**Содержание:**

# Введение

Для рассмотрения видов и угроз информационной безопасности нужно определить, что мы понимаем под термином «информация». Информация - это любые сведения, принимаемые и передаваемые, сохраняемые различными источниками. Информация - это вся совокупность сведений об окружающем нас мире, о всевозможных протекающих в нем процессах, которые могут быть восприняты живыми организмами, электронными машинами и другими информационными системами [[1]].

Защита информации – важная часть деятельности любого предприятия. Почти вся информация сейчас хранится в электронном виде. Любая угроза несанкционированного доступа к ней может привести к финансовым потерям и потере репутации предприятия.

Целью защиты информации является предотвращение и защиту информации от уничтожения, модификации, искажения, копирования, блокирования информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы. Так же зашита информации создается для соблюдения конфиденциальности клиентов, сохранения в тайне их личных данных и данных по работе с предприятием. Для государственных предприятий вводится сохранение государственной тайны и ограничение доступа к информации для определенного круга лиц.Данная тема курсовой работы была выбрана мною как наиболее актуальная в настоящее время. Так же защита информационных ресурсов от угроз является частью моей работы. Своевременное выявление угроз может являться ключевым фактором для успешной борьбы с угрозой и предотвращения угрозы для информации.

Целью данной работы является определение видов угроз информационной безопасности и их состава.

# Глава 1

## 1.1 Понятие информационной безопасности

Для более полного раскрытия темы курсовой работы нужно дать определение информационной безопасности. Итак, информационная безопасность – это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю.

Основными принципами информационной безопасности являются:

1. Целостность данных - такое свойство, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Создавать, уничтожать или изменять данные может только пользователь, имеющий право доступа.
2. Конфиденциальность — свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц. Таким образом, конфиденциальность дает гарантию того, что в процессе передачи данных, они могут быть известны только авторизованным пользователям
3. Доступность информации - это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации.
4. Достоверность – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

Задача обеспечения информационной безопасности подразумевает реализацию многоплановых и комплексных мер по предотвращению и отслеживанию несанкционированного доступа неавторизованных лиц, а также действий, предупреждающих неправомерное использование, повреждение, искажение, копирование, блокирование информации [[2]].

## 1.2 Классификация угроз информационной безопасности

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные

подгруппы:

1. Нежелательный контент
2. Несанкционированный доступ
3. Утечки информации
4. Потеря данных
5. Мошенничество
6. Кибервойны
7. Кибертерроризм

Далее постараемся более детально раскрыть каждый вид угрозы и привести примеры. Начнем с нежелательного контента.

Нежелательный контент включает в себя не только вредоносные программы, потенциально опасные программы и спам, которые непосредственно созданы для того, чтобы уничтожить или украсть информацию, но и сайты, которые запрещены законодательством, или нежелательные сайты, что содержат информацию, не соответствующую возрасту потребителя. К нежелательному контенту можно отнести вредоносные программы, спам, запрещенные законодательством сайты и нежелательные сайты. Открыв такой сайт или письмо со спам рассылкой, пользователь может не догадываться что уже стал жертвой мошенников, запустив на своем компьютере вредоносное программное обеспечение [[3]].

Несанкционированный доступ (традиционно используемое сокращение – НСД) следует понимать, как получение доступа к данным, хранящимся на различных носителях и накопителях (ПК, гаджеты, съёмные диски) посредством самовольного изменения или же фальсификации соответствующих прав. Подобное имеет место тогда, когда какие-то данные предназначены только определённому кругу лиц, но существующее ограничение нарушается. Осуществляется за счёт ошибок, допущенных контролирующей структурой, системой компьютерной безопасности, или же подменой удостоверяющих документов, противоправным завладением информацией о другом лице, которому предоставлен такой доступ. Несанкционированный доступ киберпреступники могут получить, проведя атаку на сайты или веб-приложения, это может быть возможно, когда сайт заражен вредоносными программами, он взломан или имеет незакрытые уязвимости, кроме этого сайт может быть подвергнут DDoS-атаке. Злоумышленники могут получить доступ к данным перехватив данные по сети с помощью шпионских программ или снифферы (Сниффер -это компьютерная программа или часть компьютерной техники, которая может перехватывать и анализировать трафик, проходящий

через цифровую сеть или ее часть.). Уязвимое программное обеспечения и его последующий взлом становятся наиболее частой причиной несанкционированного доступа к данным. Также доступ может быть получен с использованием брутфорса (Брутфорс -долгий, но весьма действенный способ подбора паролей. Подбираются все возможные комбинации для заданной длины пароли и набора символов (латинские символы малого и большого регистра, спецзнаки, цифры и т. д.) для подбора паролей к административным учетным записям или же более деликатно с помощью социальной инженерии. Допущенные ошибки при настройке программ и несанкционированное с отделом информационной безопасности программное обеспечение - очень распространенные проблемы, которые открывают серьезные бреши в безопасности [[4]].

Утечки информации - неправомерное получение конфиденциальной информации (информация важная для различных компаний или государства, персональные данные граждан), которое может быть умышленной или случайной. Любые сведения, находящиеся в компьютере, имеют свою стоимость. Похищение личных данных владельца компьютера через программы с вирусами способно нанести ему вред. Имея доступ к логинам и паролям, а также к карточкам банка и счетам, хакеры крадут деньги граждан, промышленные секреты и тайны предприятий. Информация утекает в результате бесконтрольного распространения секретов за стены кабинета, помещения, предприятия. Утрата ценных сведений может случиться при неправильном использовании норм и правил информационной защиты и их несоблюдение. Не соблюдение правил защиты и хранения данных влекут за собой их утечку и распространение в общедоступных местах, таких как сеть интернет [[5]]. Каналы утечки данных могут быть внутренние и внешние. К внутренним каналам относятся так называемые инсайдеры – сотрудники, своими действиями создающие угрозы информационной безопасности. Их действия зачастую финансируются злоумышленниками, охотящимися за информацией о предприятии, но не имеющими возможности получить эту информацию извне. К внешним каналам относятся взломы информационных систем, кража носителей данных, установка вредоносных программ для скрытого доступа. Третьим каналом являются случайные утечки. К таким утечкам данных можно отнести потерю ноутбука, флеш-карты с данными, или ошибочные действия сотрудников фирмы.

