## Содержание

[Введение 2](#_Toc168204465)

[Виды, средства и методы защиты информации 5](#_Toc168204466)

[Объекты защиты информации 19](#_Toc168204467)

[Сопоставление методов защиты информации и объектов защиты 28](#_Toc168204469)

[Заключение 37](#_Toc168204470)

[Приложение 39](#_Toc168204471)

[Использованные источники 41](#_Toc168204472)

## Введение

Обеспечение информационной безопасности России является одной из приоритетных государственных задач. Под информационной безопасностью (безопасностью информации) понимают состояние защищенности собственно информации и её носителей (человека, органов, систем и средств, обеспечивающих получение, обработку, хранение, передачу и использование информации) от различного вида угроз. Источники этих угроз могут преднамеренными (т.е. имеющими цель незаконного получения информации) и непреднамеренными (такую цель не преследующими).

Обеспечить безопасность информации можно различными методами и средствами как организационного, так и инженерного характера. Комплекс организационных мер, программных, технических и других методов и средств обеспечения безопасности информации образует систему защиты информации.

В Российской Федерации формируется Концепция информационной безопасности как составной части национальной безопасности России. В рамках проекта этой Концепции сформулированы основные положения государственной политики обеспечения информационной безопасности, имеющие большое значение для построения как государственной, так и ведомственных систем защиты информации и заключающиеся в следующем:

– государство формирует Федеральную программу ИБ, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности России;

– государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

– ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

– доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

– ответственность за сохранность, засекречивание и рассекречивание информации персонифицируется;

– юридические и физические лица, собирающие, накапливающие и обрабатывающие персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

– государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования предприятий и организаций в области защиты информации;

– государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации, и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

– государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

– государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через СМИ;

– государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

– государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем.

На основе приведенных положений государственной политики обеспечения информационной безопасности должны проводиться все мероприятия по защите информации в различных сферах деятельности государства, в т.ч. в оборонной сфере. Это предполагает, в свою очередь, разработку соответствующего научно-технического и организационно-правого обеспечения защиты информации.

Научно-техническое обеспечение должно быть направлено на достижение необходимого уровня защищенности информационных технологий, систем и средств информатизации и связи и заключается в проведении фундаментальных и прикладных исследований, создании защищенных технологий, средств и систем, а также создании средств и систем контроля состояния защиты информации.

Организационно-правовое обеспечение защиты информации должно представлять собой высокоупорядоченную совокупность организационных решений, законов, нормативов и правил, регламентирующих как общую организацию работ по защите информации в масштабах государства и ведомства, так и создание, и функционирование систем защиты информации на конкретных объектах.

Целью данной курсовой работы является – сопоставить виды, средства и методы защиты информации с объектами защиты.

Объект исследования – объекты защиты информации.

Поставленная цель раскрывается через следующие задачи:

1. рассмотреть виды, средства и методы защиты информации;
2. обозначить объекты защиты информации;
3. сопоставить способы защиты информации с объектами защиты.

## Виды, средства и методы защиты информации

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

* угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
* угрозы информационному обеспечению государственной политики Российской Федерации;
* 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;
* угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

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

Угрозами 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 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 телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на 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;
* разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно – телекоммуникационных систем, в том числе систем защиты информации;
* 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;
* 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 линиях связи, дешифрование этой информации и навязывание ложной информации;
* использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
* несанкционированный доступ к информации, находящейся в банках и базах данных;
* нарушение законных ограничений на распространение информации.

Все известные на настоящий момент меры защиты информации можно разделить на следующие виды:

* правовые;
* организационные;
* технические.

В большинстве работ правовые меры защиты информации принято рассматривать в рамках организационно-правового обеспечения защиты информации. Объединение организационных и правовых мер вызвано отчасти объективно сложившимися обстоятельствами:

* проблемы законодательного регулирования защиты информации регламентировались ограниченным и явно недостаточным количеством нормативно-правовых актов;
* в отсутствии законодательства по вопросам защиты информации разрабатывалось большое количество ведомственных нормативных документов, основное назначение которых заключалось в определении организационных требований по обеспечению защиты информации;
* внедрение автоматизированных информационных систем требует соответствующего правового обеспечения их защиты, однако, на практике в развитии правовой базы не произошло существенных изменений и приоритет остается за организационными мерами.

Организационно-правовое обеспечение защиты информации представляет совокупность законов и других нормативно-правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения защиты информации, так и организацию, и функционирование защиты конкретных объектов и систем. Правовые аспекты организационно-правового обеспечения защиты информации направлены на достижение следующих целей:

1. формирование правосознания граждан по обязательному соблюдению правил защиты конфиденциальной информации;
2. определение мер ответственности за нарушение правил защиты информации;
3. придание юридической силы технико-математическим решениям вопросов организационно-правового обеспечения защиты информации;
4. придание юридической силы процессуальным процедурам разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

В современной юриспруденции организационный и правовой подходы не объединяют. Однако, вопреки сложившимся традициям, не следует ограничиваться рассмотрением вопросов правовой защиты информации в рамках правовых аспектов комплексной защиты информации.

