Содержание:

Введение

В настоящее время современное человечество живет в информационную эпоху, в сфере информационного пространства происходит улучшение технических возможностей получения и передачи (распространения) информации. Информация является одним из фундаментальных понятий современности и относится к разряду тех, которые имеют очень широкое употребление.

Современные информационные технологии используются во всех отраслях российской экономики и сферах общественной жизни, а в стремительно происходящем процессе информатизации тем или иным образом участвует все большая часть населения нашей страны.

Сегодня понятие информационная безопасность входит во все сферы жизнедеятельности общества. Защиту информации можно рассматривать как совокупность тесно связанных между собой задач в области международной этики, права, организации управления, разработки технических средств, программирования и математики.

Главной целью любой системы обеспечения информационной безопасности является создание условий функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение в рамках производственной деятельности всех подразделений предприятия

Таким образом, под информационной угрозой понимают потенциальную возможность нарушения информационной безопасности или потенциально возможные событие, действие, несущее определенную информацию явление, которое может привести к нанесению ущерба чьим-либо интересам.

Целью курсовой работы является изучить основные виды и составы угроз информационной безопасности.

Задачи работы:

1. Изучить основные понятия информационной безопасности.
2. Рассмотреть виды и источники угрозы информационной безопасности.
3. Рассмотреть основные составляющие информационной безопасности.

Для выполнения курсовой работы по теме «Виды и состав угроз информационной безопасности», проведем изучение научных работ, статей, учебных пособий, нормативно-правовых актов и электронных источников.

Впроцессенаписаниякурсовой работы будут использоватьсяследующиеметодыисследования:анализлитературныхисточников,методоб

В результате анализа, можно сделать вывод, что данная тема в настоящее время мало изучена и практически не раскрыта в полном объеме, а также выявлен значительный дефицит современной учебной литературы в данном направлении.

Нормативную базу исследования составили действующие нормативные акты:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»;
- Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Доктрине информационной безопасности Российской Федерации утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895.

Структурноработапредставленаизведения,трехразделов,заключенияиСписок использованной литературы.

1. Основные понятия информационной безопасности

Для рассмотрения сущности понятия «угроза информационной безопасности», рассмотрим каждое понятие по отдельности, «угроза», «информация», «безопасность».

В современном мире всеобщей компьютеризации, информация приобретает новое качество, влияющее на развитие общества. Понятие информация является одним из фундаментальных в современной науке вообще и базовым для информатики и информационных технологий.

В настоящее время отсутствует общепринятое представление о том, что такое информация. Информация является одним из фундаментальных понятий современности и относится к разряду тех, которые имеют очень широкое употребление.

СогласноФедеральномузаконуподинформациейпонимаютсясведения(сообщения,данные) представления[1].

В ГОСТ Р 50922-2006дано следующее определение информация – сведения (сообщения, данные) независимо от формы их представления, подзащищаемой информацией понимают информацию, которая является предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации[2].

Автор Толкового словаря русского языка С.И. Ожегов выделил следующее понятие «информация» - это сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством[3].

Информация в электронной сфере – это число, которое всегда фиксировано и хранится в памяти персонального компьютера.

В учебнике Гаврилова О.А. под информацией понимаются сведения об окружающем мире (объекты, явления, события, процессы и т.д.), которые уменьшают существующую неопределенность, неполноту знаний, которые можно передавать устным, письменным или другим способом, а также с помощью условных сигналов, технических и вычислительных средств и др[4].

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства.

В утратившем силу ФЗ «Об информации, информатизации и защите информации» под информационной безопасностью понималось состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства.

В других источниках приводятся следующие определения:

Согласно Доктрине информационной безопасности Российской Федерации под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[5].

В Конституции Российской Федерации, а также Декларации прав и свобод человека и гражданина Российской Федерации определено, что каждый имеет право свободно искать, получать, передавать, производить и распространить информацию любым законным способом. Ограничения этого права могут устанавливаться законом только в целях охраны личной, семейной, профессиональной, коммерческой и государственной тайны, а также нравственности[6].

Информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[7].

Автор Макаренко С.И. в учебном пособии под информационной безопасностью понимает защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры[8].

Таким образом, защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (рисунок 1).

