является обязанность всех сотрудников, независимо от иерархии и должности в компании, заниматься консультационной деятельностью.

Линейно-функциональная структура в управлении применяется в случае многопрофильной деятельности фирмы, которая специализируется как по отраслевому, так и функциональному принципу, имеющая региональную сеть, а также филиалы в других странах. Свойством таких компаний является создание вспомогательных подразделений, которые упрощают работу основных департаментов организации. Вспомогательные службы призваны выполнять следующие задачи:

* отбор, подготовку и усовершенствование кадров фирмы
* оказание помощи в работе консультантов
* расширение клиентуры компании

Отдел или служба информации (информационно-исследовательский) и библиотека позволяют более эффективно работать с информацией и упростить работу консультантов. Эти отделы занимаются работой, связанной с поиском нового в области теории и практики управления, систематизацией и переработкой полученной информации, осуществляют анализ опыта, накопленный консультантами при проведении исследований.

Центры по совершенствованию персонала консультационной фирмы (учебные центры) предназначены для проведения занятий с руководителями предприятий с использованием информации о новинках в области управления, а также примеров и ситуаций.

Консультационная работа неразрывно связана с исследованием управленческих процессов и подготовкой управленческих кадров. Поэтому создание структуры, в которой присутствуют все эти виды отделов, позволяет совместить опыт консультантов с творческим поиском.

Матричная структура управления, как правило, создается на базе функциональной структуры. Во время своего роста консультационная фирма идет путем «захвата» новых районов, стран и континентов. Это требует создания региональных отделений, обслуживающих тот или иной регион. Ими могут быть временные группы, занятые поиском новых клиентов; крупные конторы, способны самостоятельно предоставлять консультации по широкому кругу проблем.

Главная идея структуры управления региональных отделений состоит в том, что члены целевой группы или бригады, включая как консультантов региональных отделений, так и специалистов из функциональных отделов, находятся в двойном подчинении: временном - у руководителя регионального отделения; постоянном - в руководителя функционального отделения.

Создание временных целевых групп получило широкое развитие в проектном управлении. Объективный процесс усложнения уровня решаемых проблем, и специализация консультантов в отдельных отраслях знаний требуют создания временных групп для более успешной работы. Именно они являются ядром матричной структуры.

Преимуществами матричной структуры консалтингового бизнеса является возможность гибко маневрировать за счет перераспределения консультантов между проектами, а также привлекать вспомогательных специалистов (это повышает качество работы и обеспечивает максимальную скорость выполнения задач при минимальных затратах).

Создание матричной структуры по проектному принципу позволяет менеджеру проекта объединить консультантов из разных функциональных подразделений для выполнения проектных работ. Менеджер проекта отвечает на вопрос «что и когда должно быть выполнено?» Функциональный руководитель - «кто и каким образом будет выполнять работу».

Организационная структура филиалов строится по функциональному принципу. Она позволяет снизить расходы, связанные с переездами консультантов, облегчить поиск клиентов, ознакомиться со спецификой многих стран. Преимуществами такого структурирования является хранение традиций и политики головной компании, возможность обучения консультантов в главном центре, понимание кадров внутри компании, преодоление языкового барьера в общении с клиентами и проведение регулярных встреч, семинаров главным и региональными отделениями.  
Плоскостная структура, как разновидность матричной, строится по принципу уменьшения уровней иерархии и сокращение звеньев между рабочим консультантом и главным управляющим. Это способствует развитию сотрудничества и преодолению барьеров служебного положения внутри фирмы.

Организационная структура фирм, ведущих агрессивный сбыт, предусматривает создание специальных маркетинговых подразделений, осуществляющих поиск потенциальных клиентов и их поощрение к использованию консультационной помощи. Компании, придерживающиеся политики агрессивного сбыта, используют в своей практике маркетинговый опыт отдельных ведущих консультантов-партнеров, имеющих определенный авторитет в бизнес-среде. Привлечение опытных работников к маркетингу продукта некоторой конкретной фирмы способствует персонификации консультационных услуг и формированию доверия клиентов.

Сегодня можно наблюдать такие тенденции развития консультационных фирм: во-первых, быстрое расширение крупных консультационных компаний, спектр услуг которых постоянно увеличивается, во-вторых, мелкие, узкоспециализированные фирмы не проявляют заметной тенденции к диверсификации.