К правовым мерам следует отнести нормы законодательства, касающиеся вопросов обеспечения безопасности информации. Информационные отношения достигли такой ступени развития, на которой оказалось возможным сформировать самостоятельную отрасль законодательства, регулирующую информационные отношения. В эту отрасль, которая целиком посвящена вопросам информационного законодательства, включаются:

* законодательство об интеллектуальной собственности;
* законодательство о средствах массовой информации;
* законодательство о формировании информационных ресурсов и предоставлении информации из них;
* законодательство о реализации права на поиск, получение и использование информации;
* законодательство о создании и применении информационных технологий и средств их обеспечения.

В отрасли права, акты которых включают информационно-правовые нормы, входят конституционное право, административное право, гражданское право, уголовное право, предпринимательское право.

В соответствии с действующим законодательством информационные правоотношения – это отношения, возникающие при:

* формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
* создании и использовании информационных технологий и средств их обеспечения;
* защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

В соответствии с определением, изложенным в Законе Российской Федерации «О государственной тайне», к средствам защиты информации относятся «технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты, информации».

Все средства защиты можно разделить на две группы – формальные и неформальные. К формальным относятся такие средства, которые выполняют свои функции по защите информации формально, то есть преимущественно без участия человека. К неформальным относятся средства, основу которых составляет целенаправленная деятельность людей. Формальные средства делятся на технические (физические, аппаратные) и программные.

Технические средства защиты – это средства, в которых основная защитная функция реализуется некоторым техническим устройством (комплексом, системой).

К несомненным достоинствам технических средств относятся широкий круг задач, достаточно высокая надежность, возможность создания развитых комплексных систем защиты, гибкое реагирование на попытки несанкционированных действий, традиционность используемых методов осуществления защитных функций.

Основными недостатками являются высокая стоимость многих средств, необходимость регулярного проведения регламентированных работ и контроля, возможность подачи ложных тревог.

Системную классификацию технических средств защиты удобно провести по следующей совокупности показателей:

1) функциональное назначение, то есть основные задачи защиты объекта, которые могут быть решены с их применением;

2) сопряженность средств защиты с другими средствами объекта обработки информации (ООИ);

3) сложность средства защиты и практического его использования;

4) тип средства защиты, указывающий на принципы работы их элементов;

5) стоимость приобретения, установки и эксплуатации.

В зависимости от цели и места применения, выполняемых функций и физической реализуемости технические средства можно условно разделить на физические и аппаратные:

Физические средства – механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

* внешняя защита – защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств объекта (физическая изоляция сооружений, в которых устанавливается аппаратура автоматизированной системы, от других сооружений);
* внутренняя защита – защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации (ограждение территории вычислительных центров заборами на таких расстояниях, которые достаточны для исключения эффективной регистрации электромагнитных излучений, и организации систематического контроля этих территорий);
* опознавание – специфическая группа средств, предназначенная для опознавания людей и идентификации технических средств по различным индивидуальным характеристикам (организация контрольно-пропускных пунктов у входов в помещения вычислительных центров или оборудованных входных дверей специальными замками, позволяющими регулировать доступ в помещения).

Аппаратные средства – различные электронные, электронно-механические и тому подобные устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач по защите информации. Например, для защиты от утечки по техническим каналам используются генераторы шума.

* нейтрализация технических каналов утечки информации (ТКУИ) выполняет функцию защиты информации от ее утечки по техническим каналам;
* поиск закладных устройств – защита от использования злоумышленником закладных устройств съема информации;
* маскировка сигнала, содержащего конфиденциальную информацию, – защита информации от обнаружения ее носителей (стенографические методы) и защита содержания информации от раскрытия (криптографические методы).

Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (криптографические методы).

Программные средства – специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решения задач по защите информации. Это могут быть различные программы по криптографическому преобразованию данных, контролю доступа, защите от вирусов и др. Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т.п. По функциональному назначению их можно разделить на следующие группы:

* идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей,
* определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей,
* контроль работы технических средств и пользователей,
* регистрация работы технических средств и пользователей при обработке информации ограниченного использования,
* уничтожения информации в ЗУ после использования,
* сигнализации при несанкционированных действиях,
* вспомогательные программы различного назначения: контроля работы механизма защиты, проставления грифа секретности на выдаваемых документах.

Неформальные средства делятся на организационные, законодательные и морально-этические.

Организационные средства – специально предусматриваемые в технологии функционирования объекта организационно-технические мероприятия для решения задач по защите информации, осуществляемые в виде целенаправленной деятельности людей.

Организационные мероприятия играют большую роль в создании надежного механизма защиты информации. Причины, по которым организационные мероприятия играют повышенную роль в механизме защиты, заключается в том, что возможности несанкционированного использования информации в значительной мере обуславливаются нетехническими аспектами: злоумышленными действиями, нерадивостью или небрежностью пользователей или персонала систем обработки данных. Влияние этих аспектов практически невозможно избежать или локализовать с помощью выше рассмотренных аппаратных и программных средств и физических мер защиты. Для этого необходима совокупность организационных, организационно-технических и организационно-правовых мероприятий, которая исключала бы возможность возникновения опасности утечки информации подобным образом.