Целью реализации информационной безопасности какого-либо объекта является построение Системы обеспечения информационной безопасности данного объекта (СОИБ). Для построения и эффективной эксплуатации СОИБ необходимо:

Рисунок 1. Компоненты защиты информации

- выявить требования защиты информации, специфические для данного объекта защиты;

- учесть требования национального и международного законодательства;
- использовать наработанные практики (стандарты, методологии) построения подобных СОИБ;
- определить подразделения, ответственные за реализацию и поддержку СОИБ;
- распределить между подразделениями области ответственности в осуществлении требований СОИБ;
- на базе управления рисками информационной безопасности определить общие положения, технические и организационные требования, составляющие Политику информационной безопасности объекта защиты;
- реализовать требования Политики информационной безопасности, внедрив соответствующие программно-технические способы и средства защиты информации;
- реализовать Систему менеджмента (управления) информационной безопасности (СМИБ);
- используя СМИБ, организовать регулярный контроль эффективности СОИБ и, при необходимости, пересмотр и корректировку СОИБ и СМИБ.

Основным понятием информационной безопасности является понятие «угроза». В учебной литературе под угрозой безопасности информации, понимают возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию: нарушение физической целостности, логической структуры, несанкционированная модификация информации, несанкционированное получение и размножения информации[9].

Согласно ГОСТ Р 50922-2006,под угрозой понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации[10].

В Указе Президента Российская федерация от 05 декабря 2016 №646, под угрозой информационной безопасности понимается совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере[11].

В учебном пособии Макаренко С.И.,понятие угрозы информационной безопасности, трактуется, как оборотная сторона использования информационных технологий [12].

В учебном пособии Грибунина В.Г., понимается угроза безопасности информации — это совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее[13].

Таким образом, можно сделать вывод, из рассмотренных выше определений следует, что некоторые приведенные факторы являются одновременно и угрозами, например, возможная диверсия в отношении объекта информатизации. С другой стороны, такой фактор, как несоблюдение требований по защите информации, угрозой не является.

2. Угрозы информационной безопасности

2.1 Виды угроз информационной безопасности

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующиевиды:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
2. угрозы информационному обеспечению государственной политики Российской Федерации;
3. угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
4. угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности,индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных

правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственнойполитики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории.

Угрозами развитию отечественной индустрии информации,включая индустрию средств информатизации, телекоммуникациии связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационныхсредств и систем, как уже развернутых, так и создаваемыхна территории России, могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств 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;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линияхсвязи, дешифрование этой информации и навязывание ложной информации;
- использование сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации,средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейсяв банках и базах данных;
- нарушение законных ограничений на распространение информации.

Создание системы информационной безопасности предполагает выявление источниковинформационных опасностей и угроз. Существуют четыре действия, производимые с информацией, которые могут содержатьв себе угрозу: сбор, модификация (искажение), утечка и уничтожение информации. Эти действия являются базовыми для рассмотрения классификации источников информационных опасностей и угроз.

Рассмотрим внешние и внутренние источники информационных опасностей и угроз.

Источниками внутренних угроз являются[14]:

1. Сотрудники организации.
2. Программное обеспечение.
3. Аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

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

К внешним источникам угроз относятся:

1. Компьютерные вирусы и вредоносные программы.
2. Организации и отдельные лица.
3. Стихийные бедствия.

Формами проявления внешних угроз являются[15]:

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

Все перечисленные выше виды угроз (формы проявления) можно разделить на умышленные и неумышленные.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации: информационные,программные, физические, радиоэлектронные и организационно-правовые.

К информационным угрозам относятся:

- несанкционированный доступ к информационным ресурсам;
- незаконное копирование данных в информационных системах;
- хищение информации из библиотек, архивов, банков и баз данных;
- нарушение технологии обработки информации;
- противозаконный сбор и использование информации;
- использование информационного оружия.

К программным угрозам относятся:

- использование ошибок и «дыр» в программном обеспечении;
- компьютерные вирусы и вредоносные программы;
- установка «закладных» устройств.

К физическим угрозам относятся:

- уничтожение или разрушение средств обработки информации и связи;
- хищение носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты данных;
- воздействие на персонал.