# **Основные угрозы и их источники**

Под угрозой информационной безопасности обычно принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию.

Такие угрозы, воздействуя на ресурсы, могут привести к искажению данных, копированию, ограничению или блокированию к ним доступа. В настоящее время известно достаточно большое количество различных угроз, которые классифицируют по различным признакам.

По природе возникновения различают естественные и искусственные угрозы. К первой группе относятся те, что вызваны воздействием на компьютерную систему объективных физических процессов или стихийных природных явлений. Вторая группа – те угрозы, которые обусловлены деятельностью человека.

По степени преднамеренности проявления, угрозы разделяют на случайные и преднамеренные.

Также есть разделение в зависимости от их непосредственного источника, в качестве которого может выступать природная среда (например, стихийные бедствия), человек (разглашение конфиденциальных данных), программно-аппаратные средства: санкционированные (ошибка в работе операционной системы) и несанкционированные (заражение системы вирусами).

Случайными, или непреднамеренными называются такие угрозы, которые не связаны с действиями злоумышленников. Механизм их реализации изучен достаточно хорошо, поэтому существуют разработанные методы противодействия.

Аварии и стихийные бедствия представляют особую опасность для компьютерных систем, так как они влекут за собой наиболее негативные последствия. Вследствие физического разрушения систем информация становится недоступной, либо утрачивается. Кроме того, невозможно полностью избежать или предупредить сбои и отказы в сложных системах, в результате которых, как правило, хранящаяся на них информация искажается или уничтожается, нарушается алгоритм работы технических устройств.

Ошибки, которые могут быть допущены в процессе разработки компьютерной системы, включая неверные алгоритмы работы и некорректное программное обеспечение, способны привести к последствиям, которые аналогичны тем, что происходят при сбое и отказе в работе технических средств. Более того, подобные ошибки могут использоваться злоумышленниками в целях воздействия на ресурсы системы.

Ошибки пользователей приводят к ослаблению информационной безопасности в 65% случаев котоые случаются. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками на предприятиях приводит к уничтожению, нарушению целостности и конфиденциальности информации.

Выделяют также преднамеренные угрозы, которые всегда связаны с целенаправленными действиями нарушителя. Изучение этого класса затруднено, так как он имеет очень динамичный характер и постоянно пополняется новыми видами угроз.

Для проникновения в компьютерную систему с целью дальнейшего хищения или уничтожения информации используются такие методы и средства шпионажа, как прослушивание, хищение программ, атрибутов защиты, документов и носителей информации, визуальное наблюдение и другие.

При несанкционированном доступе к данным обычно используют штатные аппаратные и программные средства компьютерных систем, вследствие чего нарушаются установленные правила разграничения доступа пользователей или процессов к информационным ресурсам. Самые распространенные нарушения – это перехват паролей (производится с помощью специально разработанных программ), выполнение каких-либо действий под именем другого человека, а также использование злоумышленником привилегий законных пользователей.

Угрозы, с которыми предстоит столкнуться компании можно разделить на классификации:

* хищение (копирование) информации;
* уничтожение информации;
* модификация (искажение) информации;
* нарушение доступности (блокирование) информации;
* отрицание подлинности информации;
* навязывание ложной информации.

Хищение - действия совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.

Копирование компьютерной информации - повторение и устойчивое запечатление информации на машинном или ином носителе.

Уничтожение - внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

Повреждение - изменение свойств имущества при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.

Модификация компьютерной информации - внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

Блокирование компьютерной информации - искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

Несанкционированное уничтожение, блокирование модификация, копирование информации - любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

Обман (отрицание подлинности, навязывание ложной информации) - умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Для хранения информации данной компании используется база данных. Очень часто злоумышленники используют специальные вредоносные программы:

* «компьютерные вирусы» — это небольшие программы, способные самостоятельно распространятся после внедрения в компьютер путем создания своих копий. При определенных условиях вирусы оказывают негативное воздействие на систему;
* «черви» – утилиты, которые активируются при каждой загрузке компьютера. Они обладают способностью перемещаться в пределах системы или сети и размножаться аналогично вирусам. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти, а затем к блокировке работы;
* «троянские кони» — такие программы «скрываются» под видом полезного приложения, а, на самом деле, наносят вред компьютеру: разрушают программное обеспечение, копируют и пересылают злоумышленнику файлы с конфиденциальной информацией и т.д.