Основными мероприятиями являются следующие:

### *Обязательные*

* Мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров.
* Мероприятия, осуществляемые при подборе и подготовки персонала вычислительного центра (проверка принимаемых на работу, создание условий, при которых персонал не хотел бы лишиться работы, ознакомление с мерами ответственности за нарушение правил защиты).
* Организация надежного пропускного режима.
* Контроль внесения изменений в математическое и программное обеспечение.
* Ознакомление всех сотрудников с принципами защиты информации и принципами работы средств хранения и обработки информации. Представляя себе хотя бы на качественном уровне, что происходит при тех или иных операциях, сотрудник избежит явных ошибок.
* Чёткая классификация всей информации по степени её закрытости и введение правил обращения с документами ограниченного распространения.
* Обязать сотрудников исполнять требования по защите информации, подкрепив это соответствующими организационными и дисциплинарными мерами.

### *Желательные*

* Заставить всех сотрудников изучить современные средства защиты информации и сдать по ним зачёт.
* Иметь в штате специалиста, профессионально разбирающегося в проблемах защиты информации.
* Не использовать в работе программное обеспечение, в отношении которого не имеется чёткой уверенности, что оно не совершает несанкционированных действий с обрабатываемой информацией, таких, например, как самовольное создание копий, сбор информации о компьютере, отсылка по Интернету сведений изготовителю программного обеспечения. Особенно подобным поведением «грешат» программные продукты фирмы «Microsoft».
* Поставив себя на место вероятного противника (конкурента), подумать, что он мог бы предпринять для получения несанкционированного доступа к вашей информации. Продумать ответные меры защиты.
* Приобрести сертифицированные средства защиты информации.
* Запретить сотрудникам (кроме уполномоченных специалистов) инсталлировать какое-либо новое программное обеспечение. При получении любых исполняемых файлов по электронной почте стирать их, не разбираясь.

### *Дополнительные*

* + Разработать комплексную стратегию защиты информации на вашем предприятии. Лучше поручить такую задачу сторонним специалистам.
  + Провести «испытание» имеющихся у вас средств защиты информации, поручив стороннему специалисту испробовать на прочность вашу защиту.

Одно из важнейших организационных мероприятий – содержание в вычислительном центре специальной штатной службы защиты информации, численность и состав которой обеспечивали бы создание надежной системы защиты и регулярное ее функционирование.

Законодательные средства – существующие в стране или специально издаваемые нормативно-правовые акты, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.

Морально-этические нормы – сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

Морально-этические способы защиты информации можно отнести к группе тех методов, которые, исходя, исходя из расхожего выражения, что «тайну хранят не замки, а люди», играют очень важную роль в защите информации. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам накапливающий в своей памяти колоссальные объемы информации, в том числе секретной, нередко становится источником утечки этой информации, или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные способы защиты информации предполагают, прежде всего, воспитание сотрудника, допущенного к секретам, то есть проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение сотрудника, осведомленного о сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Основными организационными и техническими методами, используемыми в защите государственной тайны, являются: скрытие, ранжирование, дробление, учет, дезинформация, морально-нравственные меры, кодирование и шифрование.

*Скрытие* как метод защиты информации является в основе своей реализации на практике одним из основных организационных принципов защиты информации – максимального ограничения числа лиц, допускаемых к секретам. Реализация этого метода достигается обычно путем:

* засекречивания информации, т.е. отнесения ее к секретной или конфиденциальной информации различной степени секретности и ограничения в связи с этим доступа к этой информации в зависимости от ее важности для собственника, что проявляется в проставляемом на носителе этой информации грифе секретности;
* устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

Скрытие – один из наиболее общих и широко применяемых методов защиты информации.

*Ранжирование* как метод защиты информации включает, во-первых, деление засекречиваемой информации по степени секретности и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться но тематическому признаку или по признаку секретности информации и определяется матрицей доступа.

Ранжирование как метод защиты информации является частным случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

*Дезинформация* – один из методов защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности.

Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты, и др.

*Дробление (расчленение)* информации на части с таким условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю технологию в целом.

Применяется достаточно широко при производстве средств: вооружения и военной техники, а также при производстве товаров народного потребления.

*Учет (аудит)* также является одним из важнейших методов защиты информации, обеспечивающих возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также данные о всех пользователях этой информации. Без учета решать проблемы было бы невозможно, особенно когда количество носителей превышает какой-то минимальный объем.

Принципы учета засекреченной информации:

* обязательность регистрации всех носителей защищаемой информации;
* однократность регистрации конкретного носителя такой информации;
* указание в учетах адреса, где находится в данное время данный носитель засекреченной информации;
* единоличная ответственность за сохранность каждого носителя защищаемой информации и отражение в учетах пользователя данной информации в настоящее время, а также всех предыдущих пользователей данной информации.

*Кодирование* – метод защиты информации, преследующий цель скрыть от нарушителя содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть угроза, что оно может попасть в чужие руки, а также при обработке и хранении информации в средствах вычислительной техники (СВТ).

Для кодирования используются обычно совокупность знаков (символов, цифр и др.) и система определенных правил, при помощи которых информация может быть преобразована (закодирована) таким образом, что прочесть ее можно будет, только если пользователь располагает соответствующим ключом (кодом) для ее раскодирования. Кодирование информации может производиться с использованием технических средств или вручную.

*Шифрование* – метод защиты информации, используемый чаще при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений. Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра.

Шифрование может быть предварительное (шифруется текст документа) и линейное (шифруется разговор). Для шифрования информации может использоваться специальная аппаратура.