Потеря данных (Data Loss) – повреждение или утрата информации в результате различных факторов. При этом информация может быть удалена или повреждена в результате ряда случайных или намеренных действий. Потерять данные можно во время работы с ними, а также при хранении информации на компьютере, сервере

или на массивах RAID. Данные могут быть потеряны из-за нарушения целостности информации по причине сбоя программного обеспечения или же из-за неисправности оборудования. Нарушение целостности информации означает повреждение данных, в результате которого невозможно прочитать/скопировать информацию без выполнения процедуры восстановления. При нарушении целостности возникает риск потери всех и части данных, а также угроза работы всей компьютерной системы. Нередко целостность данных нарушается в результате саботажа. Ряд злонамеренных действий приводит преступника к поставленной цели. Это может быть вредительская деятельность персонала компании, атаки киберпреступников, другие ситуации. К нарушению целостности может привести сбой программного обеспечения. Сбой может возникнуть из-за воздействия вредоносных программ, некорректной настройки приложений, неудачного обновления программ, форматирования не тех файлов при установке операционной системы или ошибок при ее обновлении. Неисправность оборудования может привести к полной потере данных пользователя или любой компании. Она может возникнуть по непреднамеренным причинам или же в результате определенных действий злоумышленника. Выделяют несколько причин неисправности оборудования, например, стихийные бедствия. Компьютерные устройства могут пострадать от наводнения, урагана, молнии, пожара и т.п. Оборудование придет в нерабочее состояние и приведет к потере данных в результате катастрофы, будь она техногенной или экологической. Скачок напряжения, сильное повышение температуры окружающей среды ведет к воспламенению компонентов персональных компьютеров или серверов, повреждению жесткого диска. Оборудование может стать неисправным по вине вандалов. Это могут как обычные правонарушители, так и специально люди, нанятые недоброжелателями или конкурентами. Сотрудники или люди, обслуживающие компьютерную технику, могут нанести вред деятельности своей компании из корыстных целей (подкуп конкурентами), из-за мести. Кроме того, неисправность оборудования может возникнуть из-за проблем работы составных узлов или по причине сбоя программного обеспечения. Нарушают целостность данных, прежде всего, сами пользователи и лица, обслуживающие компьютерные устройства. Информация может изменяться/удаляться случайно или специально. Нередко пользователи пренебрегают антивирусами и другими средствами безопасности от вредоносных программ, некорректно устанавливают программы, вмешиваются в работу составных узлов. Источником угрозы являются сотрудники компаний, умышленно удаляющие или изменяющие информацию, а также киберпреступники. Для оборудования угрозой являются природные явления,

вандалы, сотрудники, киберпреступники. К неисправностям компьютеров могут привести ливни, пожары, торнадо и другие природные катаклизмы. Деятельность злоумышленников и саботаж персонала тоже ведут к порче оборудования и потере данных [[6]].

Мошенничество или фрод (англ. fraud - "мошенничество") - вид мошенничества незаконного использования информационных технологий в различных областях бизнеса, от телекоммуникаций до банковского сектора. Для фрода кибермошенники могут использовать множество методов: фишинг, скамминг, социальную инженерию, кардинг, нигерийские письма, и т.п. Фрод известен очень давно: мошенники научились использовать телефон для своих дел еще в 60-70-х годах XX века. С появлением интернета кибермошенники перебрались и в него: начали появляться фишинговые сайты, на электронную почту пользователей стали приходить письма мошеннического содержания. При фишинге хакеры пытаются всеми способами вытянуть из пользователя его личные данные, его логины и пароли. Мошенники могут создавать поддельные сайты, внешне не отличимые от настоящего, с похожим доменным именем, которые заставят пользователя войти под своим логином и паролем, после чего они окажутся у злоумышленников. Также фишинг может быть в виде e-mail писем, в которых мошенники будут от имени компании (банка, социальной сети, и т.п) достать из пользователя его данные для входа в аккаунт или его личные данные (номера кредитных карт, копии документов). К данному виду угрозы так же относится и кража личности - преступление, при котором один человек выдает себя за другого. Мошенники могут выдать себя за другого человека для того, чтобы получить кредит удаленно (с помощью специальных Интернет-ресурсов), например. По информации исследователей, на черном рынке полный комплект данных для кражи личности (включая документы) стоит $16-30 [[7]].

Кибервойны (Cyberwarfare) – это военные действия, осуществляемые электронным способом, а не физическим, где в качестве оружия выступает информация, а инструментами являются компьютеры и Интернет. Задача такого рода войны – достичь определенных целей в экономической, политической, военной и других областях, посредством влияния на общество и власть тщательно подготовленной информацией. Именно поэтому войну нового времени можно назвать психологической. Кибервойна является одной из разновидностей информационной войны и представляет собой противостояние в кибернетическом пространстве. Компьютерные технологии и Интернет получили широкое распространение по всему миру и используются не только в повседневной жизни граждан, но и на