Информация, которая содержит в себе данные о услугах, заработных платах сотрудников и т.д., храниться в базе данных, и имеет большую ценность. Если доступ получит злоумышленник, тогда эта информация может использоваться для противоправных действий. Получив доступ к базе данных, злоумышленник может изменить цену на услуги, заработные выплаты сотрудникам или расчетные счета поставщиков, тем самым нарушит экономику компании.

# **Оценка угроз, рисков и уязвимостей**

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

* по расположению источника угроз (внешние, внутренние):
* источниками внутренних угроз являются:
* сотрудники;
* программное обеспечение;
* аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

Ошибки пользователей и системных администраторов; нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации; ошибки в работе программного обеспечения; отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

Формами проявления внешних угроз являются:

заражение компьютеров вирусами или вредоносными программами; несанкционированный доступ (НСД) к корпоративной информации; информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб; действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации; аварии, пожары, техногенные катастрофы.

* по степени преднамеренности проявления (случайные и преднамеренные:
* случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия, ошибки пользователей и т.п.).
* преднамеренные (умышленные действия, например, шпионаж, диверсия, перехват информации, хакерские атаки, фальсификация документов и т.п.)
* по размерам наносимого ущерба:
* общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба).
* локальные (причинение вреда отдельным частям объекта безопасности).
* частные (причинение вреда отдельным свойствам элементов объекта безопасности).
* по степени воздействия на информационную систему:
* пассивные (структура и содержание системы не изменяются).
* активные (структура и содержание системы подвергается изменениям).

По аспекту информационной безопасности, на который направлены угрозы:

* угрозы [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (неправомерный доступ к информации);
* угрозы [целостности](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (неправомерное изменение данных);
* угрозы [доступности](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

Для фирмы характерно хозяйственное внутриорганизационное управление, так как агентство не является муниципальным и относится к сфере дополнительных услуг. Также в фирме имеет место техническое управление, применяемое для технической поддержки сайта и электронного документооборота.

# **Условная численная шкала для оценки ущерба агентству от НСД**

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ. При оценивании рисков учитывается:

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами: количественными (например, стоимостными), качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный) или их комбинацией.

Таблица 1 –Шкала для оценки ущерба Консалтинговой-компании от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 1 | Раскрытие данных принесет ничтожно малый моральный и экономический ущерб компании |
| 2 | Ущерб от атаки есть, но основные операции и положения затронуты не будут |
| 3 | Значительные финансовые потери и потери доверия со стороны клиента, ощутимая часть которых уйдет |
| 4 | Потери очень значительные, компания теряет свое положение на рынке на период до 2-ух лет. Для восстановления положения потребуются крупные финансовые займы |
| 5 | Компания прекращает существование |

Несанкционированный доступ – это доступ к некоторой [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) с нарушением  [должностных полномочий](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BB%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D0%BD%D1%8B%D0%B5_%D0%BB%D0%B8%D1%86%D0%B0) сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации. Также несанкционированным доступом в отдельных случаях называют получение доступа к информации лицом, имеющим [право на доступ](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B0_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0) к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

# **Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам агентства**

Таблица 2 – Шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

С помощью данных таблиц можно рассчитать риски, которым могут быть подвержены компоненты системы. На этапе анализа таблицы риски задаются максимально допустимым уровнем (порогом) – значением 0,5.

Таблица 3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Хищение личных данных отдельного клиента сотрудником компании | 1 | 0,1 | 0,1 |
| Хищение клиентской базы сотрудником компании | 2 | 0,1 | 0,2 |
| Хищение личных данных отдельного клиента человеком внешним для компании | 2 | 0,1 | 0,2 |
| Хищение клиентской базы человеком внешним для компании | 2 | 0,1 | 0,2 |
| Удаление базы данных клиентов с главного компьютера | 1 | 0,1 | 0,1 |
| Распространение исследований компании | 2 | 0,1 | 0,2 |
| Ненадежность программ, используемых компании для ведения внутренних процессов | 2 | 0,1 | 0,2 |

Продолжение Таблицы 3

|  |  |  |  |
| --- | --- | --- | --- |
| Аппаратные ошибки в настройке локальной сети компании | 3 | 0,1 | 0,3 |
| Программные ошибки в настройке локальной сети компании | 2 | 0,1 | 0,2 |
| Недостаточная квалификация сотрудников | 3 | 0,1 | 0,3 |

Оценка риска - установление (идентификация) соответствия опасности и возможных ее источников, исследование механизмов их возникновения, оценка вероятности возникновения опасных событий и их последствий. Оценка риска является компонентом анализа риска, относящимся к качественному и предварительному количественному определению риска и его составных элементов при сопоставлении, разработке и реализации новых объектов, а также при определении и назначении сроков безопасной эксплуатации действующих объектов.