К радиоэлектронным угрозам относятся:

- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К организационно-правовым угрозам относятся:

- нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере;
- закупки несовершенных или устаревших информационных технологий и средств информатизации[16].

Угроза реализуется в виде атаки, в результате чего и происходитнарушение безопасности информации. Целесообразно выделитьследующие основные виды нарушения безопасности информации[17]:

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение доступности.

Знание возможных угроз, а также уязвимых мест зашиты, которыеэти угрозы обычно эксплуатируют, необходимо для выборанаиболее эффективных средств обеспечения безопасности.

В ГОСТ15408-2002приведена другая классификация видов угроз.

Основные угрозы для паролевой защиты можно подразделить на явные и скрытые.

Наиболее очевидными явными угрозами являются физические — хищение носителя (диска с паролем, электронного ключа с парольной информацией и т. д.), а также визуальный съем пароля при вводе с клавиатуры либо монитора. Кроме того, при использовании длинных сложных паролей пользователи подчас записывают свой пароль, что также является объектом физического хищения.

К техническим явным угрозам можно отнести подбор пароля: автоматизированный (вручную пользователем), либо автоматический, предполагающий запуск пользователем специальной программы подбора паролей. Кроме того, для сравнения, вводимого и эталонного значений пароля эталонное значение пароля должно храниться на защищаемом объекте либо на сервере в сети. Это эталонное значение без соблюдения соответствующих мер по хранению паролей (разграничение доступа к области памяти или реестра, где хранятся пароли) может быть похищено злоумышленником.

Наиболее опасными являются скрытые угрозы: технический съем пароля при вводе, модификация механизма парольной защиты и модификация учетных данных на защищаемом объекте.

Технический съем пароля при вводе. В этом случае злоумышленник размещает на компьютере соответствующую программу, позволяющую перехватывать поступающую на защищаемый объект информацию. Подобные программы дают возможность автоматически фильтровать перехватываемую информацию по определенным признакам, в том числе в целях обнаружения паролей.

Модификация механизма парольной защиты. Существует возможность отключения механизма парольной защиты злоумышленником, например, путем загрузки системы с внешнего носителя. Если механизм парольной защиты представляет собой некий процесс, то выполнение данного процесса можно остановить средствами системного монитора либо монитора приложений. Подобная возможность существует для ОС Windows.

Модификация учетных данных на защищаемом объекте (замена учетных записей, сброс пароля). Угроза заключается в модификации учетных данных на защищаемом объекте. Это осуществляется путем либо их замены, либо сброса в исходное состояние настроек механизма защиты. Примером может служить известная программная атака на BIOS — сброс настроек BIOS в исходное состояние посредством изменения контрольных сумм BIOS[18].

Согласно требованиям, прописанным в действующем уголовном праве, в котором определяется состав преступления и к нему можно отнести:

- копирование компьютерной информации;
- хищение совершенные с корыстной целью;
- стирание компьютерной информации;
- порча или полное уничтожение имущества;
- искусственное затруднение доступа пользователей к информации;
- несанкционированное уничтожение, блокирование, модификация, копирование информации;
- повреждение или изменение свойств имущества, ухудшающее его состояние;
- изменение компьютерной информации;
- обман, умышленное искажение или сокрытие информации.

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления.

2.2 Источники угроз информационной безопасности

Все источники угроз информационной безопасности можно разделить на три основные группы (рисунок 1).

1. Обусловленные действиями субъекта, которые приводят к нарушению безопасности информации. Данные действия могут быть квалифицированы как умышленные или случайные преступления.
2. Непреднамеренные угрозы на объект информатизации.
3. Преднамеренные угрозы на объект информатизации.
4. Обусловленные техническими средствами. Данные источники угроз менее прогнозируемые и напрямую зависят от свойств техники, а также могут быть

как внутренними, так и внешними.

5. Стихийные источники.

Данная группа объединяет следующие обстоятельства: стихийные бедствия, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить. Данные обстоятельства 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 являются внешними по отношению к защищаемому объекту, под которыми понимаются природные катаклизмы[19].

