**Содержание:**

# ВВЕДЕНИЕ

Вопрос информационной безопасности был всегда актуальным и злободневным для любого государства, общества, человека, он существовал всегда, во все времена и у всех народов. Формирование современного информационного общества является закономерным этапом эволюции социума, характеризующегося, в первую очередь, масштабным внедрением информационных технологий и развитием глобального информационного пространства. Информационная среда определяет качество функционирования жизнедеятельности общества, его уровень развития и безопасность. Информационные технологии повлияли на сознание человека и возможности, изменили его образ жизни. Современные информационные технологии поменяли приоритеты и ценности. Сегодня, используемые в обществе информационные технологии рассматриваются как фактор, оказывающий огромное влияние на глобальное развитие социума и формирование информационной реальности. В настоящее время информационная сфера оказалась сердцевиной экономических, социальных, политических и других конфликтов в обществе. Научно-технический прогресс превратил информацию в продукт, который может являться оружием, средством достижения определенных целей либо удовлетворения потребностей отдельного покупателя.

Проблема защиты от проявившихся в третьем тысячелетии новых видов опасностей и угроз, порожденных информатизацией, беспокоит исследователей современного общества. Информационное взаимодействие, его своевременность, полнота и интенсивность регулируют все процессы жизнеобеспечения общества. Оттого информационная инфраструктура приобретает огромную ценность, безопасность которой необходимо обеспечивать всеми доступными инструментами и способами, постоянно разрабатывать новые средства обеспечения защиты информации и пересматривать эффективность и надежность уже используемых средств.

Целью данной курсовой работы является определение современных существующих видов угроз информационной безопасности в обществе и в коммерческих организациях и изучение их состава. Акцент в изучении понятия угроз сделан на современные интернет технологии, как на самую перспективную и стремительно

развивающуюся область деятельности, и в то же время, являющейся самой уязвимой.

Задачами курсовой работы являются:

1. Изучение основных понятий, видов и источников угроз информационной безопасности;
2. Определение видов угроз информационной безопасности на государственном уровне;
3. Определение видов и изучение состава угроз на мобильных устройствах;
4. Изучение видов угроз на коммерческих предприятиях;
5. Изучение комплекса мер, разрабатываемых организациями для защиты коммерческой информации.

# ГЛАВА 1. ПОНЯТИЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1.1 Основные определения понятия угрозы информационной безопасности

Для лучшего понимания изучаемой темы рассмотрим некоторые связанные понятия и определения.

Информационная безопасность - это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю.

В настоящее время выделяют четыре основных аспекта информационной безопасности:

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.

Угроза информационной безопасности - совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Под угрозой понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Под угрозой интересам субъектов информационных отношений понимают потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты информационной системы может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Для структурирования понимания проблемы рассмотрим различные классификации угроз.

## 1.2 Классификация и виды угроз

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

По аспекту информационной безопасности, на который направлены угрозы:

1. Угрозы конфиденциальности (неправомерный доступ к информации). Угроза нарушения конфиденциальности заключается в том, что информация

становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности, используется термин "утечка". Подобные угрозы могут возникать вследствие "человеческого фактора" (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств. К информации ограниченного доступа относится государственная тайна и конфиденциальная информация (коммерческая тайна, персональные данные, профессиональные виды тайна: врачебная, адвокатская, банковская, служебная, нотариальная, тайна страхования, следствия и судопроизводства, переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений (тайна связи), сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации (ноу-хау) и другие;
2. Угрозы целостности (неправомерное изменение данных). Угрозы нарушения целостности это - угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами - от умышленных действий персонала до выхода из строя оборудования;
3. Угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы). Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес целей.

По расположению источника угроз:

- 1. Внутренние (источники угроз располагаются внутри системы);
  2. Внешние (источники угроз находятся вне системы).

По размерам наносимого ущерба:

- 1. Общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);
  2. Локальные (причинение вреда отдельным частям объекта безопасности);
  3. Частные (причинение вреда отдельным свойствам элементов объекта безопасности).

По степени воздействия на информационную систему:

- 1. Пассивные (структура и содержание системы не изменяются);
  2. Активные (структура и содержание системы подвергается изменениям).

По природе возникновения:

- 1. Естественные (объективные) - вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;
  2. Искусственные (субъективные) - вызванные воздействием на информационную сферу человека.