# **Разработка мер защиты**

Любая система безопасности, в принципе, может быть вскрыта. Эффективной считают такую защиту, стоимость взлома которой соизмерима с ценностью добываемой при этом информации.

Применительно к средствам защиты от несанкционированного доступа определены семь классов защищенности (1 - 7) средств вычислительной техники и девять классов (1А, 1Б, 1В, 1Г, 1Д, 2А, 2Б, 3А, 3Б) автоматизированных систем. Для средств вычислительной техники самым низким является класс 7, а для автоматизированных систем - 3Б.

Технические, организационные и программные средства обеспечения сохранности и защиты от несанкционированного доступа

Существует четыре уровня защиты компьютерных и информационных ресурсов, которые нужно соблюдать:

* Предотвращение предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.
* Обнаружение предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.
* Ограничение уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.

Восстановление обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

Для улучшенной защиты информационной безопасности, следует ввести следующие меры:

1. Аутентификация пользователей.

Данная мера требует, чтобы пользователи выполняли процедуры входа в компьютер, используя это как средство для идентификации в начале работы. Для аутентификации личности каждого пользователя нужно использовать уникальные пароли, не являющиеся комбинациями личных данных пользователей, для пользователя. Необходимо внедрить меры защиты при администрировании паролей, и ознакомить пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению. Если в компьютере имеется встроенный стандартный пароль, его нужно обязательно изменить.

Еще более надёжное решение состоит в организации контроля доступа в помещения или к конкретному компьютеру сети с помощью идентификационных пластиковых карточек с встроенной микросхемой - так называемых микропроцессорных карточек (smart - card). Их надёжность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Установка специального считывающего устройства таких карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

Существуют также различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д.

2. Защита пароля.

Следующие правила полезны для защиты пароля:

* нельзя делится своим паролем ни с кем;
* пароль должен быть трудно угадываемым;
* для создания пароля нужно использовать строчные и прописные буквы, а еще лучше позволить компьютеру самому сгенерировать пароль;
* не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным;
* предпочтительно использовать длинные пароли, так как они более безопасны, лучше всего, чтобы пароль состоял из 6 и более символов;
* пароль не должен отображаться на экране компьютера при его вводе;
* пароли должны отсутствовать в распечатках;
* нельзя записывать пароли на столе, стене или терминале, его нужно держать в памяти;
* пароль нужно периодически менять и делать это не по графику;
* на должности администратора паролей должен быть самый надежный человек;
* не рекомендуется использовать один и тот же пароль для всех сотрудников в группе;
* когда сотрудник увольняется, необходимо сменить пароль;
* сотрудники должны расписываться за получение паролей.

3. Процедуры авторизации.

В организации, имеющей дело с критическими данными, должны быть разработаны и внедрены процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям.

В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Если информация обрабатывается на большом вычислительном центре, то необходимо контролировать физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана. Ответственный за информационную безопасность должен знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

4. Предосторожности при работе.

Рекомендуется:

* отключать неиспользуемые терминалы;
* закрывать комнаты, где находятся терминалы;
* разворачивать экраны компьютеров так, чтобы они не были видны со стороны двери, окон и прочих мест, которые не контролируются;
* установить специальное оборудование, ограничивающее число неудачных попыток доступа, или делающее обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру
* использовать программы отключения терминала после определенного периода неиспользования;
* выключать систему в нерабочие часы;
* использовать системы, позволяющие после входа пользователя в систему сообщать ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов.

5. Физическая безопасность.

В защищаемых компьютерных системах необходимо принимать меры по предотвращению, обнаружению и минимизации ущерба от пожара, наводнения, загрязнения окружающей среды, высоких температур и скачков напряжения.

Пожарная сигнализация и системы пожаротушения должны регулярно проверяться. ПЭВМ можно защитить с помощью кожухов, чтобы они не были повреждены системой пожаротушения. Горючие материалы не должны храниться в этих помещениях с компьютерами.