предприятиях, в государственных учреждениях, которые в свою очередь являются важной структурной единицей страны. Манипуляция «противником» данными, полученными из подобных мест, представляет угрозу для национальной безопасности стран. Высоким приоритетом информационной войны является не только нанесение ущерба противнику, но и защита собственных данных, поэтому кибербезопасность – неотъемлемая часть подобного рода противостояний. Она представляет собой совокупность принципов, средств и стратегий для обеспечения неуязвимости, и защиты киберсреды, а именно доступность, целостность и конфиденциальность данных. Способы и этапы ведения кибервойны (Cyberwarfare) Кибернетическая война состоит из двух этапов: шпионаж и атаки. Первый этап подразумевает сбор данных, посредством взлома компьютерных систем других государств. Атаки можно разделить в зависимости от цели и задач военных действий: Вандализм – размещение пропагандистских или оскорбительных картинок на веб-страницах вместо исходной информации. Пропаганда и информационная война – использование пропаганды в контенте веб-страниц, в рассылках обращений. Утечки конфиденциальных данных – все, что представляет интерес, копируется со взломанных частных страниц и серверов, также секретные данные могут быть подменены. DDoS-атаки – атака с нескольких машин с целью нарушить функционирование сайта, системы компьютерных устройств. Нарушение работы компьютерной техники – атаке подвергаются компьютеры, отвечающие за функционирование оборудования военного или гражданского назначения. Атака приводит к выходу из строя техники или к ее отключению. Атака инфраструктурных и критически важных объектов и воздействие на машины, регулирующие инженерные, телекоммуникационные, транспортные и другие системы, обеспечивающие жизнедеятельность населения. Цели кибервойны Все действия кибервойны (cyberwarfare) направлены на нарушение функционирования вычислительных систем, отвечающих за работу деловых и финансовых центров, государственных организаций, создание беспорядка в жизни страны, поэтому в первую очередь страдают важные жизнеобеспечивающие и функциональные системы населенных пунктов. К ним относятся система водоснабжения, канализация, электростанции, энергетические узлы, другие коммуникационные сети [[8]].

Кибертерроризм – комплекс незаконных действий, создающих угрозу государственной безопасности, личности и обществу. Может привести к порче материальных объектов, искажению информации или другим проблемам. Основной целью кибертерроризма является получение преимущества в решении социальных, экономических и политических задачах. В мире стремительно растет количество

умных IoT-устройств. Однако, все они дают почву для целенаправленных атак с целью террора или шантажа. Тем более, что сейчас даже многие заводы и фабрики используют такие устройства в автоматизированных системах управления технологическим процессом (АСУ ТП), которые киберпреступники могут взломать с целью террора населения: например, выводом цеха из строя или даже взрывом АЭС. Конечно, на данный момент таких атак замечено не было, однако кто дает гарантию, что их не будет в будущем? В своих акциях преступники активно используют все возможности современных технологий, в том числе современные гаджеты и программные продукты, радиоэлектронные устройства, достижения в области микробиологии и генной инженерии. Официально кибертерроризмом признаются акты, совершенные одним человеком или независимыми группами, состоящими из нескольких членов. Если в совершении подпадающих под это определение действий принимают участие представители правительственных или иных государственных структур, это считается проявлениями кибервойны. Влияние подобных акций на экономические и геополитические процессы зачастую преувеличивается журналистами в СМИ и сценаристами голливудских блокбастеров, что может привести к неправильной оценке сложившейся ситуации. Действия кибертеррористов направлены на:

- Взлом компьютерных систем и получение доступа к личной и банковской информации, военным и государственным конфиденциальным данным
- Вывод из строя оборудования и программного обеспечения, создание помех, нарушение сетей электропитания
- Кражу данных с помощью взлома компьютерных систем, вирусных атак, программных закладок
- Утечку секретной информации в открытый доступ
- Распространение дезинформации с помощью захваченных каналов СМИ
- Нарушение работы каналов связи
- Прочее

Главной целью кибертерроризма является получение преимуществ в решении политических, социальных и экономических вопросах. Чтобы достичь желаемую цель, кибертеррористы применяют специальное ПО, используемое для взлома компьютерных систем компаний и организаций, проводят атаки на удаленные сервера компаний и организаций. Кибертеррористы не закладывают бомб, не берут заложников. Они угрожают компьютерными средствами: выводом крупной компьютерной сети какой-нибудь компании из строя, уничтожением данных клиентов банков, даже выводом из строя “умных” заводов и электростанций и т.п.

с целью получения выкупа. Для достижения поставленных целей могут использоваться различные методы: незаконное получение доступа к государственным и военным архивам с секретной информацией, реквизитам банковских счетов и платежных систем, личным данным; осуществление контроля над объектами инфраструктуры для оказания влияния на их работоспособность вплоть до вывода из строя отдельных компонентов и полного останова систем жизнеобеспечения; похищение или уничтожение информации, программных средств или технических ресурсов путем внедрения вредоносного ПО различных типов; ложные угрозы совершения атак, которые могут повлечь дестабилизацию экономической или социально-политической обстановки. Способы проведения этих и подобных операций постоянно изменяются в связи с развитием систем информационной безопасности, которые применяются в различных компьютерных сетях. Выявлена зависимость между уровнем развития информационной инфраструктуры и количеством хакерских атак. Чем выше уровень глобализации и использования систем автоматизации различных процессов в данном регионе, тем больше вероятность проведения кибератак террористической направленности [[9]].

Проведя классификацию угроз можно сделать вывод, что угрозы информационной безопасности могут подразделяться на различные категории, исходя из различных методов классификации. Для дальнейшего изучения угроз мы перейдем к их анализу.

## 1.3 Анализ угроз

Для эффективной защиты от различных угроз информационной безопасности нужно уметь их анализировать. В предыдущем параграфе мы провели классификацию угроз теперь нужно провести анализ каждой из них, чтобы выявить объекты воздействия и источники угрозы. Зная методы воздействия и объекты воздействия гораздо проще определить, что являлось источником угрозы и каким способом осуществлялась атака на предприятие.

Нежелательный контент. К нему относятся:

- Вредоносные программы
- Спам
- Потенциально опасные программы
- Запрещенные законодательством сайты
- Нежелательные сайты

Объектами воздействия данного вида угрозы являются персональные и корпоративные компьютеры, смартфоны, устройства, поддерживающие выход в интернет. От данного вида угрозы нет 100% защиты, но от большинства компонентов данной угрозы может защитить выполнение элементарных норм безопасности работы в сети Интернет. Обучения сотрудников основам информационной безопасности может помочь избежать данного вида угрозы.

Основным источником вредоносных программ является киберкриминальные элементы, использующие нежелательный контент и спам рассылки для распространения вредоносных программ и заражения как можно большего количества компьютеров.