Знание возможностей приведенных методов позволяет активно и комплексно применять их при рассмотрении и использовании правовых, организационных и инженерно-технических мер защиты секретной информации.

## 

## Объекты защиты информации

В соответствии с законами Российской Федерации защите подлежит информация, отнесенная к государственной тайне, конфиденциальная информация, в том числе персональные данные, неправомерное обращение с которыми может нанести ущерб ее собственнику, владельцу, пользователю или другому лицу. Законодательно определены и режимы защиты такой информации.

Собственниками, владельцами, пользователями (потребителя) информации могут быть государственные и негосударственные предприятия, организации, физические лица.

Основные объекты защиты можно объединить в следующие группы:

* собственники, владельцы, пользователи (потребители) информации;
* информационные ресурсы с ограниченным доступом, составляющие коммерческую, банковскую тайну, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления;
* процессы обработки информации в автоматических системах – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический персонал разработчиков и пользователей системы и ее обслуживающий персонал;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты автоматической системы;

Очень часто путают саму информацию и её носитель. Такая путаница приводит к непониманию сути проблемы и, следовательно, к невозможности её решить. Поэтому следует чётко представлять себе, где информация, а где её материальный носитель.

Информация – вещь нематериальная. Это сведения, которые зафиксированы (записаны) тем или иным расположением (состоянием) материального носителя, например, порядком расположения букв на странице или величиной намагниченности ленты.

Носителем информации может быть любой материальный объект. И наоборот – любой материальный объект всегда несёт на себе некую информацию (которая, однако, далеко не всегда имеет для нас значение). Например, книга как совокупность переплёта, бумажных листов, и типографской краски на них является типичным носителем информации.

Чтобы отличать информацию от её носителя, надо твёрдо помнить, что информация – это сугубо нематериальная субстанция. Всё, что является материальным объектом, информацией быть не может, но только лишь её носителем. В том же примере с книгой и листы, и знаки на них – только носитель; информация же заключена в порядке расположения печатных символов на листах. Радиосигнал – тоже материальный объект, поскольку является комбинацией электрических и магнитных полей (с другой точки зрения – фотонов), поэтому он не является информацией. Информация в данном случае – порядок чередования импульсов или иных модуляций указанного радиосигнала.

Материя и информация неотделимы друг от друга. Информация не может существовать сама по себе, в отрыве от материального носителя. Материя же не может не нести информации, поскольку всегда находится в том или ином определённом состоянии.

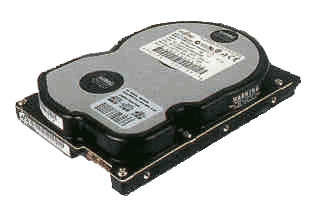
Теперь перейдём к более конкретному рассмотрению. Хотя любой материальный объект – носитель информации, но люди используют в качестве таковых специальные объекты, с которых информацию удобнее считывать.

Традиционно используемым носителем информации является бумага с нанесёнными на ней тем или иным способом изображениями.

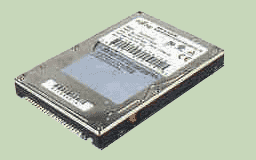
Поскольку в наше время основным средством обработки информации является компьютер, то и для хранения информации используются в основном машинно-читаемые носители.

В группе носителей и технических средств передачи и обработки информации защите подлежат:

* Собственно носители информации в виде информационных физических полей и химических сред, сигналов, документов на бумажной, магнитной, оптической и других основах:
* Жёсткий магнитный диск, ЖМД, НЖМД (hard disk, HD). Применяется как основной стационарный носитель информации в компьютерах. Большая ёмкость, высокая скорость доступа. Иногда встречаются модели со съёмным диском, который можно вынуть из компьютера и спрятать с сейф. [Так выглядит НЖМД.](http://www.college.ru/UDP/texts/hd.html)



*HDD габаритом 5,25 дюйма*



*HDD габаритом 3,5 дюйма*

* Гибкий магнитный диск, ГМД (floppy disk, FD) или дискета (diskette). Основной сменный носитель для персональных компьютеров. Небольшая ёмкость, низкая скорость доступа, но и стоимость тоже низкая. Основное преимущество – транспортабельность.
* Лазерный компакт-диск (CD, CD-ROM). Большая ёмкость, средняя скорость доступа, но отсутствует возможность записи информации. Запись производится на специальном оборудовании. [Так выглядит CD‑привод.](http://www.college.ru/UDP/texts/cd.html)



*Внешний*



*Внутренний*

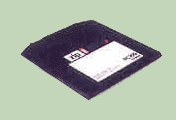


*Привод компакт-дисков обязательно помечен значком*

* Перезаписываемый лазерный компакт-диск (CD-R, CD-RW). В одних случаях возможна только запись (без перезаписи), в других – также ограниченное число циклов перезаписи данных. Те же характеристики, что и для обычного компакт-диска.
* DVD‑диск. Аналогичен CD-ROM, но имеет более высокую плотность записи (в 5–20 раз). Имеются устройства как только для считывания, так и для записи (перезаписи) DVD.
* Сменный магнитный диск типа ZIP или JAZZ. Похож на дискету, но обладает значительно большей ёмкостью. [Так выглядит ZIP‑диск и привод для него.](http://www.college.ru/UDP/texts/zip.html)