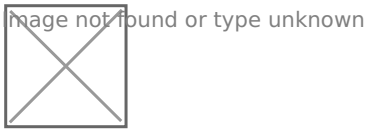

Рисунок 2. Классификация источников угроз

1. Основные составляющие информационной безопасности

Информационная безопасность представляется весьма многомерной областью деятельности, в которой успех может принести только систематический, комплексный подход.

С методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и их интересов.

В обеспечении информационной безопасности нуждаются разные субъекты информационных отношений:

- государство в целом или отдельные органы и организации;
- общественные или коммерческие организации (объединения), предприятия (юридические лица);
- отдельные граждане (физические лица).

Весь спектр интересов субъектов, связанных с использованием информации, можно разделить на следующие составляющие информационной безопасности: обеспечение доступности, целостности и конфиденциальности информации и поддерживающей инфраструктуры[20].

Доступность - это возможность за приемлемое время получить требуемую информационную услугу. Доступность характеризует способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующей их информации.

Целостность - защищенность информации от разрушения и несанкционированного изменения. Целостность гарантирует то, что информация существует в ее исходном, неискаженном виде (неизмененном по отношению к некоторому фиксированному состоянию). Нарушение этой категории является фальсификацией.

Конфиденциальность - это защита от несанкционированного доступа к информации. Конфиденциальность гарантирует, что конкретная информация доступна только кругу лиц, для которого она предназначена и, следовательно, указывает на необходимость введения ограничений доступа к данной информации для определенного круга пользователей. Нарушение этой категории является хищением либо называется раскрытием информации.

Для получения субъектами определенных информационных услуг используются информационные системы. Если по некоторым причинам предоставить эти услуги пользователям оказывается невозможно, то тем самым наносится ущерб всем субъектам информационных отношений. Поэтому, принято выделять доступность как важнейший элемент информационной безопасности, однако при этом, не противопоставляя доступность остальным аспектам.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий). Средства контроля динамической целостности применяются в частности при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений[21].

Конфиденциальность - самый проработанный аспект информационной безопасности. Но практическая реализация мер по обеспечению конфиденциальности информации имеет в Россиисерьезные трудности.

Во-первых, сведения о технических каналах утечки информации являются закрытыми. Большинство пользователей лишено возможности составить представление о потенциальных рисках.

Во-вторых, возможность использования пользовательской криптографии как основного средства обеспечения конфиденциальности ограничена техническими проблемами и законодательными препятствиями.

Значение каждой из составляющих информационной безопасности для разных категорий субъектов информационных отношений различно. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные заведения. В первом случае «пусть все сломается, но злоумышленник не должен узнать ни один секретный бит», во втором – «у нас нет никаких секретов, только бы все работало».

В случае государственных организаций во главу ставится конфиденциальность. Далее, для государственных структур особую значимость принимает целостность информации. Доступность как одна из составляющих ИБ по отношению к двум другим составляющим обладает наименьшим приоритетом для государственных структур.

Для коммерческих организаций ведущую роль играет доступность информации. Особенно ярко это проявляется в разного рода системах управления - производством, транспортном и т.п. Весьма неприятные последствия - и материальные, и моральные - может иметь длительная недоступность информационных услуг, которыми пользуется большое количество пользователей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность также важнейший аспект ИБ коммерческих структур. Набор и характеристики комплектующих изделий, ход технологического процесса, значение скорости самолета, заходящего на посадку - все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. В то же время конфиденциальность в случае коммерческой информации играет несколько меньшую роль[22].

Для граждан на первое место можно поставить целостность и доступность информации, обладание которой необходимо для осуществления нормальной жизнедеятельности. Конфиденциальность также играет важную роль, поскольку информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар и, находясь в чужих руках, может становиться орудием преступления, средством мщения, товаром для продажи конкуренту. В этой связи надо отметить, что физические лица на сегодняшний день являются самыми незащищенными субъектами информационных отношений

[23].

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных[24]:

- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Классификацию мер защиты можно представить в виде трех уровней.

- Законодательный уровень. В Уголовном кодексе Российской Федерации имеется гл. 28 «Преступления в сфере компьютерной информации».
- Административный и процедурный уровни. На административном и процедурном уровнях формируются политика безопасности и комплекс процедур, определяющих действия персонала в штатных и критических условиях.
- Программно-технический уровень. К этому уровню относятся программные и аппаратные средства, которые составляют технику информационной безопасности, например, идентификация пользователей, управление доступом, криптография, экранирование[25].