Среди искусственных угроз в свою очередь выделяют:

- 1. Непреднамеренные (случайные) угрозы - ошибки программного обеспечения, персонала, сбои в работе систем, отказы вычислительной и коммуникационной техники;
  2. Преднамеренные (умышленные) угрозы - неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ и т.д. Преднамеренные угрозы обусловлены действиями людей. Основные проблемы информационной безопасности связаны прежде всего с умышленными угрозами, так как они являются главной причиной преступлений и правонарушений.

Каждая угроза имеет свою природу возникновения, для обеспечения безопасности любой информации и разработки эффективных мер защиты необходимо понимание источников возникновения угроз и потенциальной опасности. Рассмотрим основные из них.

## 1.3 Источники угроз информационной безопасности

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, например, конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом

следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Все источники угроз информационной безопасности можно разделить на три основные группы:

- 1. Обусловленные действиями субъекта (антропогенные источники) - субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры.
  2. Обусловленные техническими средствами (техногенные источники) - эти источники угроз менее прогнозируемы, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними.
  3. Стихийные источники - данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить), такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию и, поэтому меры против них должны применяться всегда. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

Задача обеспечения информационной безопасности подразумевает реализацию многоплановых и комплексных мер по предотвращению и отслеживанию угроз. В зависимости от источника и видов угроз непрерывно разрабатываются и улучшаются меры предотвращения опасности.

# ГЛАВА 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕ И ОБЩЕСТВЕ

# 2.1 Виды и предупреждение угроз государственной информационной безопасности

Согласно Закону о безопасности под **угрозой информационной безопасности** понимается совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. Концепция национальной безопасности РФ не дает определения угрозы, но называет некоторые из них в информационной сфере.

Угрозы информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения, являются:

1. все виды разведывательной деятельности зарубежных государств;
2. информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети);
3. диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
4. деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

К внутренним угрозам, которые будут представлять особую опасность в условиях обострения военно-политической обстановки, относятся:

1. нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях силовых структур Российской Федерации, на предприятиях оборонного комплекса;
2. преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
3. ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
4. возможная информационно-пропагандистская деятельность, подрывающая престиж силовых структур Российской Федерации и их боеготовность;

5. нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов.

К угрозам безопасности уже развернутых и создаваемых информационных и телекоммуникационных средств и систем относятся:

1. противоправные сбор и использование информации;
2. нарушения технологии обработки информации;
3. внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
4. разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
5. уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
6. воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
7. компрометация ключей и средств криптографической защиты информации;
8. утечка информации по техническим каналам;
9. внедрение электронных устройств, предназначенных для перехвата информации, в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
10. уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
11. перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
12. использование не сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
13. несанкционированный доступ к информации, находящейся в банках и базах данных;
14. нарушение законных ограничений на распространение информации.

Основными направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации являются:

1. систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности и определение соответствующих практических задач;
2. проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления и связи, имеющих в своем составе элементы вычислительной техники;
3. постоянное совершенствование средств защиты информации, развитие
4. Оценка состояния информационной безопасности базируется на анализе источников угроз (потенциальной возможности нарушения защиты).

Деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на нее, называют защитой информации. Объектом защиты является информация или носитель информации, или информационный процесс, которые нужно защищать.

Первое направление - защита информации от утечки - деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от разглашения направлена на предотвращение несанкционированного доведения ее до потребителя, не имеющего права доступа к этой информации.

Защита информации от несанкционированного доступа направлена на предотвращение получения информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Защита информации от технической разведки направлена на предотвращение получения информации разведкой с помощью технических средств.

Второе направление - защита информации от несанкционированного воздействия - деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение

информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Третье направление - защита информации от непреднамеренного воздействия - деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате уничтожению или сбою функционирования носителя информации.

Организовать защиту информации -значит создать систему защиты информации, а также разработать мероприятия по защите и контролю эффективности защиты информации.

Правовую основу информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, федеральными законами и подзаконными актами.