От данного вида угрозы может помочь использование комплексных антивирусных средств класса Internet Security или же узкоспециализированное программное обеспечение для каждого вида угроз. Данное ПО постоянно обновляет базы данных, чтобы гарантировать максимальную защиту от новых видов угроз. Но стоит помнить, что само наличие антивирусной системы не гарантирует полную безопасность, так как пользователь своими действиями может отключить данное программное обеспечение, обеспечив доступ к ЭВМ. От спам рассылок может помочь установка антиспам-фильтров и добавление нежелательных адресов в черный список. Эти способы доступны и реализованы во всех популярных почтовых ресурсах (Яндекс Почта, Почта Mail.ru). Для защиты от рекламы в браузере используются специальные расширения, блокирующие рекламу и предотвращающие установку вредоносных программ через клик на рекламу. Использование антивирусных программ так же ограничит переходы на нежелательные и вредоносные сайты, а также сайты, заблокированные законодательно.

Несанкционированный доступ. Согласно ГОСТ Р 50922-96 "Защита информации. Основные термины и определения" несанкционированный доступ к информации – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации [[10]]. Объектами воздействия данного вида угрозы являются персональные и корпоративные персональные компьютеры, локальные информационные системы, информационные сервера, закрытые локальные сети и информационные хранилища. Любое устройство, подключенное к сети Интернет или локальной сети подвергается угрозе несанкционированного доступа.

Данная угроза может быть реализована несколькими способами:

- по принципу НСД:
  - физический. Может быть реализован при непосредственном или визуальном контакте с защищаемым объектом;
  - логический. Предполагает преодоление системы защиты с помощью программных средств путем логического проникновения в структуру АС;
- по пути НСД:
  - использование прямого стандартного пути доступа. Используются слабости установленной политики безопасности и процесса административного управления сетью. Результатом может быть маскировка под санкционированного пользователя;
  - использование скрытого нестандартного пути доступа. Используются недокументированные особенности (слабости) системы защиты (недостатки алгоритмов и компонентов системы защиты, ошибки реализации проекта системы защиты);
  - Особую по степени опасности группу представляют угрозы ИБ, осуществляемые путем воздействий нарушителя, которые позволяют не только осуществлять несанкционированное воздействие (НСВ) на информационные ресурсы системы и влиять на них путем использования средств специального программного и программно-технического воздействия, но и обеспечивать НСД к информации.
- по степени автоматизации:
  - выполняемые при постоянном участии человека. Может использоваться общедоступное (стандартное) ПО. Атака проводится в форме диалога нарушителя с защищаемой системой;
  - выполняемые специальными программами без непосредственного участия человека. Применяется специальное ПО, разработанное чаще всего по вирусной технологии. Как правило, такой способ НСД для реализации атаки предпочтительнее;
- по характеру воздействия субъекта НСД на объект защиты:
  - пассивное. Не оказывает непосредственного воздействия на АС, но способно нарушить конфиденциальность информации. Примером является контроль каналов связи;
  - активное. К этой категории относится любое несанкционированное воздействие, конечной целью которого является осуществление каких-либо изменений в атакуемой АС;
- по условию начала воздействия:

    - атака по запросу от атакуемого объекта. Субъект атаки изначально условно пассивен и ожидает от атакуемой АС запроса определенного типа, слабости которого используются для осуществления атаки;
    - атака по наступлению ожидаемого события на атакуемом объекте. За ОС объекта атаки ведется наблюдение. Атака начинается, когда АС находится в уязвимом состоянии;
    - безусловная атака. Субъект атаки производит активное воздействие на объект атаки вне зависимости от состояния последнего;
- по цели воздействия.
    - Безопасность рассматривают как совокупность конфиденциальности, целостности, доступности ресурсов и работоспособности (устойчивости) АС, нарушение которых нашло отражение в модели конфликта;
- по наличию обратной связи с атакуемым объектом:
    - с обратной связью. Подразумевается двунаправленное взаимодействие между субъектом и объектом атаки с целью получения от объекта атаки каких-либо данных, влияющих на дальнейший ход НСД;
    - без обратной связи. Однонаправленная атака. Субъект атаки не нуждается в диалоге с атакуемой АС. Примером является организация направленного "шторма" запросов. Цель – нарушение работоспособности (устойчивости) АС;
- по типу используемых слабостей защиты:
    - недостатки установленной политики безопасности. Разработанная для АС политика безопасности неадекватна критериям безопасности, что и используется для выполнения НСД:
    - ошибки административного управления;
    - недокументированные особенности системы безопасности, в том числе связанные с ПО, – ошибки, неосуществленные обновления ОС, уязвимые сервисы, незащищенные конфигурации по умолчанию;
    - недостатки алгоритмов защиты. Алгоритмы защиты, использованные разработчиком для построения системы защиты информации, не отражают реальных аспектов обработки информации и содержат концептуальные ошибки;
    - ошибки реализации проекта системы защиты. Реализация проекта системы защиты информации не соответствует заложенным разработчиками системы принципам [[11]].

Методы защиты от несанкционированного доступа очень разнообразны. Их можно разделить на физические средства ограничения доступа - USB-ключи, карты

доступа, SMART карты. Без такого ключа нельзя войти в операционную систему компьютера и начать с ним работать. Данный метод может быть обойден если носитель с ключевой информацией будет потерян или изъят злоумышленниками. Другим методом идентификации пользователя являются личные данные для входа в корпоративную сеть, которые могут меняться через определенный промежуток времени, чтобы не быть скомпрометированными. Данный метод может быть применен для отслеживания действий каждого пользователя и их протоколирования. Так же, как и у предыдущего метода, данные для доступа могут быть скомпрометированы. Поэтому максимальный уровень безопасности может быть достигнут только применением многофакторной идентификации как физическим носителем, так и введением личных данных для доступа. Возможно следующим шагом в методике защиты личной информации станет биоидентификация пользователей – по сетчатке глаза, отпечатку пальца или рисункам вен на ладони. К сожалению, сейчас данный метод не распространен повсеместно из-за своей сложности и высокой цены на оборудование, осуществляющее идентификацию.