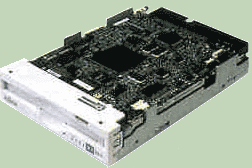


*Накопитель ZIP (внешний)*

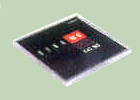


*Сменный ZIP‑диск*

* Магнитооптический или т.н. флоптический диск. Сменный носитель большой ёмкости. [Так выглядит магнитооптический диск и привод для него.](http://www.college.ru/UDP/texts/mo.html)



*Магнитооптический накопитель (внутренний)*



*Магнитооптический диск*

* Кассета с магнитной лентой – сменный носитель для стримера (streamer) – прибора, специально предназначенного для хранения больших объёмов данных. Некоторые модели компьютеров приспособлены для записи информации на обычные магнитофонные кассеты. Кассета имеет большую ёмкость и высокую скорость записи-считывания, но медленный доступ к произвольной точке ленты. [Так выглядит стример и его кассеты.](http://www.college.ru/UDP/texts/streamer.html)



*Стримеры*



*Внешний стример*



*Внутренний стример*

## Кассеты для стримера



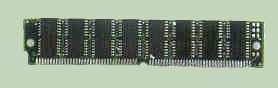
*Кассета для стримера*



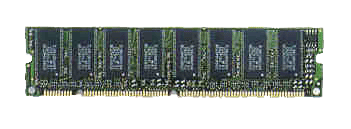
*Чистящая кассета для стримера*

* Перфокарты – в настоящее время почти не используются.
* Перфолента – в настоящее время почти не используется.
* Кассеты и микросхемы ПЗУ (read-only memory, ROM). Характеризуются невозможностью или сложностью перезаписи, небольшой ёмкостью, относительно высокой скоростью доступа, а также большой устойчивостью к внешним воздействиям. Обычно применяются в компьютерах и других электронных устройствах специализированного назначения, таких как игровые приставки, управляющие модули различных приборов, принтеры и т.д.
* Магнитные карты (полоски). Маленькая ёмкость, транспортабельность, возможность сочетания машинно-читаемой и обычной текстовой информации. Кредитные карточки, пропуска, удостоверения и т.п.
* Существует большое количество специализированных носителей, применяемых в различных малораспространённых приборах. Например, магнитная проволока, голограмма.

Кроме того, носителем информации является оперативная память компьютера, ОЗУ (RAM), но она не пригодна для долговременного хранения информации, поскольку данные в ней не сохраняются при отключении питания. [Так выглядят модули оперативной памяти.](http://www.college.ru/UDP/texts/ram.html)



*Модуль памяти SIMM   
(standart inline memory module)*



*Модуль памяти DIMM*

* Средства электронно-вычислительной техники (ЭВТ).
* Средства связи (ТЛФ, ТЛГ, ГГС, телефаксы, телетайпы).
* Средства преобразования речевой информации (средства звукозаписи, звукоусиления, звуковоспроизведения, звукового сопровождения).
* Средства визуального отображения (дисплеи, средства внутреннего телевидения).
* Средства изготовления и размножения документов (принтеры, ксероксы, плоттеры и т.д.).
* Вспомогательные технические средства (средства, не обрабатывающие защищаемую информацию, но размещенные в помещениях, где она обрабатывается).
* Помещения, выделенные для размещения объектов защиты.
* Для объектов органов управления, военных и промышленных объектов защите подлежит информация:
* о местоположении объекта;
* о предназначении, профиле деятельности, структуре объекта и режиме его функционирования;
* циркулирующая в технических средствах, используемых на объекте;
* о разрабатываемых (производимых, испытываемых) или эксплуатируемых образцах вооружения, военной техники или производствах и технологиях;
* о научно-исследовательских и опытно-конструкторских работах.

Сопоставление методов защиты информации и объектов защиты

Хорошая защита информации обходится дорого. Плохая же защита никому не нужна, ибо наличие в ней лишь одной «дырки» означает полную бесполезность всей защиты в целом (принцип сплошной защиты). Поэтому прежде чем решать вопрос о защите информации, следует определить, стоит ли она того. Способен ли возможный ущерб от разглашения или потери информации превысить затраты на её защиту? С этой же целью надо максимально сузить круг защищаемой информации, чтобы не тратить лишних средств и времени.

Прежде чем защищать информацию, нелишне определить перечень вероятных угроз, поскольку от всего на свете вы всё равно не защититесь. Возможен вариант, когда вам надо обезопасить данные от несанкционированного доступа извне, например, из Интернета. Возможно, однако, что чужих хакеров ваши данные вовсе не интересуют, и вам следует защищать информацию только от собственных сотрудников. Возможно также, что похищение или разглашение вашей информации никому не навредит, но вот её подмена может нанести вам урон. Во всех трёх случаях методы защиты будут сильно различаться.

При планировании схемы защиты информации большое значение имеет не только её объективная надёжность, но и отношение к защите других людей. В некоторых случаях достаточно, чтобы вы сами были уверены в достаточной надёжности защиты. А в других – это нужно доказать иным людям (например, заказчикам), часто не разбирающимся в соответствующих вопросах. Здесь встаёт вопрос сертификации.

Абсолютно надёжной защиты не существует. Это следует помнить всем, кто организует защиту информации. Любую защиту можно преодолеть. Но лишь «в принципе». Это может потребовать таких затрат сил, средств или времени, что добытая информация их не окупит. Поэтому практически надёжной признаётся такая защита, преодоление которой потребует от противника затрат, значительно превышающих ценность информации.