1. Защита на уровне BIOS требует ввод пароля при загрузке компьютера, а защита на заставку перекроит доступ к информации при происшествии определенного промежутка времени.
2. Защита данных на жестком диске (винчестере):

- Резервное копирование данных.
- Дефрагментация жесткого диска.

1. Защита паролем.

К основным методам, которые используются при защите информации, можно отнести следующие: скрытие, ранжирование, дезинформация, дробление, кодирование, шифрование, страхование.

Сопоставить каждому пользователю соответствующую ему разграничительную политику доступа на защищаемом объекте призвана идентификация. Для этого

пользователь должен себя идентифицировать: указать свое «имя» (идентификатор). Таким образом проверяется, относится ли регистрирующийся пользователь к пользователям, идентифицируемым системой. И в соответствии с введенным идентификатором пользователю будут сопоставлены соответствующие права доступа[26].

Субъект может подтвердить свою подлинность, если предъявит по крайней мере одну из следующих сущностей:

- пароль, личный идентификационный номер, криптографический ключ и т.п.;
- личную карточку или иное устройство аналогичного назначения;
- голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики;
- координаты.

Главное достоинство парольной аутентификации − простота и привычность.

Заключение

В ходе выполнения курсовой работы по теме «Виды и состав угроз информационной безопасности»была достигнута цель и решены поставленные задачи.

В результате анализа учебной литературы и законодательства по вопросам видов и состав угроз информационной безопасности можно сделать вывод, что информационная безопасность развивается чрезвычайно быстрыми темпами. Только комплексный, систематический, современный подход способен успешно противостоять нарастающим угрозам.

Ключевые понятия информационной безопасности: конфиденциальность, целостность и доступность информации, а любое действие, направленное на их нарушение, называется угрозой.

Основные понятия, связанные с безопасностью регламентированы в основополагающих документах.

Следовательно, угроза - это действие, направленное на повреждение конфиденциальности, целостности и доступности информации, а угроза, которая уже реализована, называется атакой.

Умышленные угрозы являются наибольшей проблемой и защита информации направленна именно на борьбу с такими угрозами. Если при случайной угрозе (ошибки пользователей, сбой оборудования), то умышленные направлены нанести вред пользователю операционной системы.

Переход к электронному государственному управлению («электронному правительству», «электронному государству») – характерная тенденция современного этапа информатизации органов государственной власти Российской Федерации. Несмотря на свою новизну, перечисленные понятия являются достаточно устоявшимися и постоянно используются как в научной литературе, так и в нормативных правовых актах.

В современном мире утечка конфиденциальной информации может повлечь серьезные последствия, но при этом многие пользователи используют для хранения файлов и совместной работы над ними средства, которые не всегда защищены достаточно надежно.

Таким образом, защита информации – комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостность, доступность и, если нужно, конфиденциальность информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Вредоносные программы способны самостоятельно распространяться, они переходят с одного компьютер на другой с помощью зараженных файлов, дискет или писем по электронной почте. Многопользовательские компьютеры в свою очередь намного меньше страдают от вирусов чем персональные, так как на них имеется система защиты.

Все рассмотренные угрозы приносят большой ущерб информационным системам, для каждого случая в отдельности разработаны свои способы.

В настоящее время существующая архитектура безопасности включает в себя следующие способы обеспечения безопасности: шифрование, электронная цифровая подпись, целостность данных и управление доступом.

Список использованной литературы

1. Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации».