Температура в помещении может контролироваться кондиционерами и вентиляторами, а также хорошей вентиляцией в помещении. Проблемы с чрезмерно высокой температурой могут возникнуть в стойках периферийного оборудования или из-за закрытия вентиляционного отверстия в терминалах или ПЭВМ, поэтому необходима их регулярная проверка.

Компьютеры должны размещаться как можно дальше источников большого количества воды, например, трубопроводов.

6. Защита носителей информации (исходных документов, лент, картриджей, дисков, распечаток).

Для защиты носителей информации рекомендуется:

* вести, контролировать и проверять реестры носителей информации;
* обучать пользователей правильным методам очищения и уничтожения носителей информации;
* делать метки на носителях информации, отражающие уровень критичности содержащейся в них информации;
* уничтожать носители информации в соответствии с планом организации;
* доводить все руководящие документы до сотрудников;
* хранить диски в конвертах, коробках, металлических сейфах;
* не касаться поверхностей дисков, несущих информацию
* осторожно вставлять диски в компьютер и держать их подальше от источников магнитного поля и солнечного света;
* убирать диски и ленты, с которыми в настоящий момент не ведется работа;
* хранить диски разложенными по полкам в определенном порядке;
* не давать носители информации с критической информацией неавторизованным людям;
* выбрасывать или отдавать поврежденные диски с критической информацией только после их размагничивания или аналогичной процедуры;
* уничтожать критическую информацию на дисках с помощью их размагничивания или физического разрушения в соответствии с порядком в организации;
* уничтожать распечатки и красящие ленты от принтеров с критической информацией в соответствии с порядком организации;
* обеспечить безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру.

7. Выбор надежного оборудования.

Производительность и отказоустойчивость информационной системы во многом зависит от работоспособности серверов. При необходимости обеспечения круглосуточной бесперебойной работы информационной системы используются специальные отказоустойчивые компьютеры, т. е. такие, выход из строя отдельного компонента которых не приводит к отказу машины.

На надежности информационных систем отрицательно сказываются и наличие устройств, собранных из комплектующих низкого качества, и использование нелицензионного ПО. Чрезмерная экономия средств на обучение персонала, закупку лицензионного ПО и качественного оборудования приводит к уменьшению времени безотказной работы и значительным затратам на последующее восстановление системы.

8. Источники бесперебойного питания.

Компьютерная система энергоемка, и потому первое условие ее функционирования - бесперебойная подача электроэнергии. Необходимой частью информационной системы должны стать источники бесперебойного питания для серверов, а по возможности, и для всех локальных рабочих станций. Рекомендуется также дублировать электропитание, используя для этого различные городские подстанции. Для кардинального решения проблемы можно установить резервные силовые линии от собственного генератора организации.

9. Разработка адекватных планов обеспечения непрерывной работы и восстановления.

Целью планов обеспечения непрерывной работы и восстановления являются гарантии того, что пользователи смогут продолжать выполнять свои самые главные обязанности в случае невозможности работы по информационной технологии. Обслуживающий персонал должен знать, как им действовать по этим планам.

Планы обеспечения непрерывной работы и восстановления (ОНРВ) должны быть написаны, проверены и регулярно доводиться до сотрудников. Процедуры плана должны быть адекватны уровню безопасности и критичности информации. План ОНРВ может применяться в условиях неразберихи и паники, поэтому нужно регулярно проводить тренировки сотрудников.

10. Резервное копирование.

Одним из ключевых моментов, обеспечивающих восстановление системы при аварии, является резервное копирование рабочих программ и данных. В локальных сетях, где установлены несколько серверов, чаще всего система резервного копирования устанавливается непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и рабочих станций в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании.

Для архивной информации, представляющей особую ценность, рекомендуется предусматривать охранное помещение. Дубликаты наиболее ценных данных, лучше хранить в другом здании или даже в другом городе. Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.

11. Дублирование, мультиплексирование и резервирование офисов.

Помимо резервного копирования, которое производится при возникновении внештатной ситуации либо по заранее составленному расписанию, для большей сохранности данных на жестких дисках применяют специальные технологии - зеркалирование дисков и создание RAID-массивов, которые представляют собой объединение нескольких жестких дисков. При записи информация поровну распределяется между ними, так что при выходе из строя одного из дисков находящиеся на нем данные могут быть восстановлены по содержимому остальных.