Утечки информации. Для проведения анализа данной угрозы нужно сначала определить какие каналы утечки информации могут быть использованы злоумышленниками. Проведем разделение каналов утечки:

1. Бумажные документы. С помощью бумажных носителей конфиденциальная информация становится доступной другим чаще всего. Независимо от того, сливает ее кто-то умышленно или утечка происходит случайно. Иногда документы с конфиденциальной информацией могут оказаться в мусоре за пределами предприятия и использоваться злоумышленниками для получения конфиденциальной информации на вполне законных основаниях. В ряде случаев бумажный носитель используется для продажи данных, так как он не несет в себе следов, от кого получен данный документ.
2. Компьютеры. Компьютеры — второй по распространенности канал, через который инсайдеры сливают на сторону конфиденциальную информацию. В большинстве случаев компьютер является каналом доступа к данным предприятия. Через него злоумышленник получает доступ к корпоративным сведениям, хранящимся на сервере компании, может скачать их на съемные носители или отправить по электронной почте.
3. Интернет. Случайная утечка может произойти, когда финансовые сведения содержатся в программах компании, работающих через интернет, а вход в них имеет примитивные пароли. Таковыми принято считать цифровые или

буквенные пароли по ходу клавиатуры: 123456, 123123, 12345678, qwerty, а также abc123, dragon, 111111, iloveyou, sunshine, passw0rd, superman, football и др.

4. Электронная почта. Сотрудники считают, что пересылать секретные данные безопаснее с личной, а не с корпоративной почты. Это заблуждение: установить, чей адрес, легко по учетным записям. Также электронная почта помогает проникнуть в тайны компании с помощью зараженных вирусами писем. Шпионы изучают интересы сотрудника (в социальных сетях, интернет переписке, блогах), затем отправляют ему такое письмо, которое он наверняка откроет, например, человеку, интересующемуся скалолазанием, могут прислать письмо с предложением скидки на снаряжение.
5. Смартфоны, ноутбуки. Смартфоны и ноутбуки тоже не самый распространенный канал утечки секретной информации, но часто используется менеджерами высшего звена. Ситуация: идет конфиденциальное совещание. У присутствующих с собой смартфоны или, что чаще всего, ноутбуки с материалами совещания. Сотрудник компании, собирающий информацию может просто включить диктофон и собирать информацию на протяжении всего совещания. Затем просто скопировать запись и передать её конкурентной организации
6. Съемные носители и резервные копии. Флешки, переносные жесткие диски в силу своего удобства тоже используются для передачи информации. Сотрудник предприятия после факта передачи информации может просто сослаться на обычную потерю данного носителя. Иногда информация уходит по оплошности. К примеру, сотрудник взял на флешке отчеты с финансовыми показателями домой доработать, а дома незащищенное Интернет-соединение.

Методы защиты от данной угрозы. От данной угрозы существует несколько видов защиты. Для более эффективной защиты можно комбинировать данные методы:

- Трудовой договор. В нем можно прямо прописать, что работодатель имеет полный доступ к информации на компьютерах работников, а в случае разглашения коммерческой тайны будет требовать возмещения убытков. Эти меры являются мощным сдерживающим психологическим фактором.
- Высокая зарплата. Боязнь ее потерять скорее всего отобьет у сотрудника желание предавать свою компанию.
- Слежка и прослушка. Существуют программы, которые контролируют все, что происходит на компьютере. Если сотрудники знают, что она у них установлена, у них вряд ли появится желание передавать секретную

информацию с рабочего компьютера. Еще устанавливают свои «жучки» в кабинетах или переговорных комнатах, а «жучки» шпионов блокируют шумогенераторами, которые создают помехи и глушат сигнал.
- Тренинг. Устраивают провокацию: сотрудникам рассылают письма с вирусами, просят по телефону выдать конфиденциальные сведения и т. п. В результате теста выясняется, как персонал реагирует на такие действия, и разрабатываются меры защиты.
- DLP-система (Data Leak Prevention). Она отслеживает пересылку и распечатку файлов, внезапные всплески интернет-общения, посещение нехарактерных для работы сайтов и т. д. Также проводит лингвистический анализ переписки и документов и, по ключевым словам, устанавливает опасность утечки [[12]].

Потеря данных. Под потерей данных подразумевается нарушение целостности данных на различных носителях. Данными носителями могут являться жесткие диски, флэш накопители, лазерные диски. Целостность данных может быть нарушена с целью саботажа предприятия. Данная угроза может осуществляться двумя путями – путем проникновения на компьютер и его заражение вирусом с целью повреждения данных или получение физического доступа к носителю данных и его уничтожение. Нарушение целостности данных с целью их потери может проводиться компьютерными вирусами. Вирус, попадая в незащищенный компьютер может удалить информацию, являющуюся важной для данного предприятия. Физическое же уничтожение носителей информации может производится при проникновении непосредственно на предприятие одним или группой лиц, с целью разрушения хранилищ данных.

Защита от потери данных. Защитой от потери данных является антивирусное программное обеспечение, настроенное на максимальную защиту от вирусных атак и вирусов-шифровальщиков. Так же хорошей защитой является установка сетевого экрана, проверяющего весь трафик.
Защитой же от физического уничтожения носителей являются различного рода системы защиты от несанкционированного доступа на предприятие, пропускной режим, ограничение персонала в зонах прямого доступа к информационным хранилищам, разделение основного хранилища данных и хранилища резервных копий. При комбинировании всех средств защиты можно достигнуть высокой степени защищенности от потери данных.