2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст)
3. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
4. Доктрина информационной безопасности Российской Федерации утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895
5. Гаврилов О. А. Курс правовой информатики. Учебник для вузов. – М.: Издательство НОРМА, 2011. – 355 с.
6. Гафнер В.В. Информационная безопасность : учеб. пособие /' В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с.
7. Горюхина, Е.Ю. Информационная безопасность: Учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. – Воронеж: ФГБОУ ВО Воронежский ГАУ, 2015. – 220 с.
8. Грибунин В.Г. Комплексная система защиты информации на предприятии учеб. пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В.В. Чудовский. — М. Издательский центр «Академия», 2009. — 416 с.
9. Загорский А.В. Угрозы информационной безопасности в кризисах и конфликтах XXI века / под ред. - А.В. Загорского, Н.П. Ромашкиной.–М.: ИМЭМО РАН, 2015.–151 с.
10. Ерохин В.В., Погонышева Д.А., Степченко И.Г. Безопасность информационных систем. Учебное пособие — М.: Флинта, Наука, 2015. — 184 с.
11. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.
12. Михеева Е.В., Титова О.И. Информационные технологии в профессиональной деятельности. Технические специальности. Учебник. — М.: Академия, 2014. — 416 с.
13. Моисеев А.И. Информационная безопасность распределённых информационных систем: учеб. / А.И. Моисеев, Д.Б. Жмуров. – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2013. – 180 с.
14. Толковый словарь Ожегова / Что такое Информация?. [Электронный ресурс].– Режим доступа: http://dic.academic.ru/dic.nsf/ogegova/75266

1. Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации». ↑

2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения ↑

3. Толковый словарь Ожегова / Что такое Информация?. [Электронный ресурс].– Режим доступа: http://dic.academic.ru/dic.nsf/ogegova/75266 (дата обращения: 22.06.2016). ↑

4. Гаврилов О. А. Курс правовой информатики. Учебник для вузов. – М.: Издательство НОРМА, 2011. – 355 с. ↑

5. Доктрина информационной безопасности Российской Федерации утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 ↑

6. Моисеев А.И. Информационная безопасность распределённых информационных систем: учеб. / А.И. Моисеев, Д.Б. Жмуров. – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2013. – С.52. ↑

7. Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» ↑

8. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – С.20. ↑

9. Ерохин В.В., Погонышева Д.А., Степченко И.Г. Безопасность информационных систем. Учебное пособие — М.: Флинта, Наука, 2015. — С.7. ↑

10. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения ↑

11. Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» ↑

12. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – С.121. ↑

13. Грибунин В.Г. Комплексная система защиты информации на предприятии учеб. пособие для стул. высш. учеб. заведений / В. Г. Грибунин, В.В.Чудовский. — М. Издательский центр «Академия», 2009. — С.121. ↑

14. Гафнер В.В. Информационная безопасность : учеб. пособие /' В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — С.24. ↑

15. Гафнер В.В. Информационная безопасность : учеб. пособие /' В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — С.25. ↑

16. Гафнер В.В. Информационная безопасность : учеб. пособие /' В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — С.26. ↑

17. Грибунин В.Г. Комплексная система защиты информации на предприятии учеб. пособие для стул. высш. учеб. заведений / В. Г. Грибунин, В.В.Чудовский. — М. Издательский центр «Академия», 2009. – С.122. ↑

18. Михеева Е.В., Титова О.И. Информационные технологии в профессиональной деятельности. Технические специальности. Учебник. — М.: Академия, 2014. — С.392. ↑

19. Пулко Т.А. Введение в информационную безопасность. Учебно-методическое пособие. — Минск.: БГУИР, 2016. — С.71. ↑

20. Горюхина, Е.Ю. Информационная безопасность: Учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. – Воронеж: ФГБОУ ВО Воронежский ГАУ, 2015. – С.10. ↑

21. Горюхина, Е.Ю. Информационная безопасность: Учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. – Воронеж: ФГБОУ ВО Воронежский ГАУ, 2015. – С.11. ↑

22. Горюхина, Е.Ю. Информационная безопасность: Учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. – Воронеж: ФГБОУ ВО Воронежский ГАУ, 2015. – С.12. ↑

23. Горюхина, Е.Ю. Информационная безопасность: Учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. – Воронеж: ФГБОУ ВО Воронежский

ГАУ, 2015. – С.13 ↑

24. Михеева Е.В., Титова О.И. Информационные технологии в про-фессиональной деятельности. Технические специальности. Учебник. — М.: Академия, 2014. — С.388. ↑

25. Михеева Е.В., Титова О.И. Информационные технологии в про-фессиональной деятельности. Технические специальности. Учебник. — М.: Академия, 2014. — С.390. ↑

26. Михеева Е.В., Титова О.И. Информационные технологии в про-фессиональной деятельности. Технические специальности. Учебник. — М.: Академия, 2014. — С.390. ↑