Государство также определят меру ответственности за нарушение положений законодательства в сфере ИБ. Например, глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи:

1. Статья 272 «Неправомерный доступ к компьютерной информации»;
2. Статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;
3. Статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

## 2.2 Состав современных угроз для мобильных устройств

Многие современные пользователи все чаще выбирают мобильные устройства в качестве своего основного способа коммуникации с Сетью. С помощью смартфонов и планшетов сегодня можно удовлетворить практически любые нужды в интернете. Совершенно неудивительно, что киберпреступники[1] взяли на прицел

мобильные платформы, куда постепенно мигрирует неискушенный в области информационной безопасности потребитель.

Следует помнить, что основная задача современных киберпреступников - получение прибыли, времена, когда вредоносные программы разрабатывали для развлечения или деструктивных действий далеко в прошлом. Следовательно, злоумышленники сосредотачиваются на методах получения прибыли за счет мобильных устройств обычных пользователей. Рассмотрим основные виды угроз в этой области.

Программы-вымогатели для мобильных устройств. Вредоносные программы, требующие выкуп, стали крайне распространенным классом злонамеренных программ для настольных компьютеров. Учитывая этот успех, злоумышленники решили использовать похожие схемы в случае с мобильными устройствами. Как правило, они блокируют работу устройства, требуя с жертвы выкуп, после выплаты которого возвращают пользователю контроль над смартфоном или планшетом. Также преступники выбирают в качестве целей истории звонков, контакты, фотографии или сообщения, что практически всегда вынуждает пользователя заплатить затребованную сумму. Среди наиболее опасных представителей вымогателей для мобильных устройств является DoubleLocker - первый мобильный шифратор, использующий службу специальных возможностей. Вредоносная программа оснащена сразу двумя инструментами для вымогательства: она шифрует данные в памяти устройства, а также может изменить PIN-код на произвольный. Использование службы специальных возможностей Android Accessibility Service (облегчает работу с устройством для людей с ограниченными возможностями) - одно из наиболее опасных нововведений, которые взяли на вооружение киберпреступники. Таким образом, злоумышленники успешно атакуют самую популярную мобильную платформу - Android.

Ботнеты[2]. Ботнеты, состоящие из взломанных смартфонов и планшетов - еще одна популярная киберугроза для владельцев смартфонов. Зараженные устройства, являющиеся частью ботнетов, находятся под контролем злоумышленников, которые в любой момент могут приказать им инициировать DDoS-атаку на какой-либо ресурс, либо начать массовую рассылку спам-писем. Очередная вредоносная программа для Android RottenSys могла превращать зараженные устройства в часть ботнета. Похожие приложения, превращающие Android-устройства в ботов, также были обнаружены в официальном магазине Google Play. В ходе расследования исследователи безопасности обнаружили более 300 вредоносных приложений в официальном магазине Play Store Google. Эти

приложения маскируются под видеоплееры, рингтоны или инструменты для управления хранилищами.

Вредоносные приложения. Еще одной киберугрозой, поджидающей пользователей мобильных устройств, являются вредоносные приложения, они тоже постоянно развиваются. Такие программы могут осуществлять самую разнообразную злонамеренную активность на устройстве жертвы, например, без его ведома совершать покупки в магазинах приложений. Деньги пользователя в таких случаях идут прямиком в карман злоумышленников. Порой таким приложениям даже не требуется взаимодействия с пользователем. Более того, вредоносные программы стали внедряться на уровне прошивки некоторыми производителями дешевых Android-устройств. Таких девайсов с "сюрпризом" исследователи насчитали 140. Эти вредоносные программы запускаются из директории "/system" с полными root-правами, их основной задачей является подключение к удаленному серверу, загрузка XML-файла и установка одного или нескольких приложений. Поскольку эти программу внедряются в прошивку, они могут установить в систему любое приложение, которое пожелает киберпреступник. При этом никакого взаимодействия с пользователем девайса не требуется. Среди злонамеренных приложений есть и те, что маскируются под легитимный софт. Недавно, например, был обнаружен вредоносный софт, атакующий пользователей Android, который при этом маскировался под Google Maps. После загрузки эти приложения пытались замаскироваться, отображая пользователю официальную иконку Google Maps или логотип Google Play Store.