Важно различать два вида защиты информации – защита объектов и защита непосредственно информации, безотносительно к тому, где она находится.

Первый вид включает несколько методов защиты объектов информации (здесь мы будем рассматривать только компьютерные носители), их можно подразделить на программные, аппаратные и комбинированные. Метод же защиты самой информации только один – использование криптографии, то есть, шифровка данных.

Наиболее распространённые методы защиты объектов:

* Для всех сменных носителей – физическая их защита, например, запереть в сейф.
* Для всех встроенных в компьютер носителей – воспрепятствование включению питания компьютера. Конечно, этот метод действенен для ограниченного числа случаев.
* Программное воспрепятствование доступу к конкретному носителю или к компьютеру целиков. Например, пароль на CMOS.
* Программно-аппаратный метод с использованием электронных ключей, которые чаще всего вставляются в COM‑порт ПК. Не получая нужный ответ от ключа, программа, для которой он предназначен, не будет работать или давать пользователю доступ к своим данным.
* Специально оборудованное (в идеале – специально построенное) помещение для размещения автоматических систем и организационных структур.
* Организация пропускного контроля в помещения, в которых размещены автоматические системы.

Наиболее простой и надежный способ защиты информации от несанкционированного доступа (НСД) – режим автономного использования ЭВМ одним пользователем, работающим в отдельном помещении при отсутствии посторонних лиц. В этом случае роль замкнутого контура защиты выполняют помещение, его стены, потолок, пол и окна. Если стены, потолок, пол и дверь достаточно прочны, пол не имеет люков, сообщающихся с другими помещениями, окна и дверь оборудованы охранной сигнализацией, то прочность защиты будет определяться техническими характеристиками охранной сигнализации при отсутствии пользователя (ЭВМ не включена) в нерабочее время.

В рабочее время, когда ЭВМ включена, возможна утечка информации за счет ее побочного электромагнитного излучения и наводок. Для устранения такой опасности, если это необходимо, проводятся соответствующие технические мероприятия по уменьшению или зашумлению сигнала. Кроме того, дверь помещения для исключения доступа посторонних лиц должна быть оборудована механическим или электромеханическим замком. В некоторых случаях, когда в помещении нет охранной сигнализации, на период длительного отсутствия пользователя ЭВМ полезно помещать в сейф, по крайней мере, хотя бы ее системный блок и носители информации. Применение в некоторых ЭВМ в системе ввода-вывода BIOS встроенного аппаратного пароля, блокирующего загрузку и работу ЭВМ, к сожалению, не спасает положения, так как данная аппаратная часть при отсутствии на корпусе системного блока замка и отсутствии хозяина может быть свободно заменена на другую – такую же (так как узлы унифицированы), но только с известным значением пароля. Обычный механический замок, блокирующий включение и загрузку ЭВМ, более эффективная в этом случае мера.

В последнее время для защиты от хищения специалисты рекомендуют механически закреплять ЭВМ к столу пользователя. Однако при этом следует помнить, что при отсутствии охранной сигнализации, обеспечивающей постоянный контроль доступа в помещение или к сейфу прочность замков и креплений должна быть такова, чтобы ожидаемое суммарное время, необходимое нарушителю для преодоления такого рода препятствий или обхода их, превышало время отсутствия пользователя ЭВМ. Если это сделать не удается, то охранная сигнализация обязательна. Тем самым будет соблюдаться основной принцип срабатывания защиты и следовательно, будут выполняться требования по ее эффективности.

Перечисленные выше меры защиты информации ограниченного доступа от нарушителя-непрофессионала в принципе можно считать достаточными при работе с автономной ЭВМ одного пользователя. На практике же человек не может постоянно быть изолированным от общества, в том числе и на работе. Его посещают друзья, знакомые, сослуживцы обращаются по тем или иным вопросам. Отдельное помещение для его работы не всегда может быть предоставлено. По рассеянности или озабоченный личными проблемами пользователь может компьютер включить, а ключ оставить в замке; на столе забыть дискету, а сам на короткое время покинуть помещение, что создает предпосылки для несанкционированного доступа к информации лиц, не допущенных к ней, но имеющих доступ в помещение. Распространенные в настоящее время развлекательные программы могут послужить средством для занесения программных вирусов в ЭВМ. Использование посторонних дискет для оказания дружеской услуги может обойтись очень дорого. Помимо заражения ЭВМ вирусом можно перепутать дискеты и отдать случайно другу дискету с секретной информацией.

Все перечисленные средства и им подобные должны с различной степенью безопасности обеспечивать только санкционированный доступ к информации и программам со стороны клавиатуры, средств загрузки и внутреннего монтажа компьютера. Возможные каналы НСД к информации ЭВМ и средства защиты, рекомендуемые для их перекрытия приведены в Приложении.

Защита от НСД со стороны клавиатуры усложняется тем, что современные компьютеры по своему назначению обладают широким спектром функциональных возможностей, которые с течением времени продолжают развиваться. Более того, иногда кажется, что требования по защите вступают в противоречие с основной задачей компьютера: с одной стороны, ЭВМ – серийное устройство массового применения, с другой – индивидуального.