Мошенничество. Данный вид угрозы очень распространен в сети Интернет и может быть реализован различными способами. От мошенничества в сфере высоких технологий страдает широкий круг людей: это владельцы интернет-магазинов,

банки, телеком операторы, теряющие огромное количество денег из-за мошенников, которые покупают у них товары с помощью чужих карт, после чего владелец карты обязательно запросит возврат средств. Например, потери телеком операторов составляют от 3 до 7% от общего дохода за продажи услуг (ip-news.ru). Таким образом, магазин останется и без товара, и без денег. Кроме того, банки часто вводят санкции против магазина в виде штрафа в размере от $5000 до $200000. Однако, обычные пользователи страдают не меньше - с их счетов мошенники воруют деньги, заполучают их учетные данные, берут под их именем кредиты. Источник мошенничества В интернете существует огромное количество форумов, посвященных мошенничеству через интернет. На них мошенники объединяются в группы, делятся опытом и учат мошенничеству новичков. Из-за такой доступности информации число кибермошенников растет. На данный момент огромное количество пользователей разного возраста и народности промышляют мошенничеством: покупают на черном рынке данные о реквизитах платежной карты, занимаются фишингом, "обворовывают" интернет-магазины. Для этого не нужно много знаний и опыта, достаточно найти схему в интернете и действовать. Особую опасность представляют организованные группировки, которые занимаются мошенничеством на профессиональной основе. Они нацеливаются на опустошения счетов сотовых операторов, использования бонусов в интернет-магазинах для получения товаров и т.д.

Анализ риска мошенничества. Мошенничество - огромный риск и огромные потери для интернет-предпринимателей и обычных пользователей. К счастью, для интернет-магазинов, банков, телеком операторов разработано много различных защитных систем, которые следят за тем, чтобы на сайте не было мошенничества. Одним из видов борьбы с мошенничеством являются ручные методы - в этом случае трудозатраты на ручные работы составляют не менее 80% от общего объема работ. Еще один вид - ИТ-зависимые методы, при таком подходе борьба основывается на специальных выборках, предоставляемых ИТ подразделениями компании, благодаря чему значительно сокращаются трудозатраты и возрастают число контролируемых потоков данных. Третий вид противодействия мошенничеству - автоматизированные методы - использование программно-аппаратных средств [[13]].

Кибервойны. Данный вид угроз является наиболее массированным и опасным для безопасности как одного предприятия, так и для целых государств. Во всем мире сейчас формируются специальные подразделения, так называемые «кибервойска», защищающие объекты инфраструктуры государства от хакерских атак.

Кибервойна – это возможная война ближайшего будущего, бескровная, но в то же время смертельная. В своем роде переворот в искусстве ведения войн. Человечество дошло до такой степени развития, что и обычный ноутбук становится в руках профессионалов настоящим оружием. В современном мире от компьютеров зависит многое: давление в нефтепроводах, функционирование энергосистемы, движение воздушных судов, работа больниц и экстренных служб. Данные системы функционируют с использованием программного обеспечения и соответственно уязвимы для вредоносных программ – вирусов, которые могут привести к феноменальным последствиям с нанесением экономического и физического ущерба сопоставимого с воздействием обычных вооружений.

Пока такие войны не носят масштабного характера, но уже сейчас можно заметить локальные очаги их проявления. Одним из самых значимых эпизодов последнего времени многие эксперты признали операцию против строящейся АЭС в Бушере. По мнению специалистов, реактор мог быть поврежден в результате атаки компьютерного вируса Stuxnet, который нанес серьезный ущерб системе управления АЭС и компьютерной сети станции. Россия и ряд стран Персидского залива, опасаясь повторения Чернобыльской катастрофы, давят на Тегеран с целью добиться разрешения на проведение инспекции реактора атомной электростанции. В частности, на этом настаивает представитель России при НАТО Дмитрий Рогозин, который выступает за проведение совместной инспекции Россия-НАТО с целью определения реального состояния атомного объекта.

Вирус, поразивший строящийся ядерный объект несколько месяцев назад попал на станцию извне. Компьютерная система управления на АЭС в Бушере не была подключена к интернету, но это не помогло. Вирус принес на станцию кто-то из сотрудников или иностранных рабочих и запустил в сеть, в результате ядерная программа Ирана оказалась парализована. Многие склоняются к версии о том, что вирус Stuxnet мог быть написан секретными кибернетическими подразделениями Израиля или США, которых очень беспокоит реализация ядерной программы в этой ближневосточной стране.

Вторым наиболее значимым актом кибервойны ближайшего времени стала публикация огромного количества секретных материалов на сайте Wikileaks. В данном случае жертвой хакеров стали сами Соединенные Штаты. Достоянием миллионов людей по всему миру стали сначала секретные документы, касающиеся войн, которые ведут США в Афганистане и Ираке, а затем и публикация переписки американских дипломатов. Публикация данных материалов не только поставила

под угрозу жизнь многих людей, сотрудничающих со спецслужбами и правительством США, но и нанесла существенный ущерб американской дипломатии и имиджу страны в целом.

В реальности кибератака может представлять существенную угрозу только при массированном коллективном воздействии на отдельные критические точки системы, которая была заранее выбрана в качестве жертвы. Подобные угрозы крайне редко могут исходить лишь от одной антиобщественной личности. Наибольшую опасность и масштаб настоящей кибервойны они примут лишь в том случае, если будут осуществляться отдельными корпорациями или правительствами стран, которые способны привлечь значительные технические и людские ресурсы для нанесения направленных кибердударов. Но даже при этом, значительным фактором в данной ситуации остается – человеческий, что и подтвердил случай в Иране. В конечном счете, как бы уникальна и прогрессивна не была написанная вредоносная программа открыть или закрыть ей доступ в систему способен зачастую только человек. [[14]].