Различные уязвимости в мобильных операционных системах только усложняют ситуацию. Многие киберпреступники отслеживают появление новых брешей, а с помощью недостатков в безопасности устройств можно сделать многое - например, обнаруженная в апреле уязвимость "Trustjacking" позволяла злоумышленникам удаленно управлять iPhone. Trustjacking можно было использовать, заманив пользователя на сайт, на котором размещен специальный код. Иногда не спасают и меры безопасности, разработанные корпорациями Google и Apple для своих магазинов Google Play и App Store. Так, в Google Play эксперты обнаружили шпионскую программу, которая пыталась замаскироваться под мессенджер (отправитель сообщений). После установки мессенджер загружал второе приложение, которое собирало информацию о местоположении устройства, сохраненные звонки, аудио- и видеозаписи, текстовые сообщение и другую частную информацию пользователей. С ростом популярности криптовалют, а также их курса, злоумышленники заинтересовались программами-майнерами[3],

добывающими для хозяина криптовалюту за счет устройств обычных пользователей. В том же Google Play исследователи нашли легитимные программы, которые были оснащены скрытыми майнерами. Сбор конфиденциальных данных также интересует преступников, поэтому они разрабатывают приложения вроде KevDroid, который может записывать звонки, совершаемые пользователем по мобильному устройству под управлением операционной системы Android.

Технология NFC призвана расширить стандарт бесконтактных карт, позволяя пользователям оплачивать покупки с помощью своего мобильного устройства. Таким образом, к смартфонам прикрепляется банковский счет или кредитная карта, что еще больше привлекает мошенников. Для кражи денежных средств пользователей в случае использования NFC злоумышленники прибегают к методу "bump and infect", который использует уязвимости в NFC. Этот метод уже зарекомендовал себя в прошлом, позволив преступникам похитить деньги со счетов граждан, использование "bump and infect" особенно характерно для таких мест, как торговые центры, парки или аэропорты.

Необходимо всегда помнить, что злоумышленников интересуют две вещи: денежные средства и личные данные (которые потом также можно продать, либо использовать для кражи денег). Исходя из этого, необходимо делать вывод, что можно хранить на устройстве, а что лучше доверить более защищенным платформам. Основными способами защиты мобильных устройств остаются использование криптостойких[4] паролей и последних версий программного обеспечения от разработчика.

# ГЛАВА 3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КОММЕРЧЕСКИХ ПРЕДПРИЯТИЯХ

## 3.1 Проблемы внешних и внутренних угроз в коммерческих организациях

Сегодня практически все предприятия используют автоматизированные системы обработки информации для повышения производственных показателей и принятия более взвешенных решений. Однако достаточно сложно обеспечить безопасность

подобных систем из-за большого количества уязвимостей в них. Чем более сложная и многофункциональная система, тем больше уязвимых мест с точки зрения угроз.

Угрозы могут исходить как от внешних компаний - поставщиков и подрядчиков, так и от сотрудников, поэтому обеспечение информационной безопасности является одной из главных проблем в современной производственной среде.

Есть обычные преступники, которые заражают мобильные телефоны, компьютеры и другие устройства. Далее идут более профессиональные киберпреступники, которые атакуют банки и другие предприятия финансовой и потребительской сферы. И есть третий, относительно новый вид киберпреступников. Такие профессионалы взламывают системы АСУ ТП[5] и похищают сырье и готовую продукцию. Это может быть уголь, бензин, зерно и т.д. Преступники вносят изменения на уровне ИТ, а потом забирают физический товар. Также, не стоит забывать о промышленном шпионаже. Зачастую при этом профессиональный уровень преступников, которые атакуют производственные предприятия, часто вполне соответствуют уровню шпионских атак.

Чтобы понять масштаб данных угроз, достаточно обратиться к статистике. Например, 10 февраля 2017 в России было зафиксировано 2 310 955 кибератак, 737 692 сетевых атак, 2 299 139 заражений, 2 045 заражений почты. Приведенная статистика показывает, что обеспечение информационной безопасности в промышленной среде все еще остается острой проблемой. Рассмотрим подробнее виды внешних и внутренних угроз в промышленной сфере.

Внешние угрозы представляют собой попытки получить доступ к данным извне и сопровождаются взломом серверов, сетей, аккаунтов работников и считыванием информации из технических каналов утечки (акустическое считывание с помощью жучков, камер, наводки на аппаратные средства, получение вибро-акустической информации из окон и архитектурных конструкций).

Внутренние угрозы подразумевают неправомерные действия персонала, рабочего отдела или управления фирмы. В результате пользователь системы, который работает с конфиденциальной информацией, может выдать информацию посторонним. На практике такая угроза встречается чаще остальных. Работник может годами выдавать конкурентам секретные данные. Это легко реализуется, ведь действия авторизованного пользователя администратор безопасности не квалифицирует как угрозу.