Технология кластеризации предполагает, что несколько компьютеров функционируют как единое целое. Кластеризуют, как правило, серверы. Один из серверов кластера может функционировать в режиме горячего резерва в полной готовности начать выполнять функции основной машины в случае ее выхода из строя. Продолжением технологии кластеризации является распределенная кластеризация, при которой через глобальную сеть объединяются несколько кластерных серверов, разнесенных на большое расстояние.

Распределенные кластеры близки к понятию резервных офисов, ориентированных на обеспечение жизнедеятельности предприятия при уничтожении его центрального помещения. Резервные офисы делят на холодные, в которых проведена коммуникационная разводка, но отсутствует какое-либо оборудование и горячие, которыми могут быть дублирующий вычислительный центр, получающий всю информацию из центрального офиса, филиал, офис на колесах и т.д.

12. Резервирование каналов связи.

При отсутствии связи с внешним миром и своими подразделениями, офис оказывается парализованным, потому большое значение имеет резервирование внешних и внутренних каналов связи. При резервировании рекомендуется сочетать разные виды связи - кабельные линии и радиоканалы, воздушную и подземную прокладку коммуникаций и т.д.

По мере того, как компании все больше и больше обращаются к Internet, их бизнес оказывается в серьезной зависимости от функционирования Internet-провайдера. У поставщиков доступа к Сети иногда случаются достаточно серьезные аварии, поэтому важно хранить все важные приложения во внутренней сети компании и иметь договора с несколькими местными провайдерами. Следует также заранее продумать способ оповещения стратегических клиентов об изменении электронного адреса и требовать от провайдера проведения мероприятий, обеспечивающих оперативное восстановление его услуг после аварий.

13. Защита данных от перехвата.

Для любой из трех основных технологий передачи информации существует технология перехвата: для кабельных линий - подключение к кабелю, для спутниковой связи – использование антенны приема сигнала со спутника, для радиоволн - радиоперехват. Российские службы безопасности разделяют коммуникации на три класса. Первый охватывает локальные сети, расположенные в зоне безопасности, т. е. территории с ограниченным доступом и за экранированным электронным оборудованием и коммуникационными линиями, и не имеющие выходов в каналы связи за ее пределами. Ко второму классу относятся каналы связи вне зоны безопасности, защищенные организационно-техническими мерами, а к третьему - незащищенные каналы связи общего пользования. Применение коммуникаций уже второго класса значительно снижает вероятность перехвата данных.

Для защиты информации во внешнем канале связи используются следующие устройства: скремблеры для защиты речевой информации, шифраторы для широковещательной связи и криптографические средства, обеспечивающие шифрование цифровых данных.

# **Вывод**

Приведенные меры по защите информации являются примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения информационной безопасности для проведения специальных тестов и экспериментов.

Организация юридической фирмы напоминает собой структуру [юридического департамента](https://moeobrazovanie.ru/yuridicheskii_departament.html): то же разделение на направления, выделение руководителей направлений, только возглавлять юридическую фирму может несколько партнеров, которые сообща принимают решения, а юридическое подразделение возглавляет один руководитель.

Согласно промежуточным результатам исследования, все юридические фирмы имеют незакрытые критические уязвимости на ПК и серверах, половина – на сетевом оборудовании. 65% юрфирм не имеют даже минимальной системы защиты, 60% – уязвимы для действий инсайдеров, а 70% – не защищены от внешних угроз. Причинами подобных цифр, по мнению авторов исследования, являются отсутствие шифрования данных; отсутствие процессов обеспечения безопасности и реагирования на инциденты; неразграничение прав доступа; из всех средств защиты в основном присутствуют только антивирус и слабые пароли.

На практике это, в частности, означает высокую вероятность взлома; моментальную доступность конфиденциальной информации при утере или выемке устройства, на которой она хранится; неотслеживаемость действий инсайдеров; невозможность узнать и отреагировать на кибератаку.

В частности, нарушение конфиденциальности данных юридической фирмы и их клиентов зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – юридическая фирма понесет ответственность – начиная от финансовой и закачивая уголовной.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки, можем выделить следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий:

* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь офиса с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, без данных милиции;
* защита главных серверов компании и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам.
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие в офисе наглядного отображения плана по работе во время чрезвычайных ситуаций.

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.