Кибертерроризм. Данный вид угрозы может быть реализован различными методами. Кибертеррористы не закладывают бомб, не берут заложников. Они угрожают компьютерными средствами: выводом крупной компьютерной сети какой-нибудь компании из строя, уничтожением данных клиентов банков, даже выводом из строя “умных” заводов и электростанций и т.п. с целью получения выкупа. Для достижения поставленных целей могут использоваться различные методы. Подвергнуться атакам сетевых террористов в равной степени могут государства, международные организации, крупные корпорации и относительно небольшие компании, политики и другие известные личности, а также выбранные случайным образом люди. Действия кибертеррористов могут быть направлены на объекты гражданской инфраструктуры и военного назначения. Некоторые эксперты склоняются к мнению, что более подвержены террористическим кибератакам могут быть энергетическая и телекоммуникационная отрасли, авиационные диспетчерские, финансовые учреждения, входящие в оборонный комплекс предприятия и другие объекты. Целями атак могут оказаться оборудование, софт, сетевые протоколы передачи данных, хранящаяся информация, специалисты в области информационных технологий и обслуживающий персонал. Злоумышленники могут захватить управление системами обороны для последующего вывода их из строя. Последний вариант развития событий встречается в большинстве случаев, при этом зачастую нарушается функционирование отдельных служб. Обычно такие акции проводят

частные лица или компании, которые разделяют взгляды террористов и являются их пособниками. Сами преступники в основном выполняют действия, направленные на разрушение коммуникаций, повреждение информационных и транспортных каналов. Если атакуемые объекты входят в состав критических систем жизнеобеспечения, стороннее вмешательство в их работу может привести к масштабным разрушениям и человеческим жертвам, как при обыкновенных террористических актах. Поскольку кибертерроризм носит трансграничный характер, его проявления могут привести к ухудшению отношений между государствами, нарушить экономические и дипломатические связи, затруднить работу межгосударственных организаций. Это может полностью разрушить выстроенную систему международных отношений, вызвать панику в обществе и затруднить возможности организованно противостоять физической преступности. Источниками кибертерроризма могут являться различные террористические группировки, активно использующие новейшие разработки в области информационных технологий для поддержания связи, решения организационных и финансовых вопросов, планирования операций и осуществления контроля над их выполнением. Они могут финансироваться или даже контролироваться отдельными государствами. Все крупнейшие террористические группировки имеют собственные сайты, их участников можно встретить на многочисленных форумах и в чатах. Социальные сети и другие подобные ресурсы в Интернете активно используются для пропаганды и вербовки новых участников запрещенными группировками. С помощью современных технологий легко шифруются любые сообщения, размещаются нужные схемы, фотографии, документы и прочие материалы. Введя соответствующий запрос в любой поисковой сети, можно обнаружить немало страниц с описанием изготовления оружия и взрывчатых веществ из подручных средств. Многие группировки пользуются тем, что в Интернете не обязательно находиться под своим настоящим именем, поэтому хакеры известны под псевдонимами. При этом нужно различать кибертеррористов от остальных хакеров, которые пишут и распространяют вирусы и другое вредоносное ПО для личного обогащения, являются компьютерными мошенниками или хулиганами. Терроризмом их действия становятся, когда они несут тяжелые последствия: разрушения или гибель людей. Многие радикальные группировки стараются, чтобы их акты произвели как можно больший резонанс, и о них узнало максимальное количество людей по всему миру. В некоторых организациях существуют целые подразделения программистов, которые создают и обновляют веб-сайты, ведут блоги и страницы в социальных сетях. Крупнейшие группы также имеют собственные телевизионные каналы и радиостанции. Руководство

группировок прибегает к кибертерроризму, потому что это обеспечивает нужный результат при минимальных вложениях, что особенно важно для выходцев из небогатых стран, а также усложняет поиск непосредственных исполнителей. В последнее время большинство хакерских атак на различные правительственные и военные организации производятся из Китая и других развивающихся государств из юго-восточной Азии. Правительство Поднебесной рассчитывает к 2020 году создать сильнейшие в мире информационные войска, численность которых на сегодня составляет 30 тысяч военных и 150 тысяч гражданских специалистов. Есть подозрение, что в качестве «троянского коня» могут выступать китайские микросхемы, содержащие специализированное ПО для копирования данных и отправки их на «базу». Похожие прецеденты имели место в сетях Госдепартамента и других ведомств США. Анализ риска В связи с развитием технологий, угроза кибертерроризма постепенно сравнивается по значимости с остальными его проявлениями. Из-за высокого уровня развития техники террорист посредством подключенного к Интернету компьютера может нанести больший вред, чем различные взрывные устройства. Новые гаджеты рассматриваются преступниками как средство для достижения целей, которые зачастую противоречат общепринятым морально-этическим нормам. Совершать акты компьютерного террора способны многие организации экстремистской направленности: ИГИЛ, Аль-Каида, ИРА, ЭТА, различные религиозные движения и прочие незаконные вооруженные формирования (запрещены в России). Их атаки поддерживают международную напряженность в ряде регионов и провоцируют возникновение глобальных кризисов в экономике и дипломатических отношениях между многими странами. Такие последствия не были характерными для традиционных терактов. Для борьбы с этим явлением требуется мобилизации усилий всего мирового сообщества. Данной проблемой вплотную занимаются ООН, Совет Европы, Интерпол и другие международные организации. Перед лицом совместной опасности объединяются даже непримиримые соперники, имеющие существенные противоречия по ряду ключевых вопросов [[15]].

Проанализировав все виды угроз и рассмотрев объекты для атак каждого вида угрозы, можно применить данные знания на практике на примере защиты от угроз информационной безопасности учреждения здравоохранения.

# Глава 2. Практическая часть

## 2.1 Описание защиты от угроз на примере предприятия

На предприятии, где я в настоящее время работаю существует несколько видов защиты от различного вида угроз. В комплексе они создают систему защиты от различного вида угроз. Начать описание стоит с внешнего уровня защиты. Каналы связи, по которым больница подключена к сети Интернет защищены криптошифрованием. Доступ к внутренним информационным ресурсам осуществляется по Ведомственной сети передачи данных (ВСПД). В ней так же реализованы алгоритмы шифрования данных, для предотвращения утечки информации посредством снятия данных с канала связи.

Внешней системой защиты так же является система охраны здания, осуществляемая охранной фирмой. По зданию расположены тревожные кнопки, так же в здании реализовано круглосуточное дежурство. Для предотвращения саботажа на предприятии установлена пожарная сигнализация.