Попытка несанкционированного доступа может происходить несколькими путями:

1. через сотрудников, которые могут передавать конфиденциальные данные посторонним, забирать физические носители или получать доступ к охраняемой информации через печатные документы;
2. с помощью программного обеспечения злоумышленники осуществляют атаки, которые направлены на кражу пар "логин-пароль", перехват криптографических ключей для расшифровки данных, несанкционированного копирования информации;
3. с помощью аппаратных компонентов автоматизированной системы, например, внедрение прослушивающих устройств или применение аппаратных технологий считывания информации на расстоянии (вне контролируемой зоны).

Организационный уровень позволяет создать регламент работы пользователей с конфиденциальной информацией, подобрать кадры, организовать работу с документацией и физическими носителями данных.

Регламент работы пользователей с конфиденциальной информацией называют правилами разграничения доступа. Правила устанавливаются руководством компании совместно со службой безопасности и поставщиком, который внедряет систему безопасности. Цель - создать условия доступа к информационным ресурсам для каждого пользователя, к примеру, право на чтение, редактирование, передачу конфиденциального документа. Правила разграничения доступа разрабатываются на организационном уровне и внедряются на этапе работ с технической составляющей системы.

Залогом успешной борьбы с несанкционированным доступом к информации и перехватом данных служит четкое представление о каналах утечки информации.

Интегральные схемы, на которых основана работа компьютеров, создают высокочастотные изменения уровня напряжения и токов. Колебания распространяются по проводам и могут не только трансформироваться в доступную для понимания форму, но и перехватываться специальными устройствами. В сам компьютер или монитор могут устанавливаться устройства для перехвата информации, которая выводиться на монитор или вводиться с клавиатуры. Перехват возможен и при передаче информации по внешним каналам связи, например, по телефонной линии.

Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация.

Идентификация - это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией. Аутентификация - это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.

Эти средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правила, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты -пароль.

## 3.2 Особенности угроз информационной безопасности в банковском секторе

Со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств.

В наши дни в связи со всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возросло. Еще 30 лет назад объектом информационных атак были данные о клиентах банков или о деятельности самого банка. Такие атаки были редкими, круг их заказчиков был очень узок, а ущерб мог быть значительным лишь в особых случаях. В настоящее время в результате повсеместного распространения электронных платежей, пластиковых карт, компьютерных сетей объектом информационных атак стали непосредственно денежные средства как банков, так и их клиентов. Совершить попытку хищения может любой -необходимо лишь наличие компьютера, подключенного к сети Интернет. Причем для этого не требуется физически проникать в банк, можно находиться и за тысячи километров от него.

Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Однако прогресс в технике преступлений шел не менее быстрыми темпами, чем развитие банковских технологий. В настоящее время

свыше 90 % всех преступлений связана с использованием автоматизированных систем обработки информации банка (АСОИБ). Следовательно, при создании и модернизации АСОИБ банкам необходимо уделять пристальное внимание обеспечению ее безопасности.

Именно эта проблема является сейчас наиболее актуальной и наименее исследованной. Особенно актуальна данная проблема в России. В западных банках программное обеспечение разрабатываются конкретно под каждый банк и устройство АСОИБ во многом является коммерческой тайной. В России получили распространение "стандартные" банковские пакеты, информация о которых широко известна, что облегчает несанкционированный доступ в банковские компьютерные системы.

Наиболее часто компании из финансового сектора сталкиваются с фишинговыми[6] атаками (30%) и DDoS-атаками[7] (26%).

Угрозы фишинговых атак продолжают расти ежегодно. Смещение фокуса в сторону фишинга - одно из следствий развития инструментов, доступных киберпреступникам. В частности, несмотря на то, что число взломов в единицу времени в целом за последние годы сохраняется на одном уровне, на данный момент финансовые организации уже не всегда могут своевременно обнаруживать и точно фиксировать подобные инциденты.