Если в каждый из выпускаемых персональных компьютеров, например, установить на заводе-изготовителе электронный замок, открываемый перед началом работы пользователем с помощью ключа-пароля, то возникает вопрос защиты хранения и последующей замены его ответной части в замке. Если ее может заменить пользователь, то это может сделать и нарушитель. Если эта часть компьютера постоянна, то она известна изготовителям, через которых может стать известной и нарушителю. Однако последний вариант более предпочтителен при условии сохранения тайны ключа фирмой-изготовителем, а также высокой стойкости ключа к подделке и расшифровке. Стойкость ключа должна быть известна и выражаться в величине затрат времени нарушителя на выполнение этой работы, так как по истечении этого времени необходима замена его на новый, если защищаемый компьютер продолжает использоваться. Но и этого условия тоже оказывается недостаточно. Необходимо также, чтобы ответная часть ключа – замок тоже не был доступен потенциальному нарушителю. Стойкость замка к замене и подделке должна быть выше стойкости ключа и равняться времени эксплуатации компьютера при обязательном условии невозможности его съема и замены нарушителем. В роли «замка» могут выступать специальные программные фрагменты, вкладываемые пользователем ЭВМ в свои программы и взаимодействующие по известному только пользователю алгоритму с электронным ключом. Анализ потенциальных угроз безопасности информации и возможных каналов НСД к ней в ЭВМ показывает их принципиальное сходство с аналогичными угрозами и каналами. Следовательно, методы защиты должны быть такими же, а технические средства защиты должны строиться с учетом их сопряжения с ее аппаратными и программными средствами. В целях перекрытия возможных каналов НСД к информации ЭВМ, кроме упомянутых, могут быть применены и другие методы и средства защиты.

При использовании ЭВМ в многопользовательском режиме необходимо применить в ней программу контроля и разграничения доступа. Существует много подобных программ, которые часто разрабатывают сами пользователи. Однако специфика работы программного обеспечения ЭВМ такова что с помощью ее клавиатуры достаточно квалифицированный программист-нарушитель может защиту такого рода легко обойти. Поэтому эта мера эффективна только для защиты от неквалифицированного нарушителя. Для защиты от нарушителя-профессионала поможет комплекс программно-аппаратных средств. Например, специальный электронный ключ, вставляемый в свободный слот ПК, и специальные программные фрагменты, закладываемые в прикладные программы ПК, которые взаимодействуют с электронным ключом по известному только пользователю алгоритму. При отсутствии ключа эти программы не работают. Однако такой ключ неудобен в обращении, так как каждый раз приходится вскрывать системный блок ПК. В связи с этим его переменную часть – пароль – выводят на отдельное устройство, которое и становится собственно ключом, а считывающее устройство устанавливается на лицевую панель системного блока или выполняется в виде выносного отдельного устройства. Таким способом можно заблокировать и загрузку ПК, и программу контроля и разграничения доступа.

Определенную проблему представляет собой защита от НСД остатков информации, которые могут прочитать при наложении на старую запись новой информации на одном и том же носителе, а также при отказах аппаратуры.

Отходы носителей скапливаются в мусорной корзине. Поэтому во избежание утечки информации должны быть предусмотрены средства механического уничтожения отработанных носителей с остатками информации.

Отдельную проблему в защите ПО и информации составляет проблема защиты от программных вирусов.

Если ЭВМ работает в автономном режиме, проникновение вируса возможно только со стороны внешних носителей ПО и информации. Если ЭВМ является элементом вычислительной сети (или АСУ), то проникновение вируса возможно также и со стороны каналов связи. Поскольку этот вопрос представляет отдельную проблему, он рассмотрен ниже в специальном разделе.

Еще один уровень защиты от неквалифицированного нарушителя может быть обеспечен путем использования*компрессии данных****.*** Этот метод выгоден тем, что:

• экономит пространство при хранении файлов на диске;

• уменьшает время шифрации-дешифрации;

• затрудняет незаконное расшифрование файла;

• уменьшает время передачи в процессе передачи данных.

Хотя этот метод дает относительно низкий уровень безопасности, его рекомендуется применять перед шифрацией.

Программные средства, работающие с дисками на физическом уровне, предоставляют в некоторых случаях возможность обхода программных средств защиты.

Кроме того, существуют программы, позволяющие создавать ПО, способное производить чтение или запись по абсолютным адресам, а также программ, обеспечивающих просмотр и отладку программных продуктов в режиме дисассемблера, просмотр и редактирование оперативной памяти ЭВМ.

Однако наличие таких программных средств служит для других целей – для восстановления испорченной вирусами или неосторожными действиями пользователей информации. Следовательно, их применение должно быть строго регламентировано и доступно только администратору системы. В последнее время появились методы защиты от анализа программ.

Для создания замкнутой оболочки защиты информации в ЭВМ и объединения перечисленных средств в одну систему необходимы соответствующие средств управления и контроля. В зависимости от режима использования ЭВМ – автономного или сетевого (в составе сети – локальной, региональной или глобальной) – они будут носить различный характер.

В автономном режиме могут быть два варианта управления: однопользовательский и многопользовательский. В первом случае пользователь сам выполняет функции управления и контроля и несет ответственность за безопасность своей и доверяемой ему информации.

В многопользовательском режиме перечисленные функции рекомендуется поручить специальному должностному лицу. Им может быть один из пользователей или руководитель работ. При этом, однако, ключи шифрования и информация, закрытая ими другим пользователем, ему могут быть недоступны до момента передачи руководителю работ.