К внутренним системам защиты можно отнести антивирусную систему Kaspersky Endpoint Security 10 для Windows (для рабочих станций и файловых серверов). Данная антивирусная система отвечает всем требованиям безопасности, что подтверждено Сертификатом соответствия № 3025 Федеральной службы по техническому и экспертному контролю (ФСТЭК). (Приложение 1). В данном антивирусном продукте можно настроить доступ к Интернет ресурсам, включить контроль за запуском программ, для предотвращения несанкционированного запуска вредоносного программного обеспечения.

Так же к внутренним системам защиты является работа с сотрудниками, повышение их компьютерной грамотности. Проведение различных лекций и показ на примерах, какие способы незаконного доступа существуют сейчас помогают бороться с угрозами информационной безопасности еще на стадии проникновения на компьютеры пользователей.

# Заключение

Угрозы информационной безопасности развиваются и совершенствуются с каждым годом. Злоумышленники изобретают новые способы нанесения вреда информации, новые методы получения несанкционированного доступа, действуют новыми

методами. Поэтому для эффективного противодействия нужно постоянно вести мониторинг угроз и разработку методов противодействия им. Анализ видов угроз является важнейшим направлением в данном процессе, так как если знать, какие виды угроз могут нанести наибольший ущерб предприятию, то можно наиболее эффективно организовать систему защиты от них. Целью данной курсовой работы было выявление основных видов угроз информационной безопасности и анализ их, на предмет влияния и методики противодействия.

# Список использованной литературы


Информация (Information) – это (http://economic-definition.com/Media/Informaciya_Information__eto.html)

1. Информационная безопасность и виды возможных угроз (http://www.inf74.ru/safety/ofitsialno/informatsionnaya-bezopasnost-i-vidyi-vozmozhnyih-ugroz/)

Нежелательный контент (https://www.anti-malware.ru/threats/unwanted-content)

Несанкционированный доступ (НСД)(www.anti-malware.ru/threats/unauthorized-access)

Утечки информации (www.anti-malware.ru/threats/leaks)

Потеря данных (Data Loss) (www.anti-malware.ru/threats/data-loss)

Мошенничество (фрод) (https://www.anti-malware.ru/threats/fraud)

1. Кибервойны (Cyberwarfare)(https://www.anti-malware.ru/threats/cyberwarfare)

Кибертерроризм (www.anti-malware.ru/threats/cyberterrorism)

ГОСТ Р 50922-96 "Защита информации. Основные термины и определения"

1. Лекция 9: Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP (https://www.intuit.ru/studies/courses/2291/591/lecture/12691)
2. Модель угроз и классификация несанкционированных воздействий в Автоматизированных Системах (http://www.m-g.ru/about/articles/105.html)

3. Как защитить компанию от утечки финансовой и другой секретной информации (https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/zaschita-ot-utechek-informatsii/)

# СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

**ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**
**№ РОСС RU.0001.01БИ00**

---

# СЕРТИФИКАТ СООТВЕТСТВИЯ
# № 3025

Выдан 25 ноября 2013 г.
Действителен до 25 ноября 2016 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Endpoint Security 10 для Windows»**, разработанное и производимое ЗАО «Лаборатория Касперского» в соответствии с техническими условиями ТУ 643.46856491.00068-01, является средством антивирусной защиты информации и соответствует требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012) и «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре643.46856491.00068-01 30.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Всесоюзный институт волоконно-оптических систем связи и обработки информации» (аттестат аккредитации от 19.06.2003 № СЗИ RU.594.Б016.040) – техническое заключение и технический отчет об оценке от 29.10.2013, экспертного заключения и отчета о сертификации от 07.11.2013 органа по сертификации ЗАО «Научно-производственное объединение «Эшелон» (аттестат аккредитации от 02.12.2010 № СЗИ RU.2321.А101.013).

Заявитель: ЗАО «Лаборатория Касперского»
Адрес: 123363, г. Москва, ул. Героев Панфиловцев, д. 10
Телефон: (495)797-8700

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанных в настоящем сертификате документов осуществляется испытательной лабораторией ЗАО «Всесоюзный институт волоконно-оптических систем связи и обработки информации».

**ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ**

**А.Куц**

---

**Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 25 ноября 2013 г.**

Приложение 1 Сертификат соответствия № 3025


1. [?] Информация (Information) – это (http://economic-definition.com/Media/Informaciya_Information__eto.html) ↑

2. [?]Информационная безопасность и виды возможных угроз (http://www.inf74.ru/safety/ofitsialno/informatsionnaya-bezopasnost-i-vidyi-vozmozhnyih-ugroz/) ↑

3. [?]Нежелательный контент (https://www.anti-malware.ru/threats/unwanted-content) ↑

4. [?]Несанкционированный доступ (НСД)(www.anti-malware.ru/threats/unauthorized-access) ↑

5. [?]Утечки информации (www.anti-malware.ru/threats/leaks) ↑

6. [?] Потеря данных (Data Loss) (www.anti-malware.ru/threats/data-loss) ↑

7. [?]Мошенничество (фрод) (https://www.anti-malware.ru/threats/fraud) ↑

8. [?]Кибервойны (Cyberwarfare)(https://www.anti-malware.ru/threats/cyberwarfare) ↑

9. [?]Кибертерроризм (www.anti-malware.ru/threats/cyberterrorism) ↑

10. [?] Лекция 9: Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP (https://www.intuit.ru/studies/courses/2291/591/lecture/12691)

    ↑

11. [?] Модель угроз и классификация несанкционированных воздействий в Автоматизированных Системах (http://www.m-g.ru/about/articles/105.html)

    ↑

12. [?] Как защитить компанию от утечки финансовой и другой секретной информации (https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/zaschita-ot-utechek-informatsii/)

    ↑

13. [?]Мошенничество (фрод) (www.anti-malware.ru/threats/fraud) ↑

14. [?]Кибервойны – войны будущего (https://topwar.ru/3261-kibervojny-vojny-budushhego.html ) ↑

15. [?]Кибертерроризмик (www.anti-malware.ru/threats/cyberterrorism) ↑