Среднее количество атак на веб-приложения в финансовой сфере составляет около 1500 в день. Основная часть из них -это автоматизированные инструменты и сканеры. Такая активность автоматизированных средств создает большой информационный фон и усложняет выявление реальных инцидентов. Основные векторы атак на веб-приложения - это внедрение SQLi операторов (26,8%) и межсайтовая подделка запросов (25,6%). Повышенный интерес к этим типам атак связан с возможностью получения информации о базах данных клиентов и персональной информации пользователей. Третье и четвертое место занимают выход за пределы значений директории - 25% и удаленное выполнение кода - 19,5%. При этом основная часть инцидентов (60%) - связана с удалённым выполнением кода.

Однако, большая часть мошенничества, связанного с хищением денег со счетов клиентов происходит "руками самих клиентов". Держатели счетов сами отдают свои пароли, свои карточки, телефоны, передают смс-коды подтверждения. Такое мошенничество называется социальной инженерией.

В рамках социальной инженерии злоумышленники находят причину, по которой человек может совершить действия, ведущие к утрате денег. Как правило, задействован корыстный интерес - например, купить что-то по скидке или интересное коммерческое предложение. Также используется предлог, что якобы родственник клиента попал в беду.

Особенно подвержены такому воздействию люди пожилого возраста, которые думают о своих внуках, детях и получив просьбу, сразу бегут к банкомату, делают то, что им говорят злоумышленники.

Бывают случаи, когда системы противодействия мошенничеству банка обнаруживают, что мошенничество происходит и останавливают транзакцию.

Случается, что на "удочку" социальных инженеров попадаются даже сотрудники банка. Технические способы защиты клиентов достаточно эффективны, но противодействие социальным инженерам представляет достаточно большую проблему. Ее решение банки видят в повышении финансовой и компьютерной грамотности населения.

# ЗАКЛЮЧЕНИЕ

Цели и задачи курсовой работы выполнены. В работе определены и рассмотрены самые актуальные угрозы информационной безопасности и их состав. Актуальность данной работы подтверждается тем, что изученная область является наболевшей проблемой современного общества, роль информации в современном мире огромна и цена безопасности становится слишком высока. Благодаря инновациям в мире появляются новые возможности для развития и расширения бизнеса, для создания удобства и комфорта жизни, для совершенства и быстроты связей и коммуникации в обществе, но киберпреступники также стремятся использовать эти преимущества в своих корыстных целях. Чтобы идти в ногу со временем, государству, организациям и обычным обывателям необходимо быть дальновидными и продумывать свои действия наперед. Ни один участок инфраструктуры не должен оставаться без защиты или наблюдения. В противном случае каждая компания или человек рискует стать следующей жертвой продуманной, целенаправленной и крупномасштабной кибератаки либо иной угрозы. Понимание возможных угроз и готовность к ним позволяет выявлять возможные риски информационной безопасности и разрабатывать и обеспечивать соответствующие способы защиты.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ


1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие /Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.
2. Форристал Д. Защита от хакеров Web-приложений [Электронный ресурс] /Джефф Форристал, Крис Брумс, Дрю Симонис и др.; Пер. с англ. В. Зорина.- М. : Компания АйТи : ДМК Пресс, 2009. - 496 с.
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.
4. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.
5. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. - М.: Русайнс, 2017. - 64 с.
6. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. - 448 с
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск: Издательский центр ЮУрГУ, 2014. – 137 с.
9. https://ru.wikipedia.org/
10. https://www.anti-malware.ru/analytics/Threats_Analysis


1. Кибер (англ. CYBER) – приставка, использующаяся для того, чтобы присвоить слову значение чего-то, относящегося к эпохе компьютеров, Интернета и цифровых технологий. ↑

2. Ботнет - компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами - автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно

используются для нелегальной или неодобряемой деятельности. ↑

3. Майнинг, также добыча (от англ. *mining — добыча полезных ископаемых*) — деятельность по созданию новых структур для обеспечения функционирования криптовалютных платформ. ↑

4. Криптографическая стойкость (криптостойкость)- способность криптографического алгоритмапротивостоять возможным атакам на не криптоанализа.Стойким считается алгоритм, который для успешной атаки требует о ↑

5. Автоматизированные системы управления технологическими процессами (АСУ ТП) — это комплекс программных и технических средств, предназначенных для создания систем автоматизации управления технологическим оборудованием и производственными процессами на предприятиях (автоматизация производства) ↑

6. Фи́шинг (англ. *phishing* от *fishing* «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. ↑

7. DoS ( англ. *Denial of Service* «отказ в обслуживании») — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. ↑