Следует отметить, что в автономном режиме функции контроля ослаблены из-за отсутствия механизма быстрого обнаружения НСД, так как это приходится осуществлять организационными мерами по инициативе человека. Следовательно, многопользовательский режим нежелателен с позиций безопасности и не рекомендуется для обработки важной информации.

В сетевом варианте можно автоматизировать процесс контроля и все перечисленные функции выполнять со специального рабочего места службы безопасности.

В сетевом варианте должностное лицо – пользователь может передавать сообщения и документы другому пользователю по каналам связи, и тогда возникает необходимость выполнять, в интересах безопасности передаваемой информации, дополнительные функции по обеспечению абонентского шифрования и цифровой подписи сообщений.

## Заключение

В последнее столетие появилось много таких отраслей производства, которые почти на 100% состоят из одной информации, например, дизайн, создание программного обеспечения, реклама и другие.

Столь же ярко демонстрирует повышение роли информации в производственных процессах появление в XX веке такого занятия, как промышленный шпионаж. Не материальные ценности, а чистая информация становится объектом похищения.

В прошлые века человек использовал орудия труда и машины для обработки материальных объектов, а информацию о процессе производства держал в голове. В XX столетии появились машины для обработки информации – компьютеры, роль которых все повышается.

С повышением значимости и ценности информации соответственно растёт и важность её защиты.

С одной стороны, информация стоит денег. Значит, утечка или утрата информации повлечёт материальный ущерб. С другой стороны, информация – это управление. Несанкционированное вмешательство в управление может привести к катастрофическим последствиям в объекте управления – производстве, транспорте, военном деле. Например, современная военная наука утверждает, что полное лишение средств связи сводит боеспособность армии до нуля.

Поэтому прежде чем защищать ту или иную информацию, следует подумать, а имеет ли это смысл. Прежде всего – с экономической точки зрения.

При построении защиты нужно руководствоваться следующим принципом. На защиту информации можно потратить средств не свыше необходимого. Необходимый же уровень определяется тем, чтобы затраты вероятного противника на преодоление защиты были выше ценности этой информации с точки зрения этого противника.

Основные выводы о способах использования рассмотренных выше средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.

2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.

3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.

4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

Цель курсовой работы достигнута.

## Приложение

Возможные каналы несанкционированного доступа к информации ЭВМ и средства защиты, рекомендуемые для их перекрытия

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Возможные каналы НСД** | **Средства защиты** |
|  | Дисплей, принтер, плоттер, графопостроитель | Отдельное помещение с контролируемым доступом |
|  | Клавиатура, сканер, манипулятор «мышь» | То же  Специальный электронный ключ в сочетании с фрагментами ПО  Программа контроля и разграничения доступа (пароли)  Средства защиты от отладочных программ  Блокировка механическим замком включения электропитания  Блокировка механическим замком механизма загрузки ПО  Средства контроля целостности ПО |
|  | Дисковод | Отдельное помещение с контролируемым доступом  Применение ЭВМ без дисковода  Установка механической крышки с механическим замком  Средства защиты от вирусов  Средства верификации НГМД  Средства защиты от несанкционированной загрузки ПО  Средства контроля целостности ПО |
|  | ГМД, Стриммер | Отдельное помещение с контролируемым доступом  Учет и регистрация  Маркировка цветом  Хранение в сейфах  Стирание остатков информации  Уничтожение остатков информации  Компрессия данных  Шифрование данных |
|  | ЖМД | Отдельное помещение с контролируемым доступом  Металлический шкаф с замком  Блокировка снятия кожуха системного блока механическим замком  Средства контроля целостности ПО  Стирание остаточной информации  Уничтожение остаточной информации  Шифрование данных |
|  | Внутренний монтаж | Отдельное помещение с контролируемым доступом  Блокировка снятия кожуха системного блока механическим замком |
|  | ПЭМИН | Средства уменьшения и зашумления сигналов и установление границ контролируемой зоны |
|  | Отходы носителей с информацией | Отдельное помещение с контролируемым доступом  Средства уничтожения отходов носителей |
|  | Документы | Отдельное помещение с контролируемым доступом  Учет и регистрация документов  Сейф |

## Использованные источники

1. СПС «КонсультантПлюс». Федеральный закон «Об информации, информатизации и защите информации».
2. СПС «КонсультантПлюс». Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.В. Путиным и принята Советом безопасности Российской Федерации 12 сентября 2000 г.).
3. СПС «КонсультантПлюс». Федеральный закон «О государственной тайне».
4. Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров и др. Технические методы и средства защиты информации. – СПб.: ООО «Издательство Полигон», 2000. – 320 с.
5. Дж. Макнамара. Секреты компьютерного шпионажа: Тактика и контрмеры. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.

Веб-документы:

1. Федотов Н.Н. Защита информации. Учебный курс (HTML‑версия). <http://www.college.ru/UDP/texts/> (22 мая 2007 г.).
2. Crion (автор)**.** Как самому написать концепцию информационной безопасности. <http://linuxportal.ru/entry.php/P2734_0_3_0/> (22 мая 2007 г.).
3. Vlad (автор). Средства защиты данных (Дата поступления 23.11.2006). http://referats.protoplex.ru/referats\_show/3902.html (29 мая 2007 г.).