Система обеспечения информационной безопасности предприятия

1. Правовые основы информационной безопасности

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами. К их числу в первую очередь относятся:

1. Конституция РФ.
2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646) Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности страны.
3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (в ред. от 19.07.2018 г.) Закон регулирует 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.

4. Федеральный Закон РФ от 7 июля 2003 г. № 126-ФЗ «О связи» (в ред. от 03 августа 2018 г.). Закон устанавливает правовые основы деятельности в области связи на территории РФ и на находящихся под юрисдикцией РФ территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

5. Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» (в ред, от 29.07.2018 г.). Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечении безопасности РФ.

6. Гражданский кодекс РФ (часть 4) от 18 декабря 2006 г. № 230-Ф 1 (в ред. от 03.08.2018 г.): гл. 70 «Авторское право»; гл. 71 «Права, смежные с авторскими»; гл. 72 «Патентное право»; гл. 74 «Право на топологии интегральных микросхем»; гл. 75 «Право на секрет производства» (ноу-хау)»; гл. 76 «Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий»; гл. 77 «Право использования результатов интеллектуальной деятельности в составе единой технологии».

7. Федеральный Закон РФ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (в ред. от 18.04. 2018 г.).
8. Федеральный Закон РФ от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в РФ» (вред, от 28.12. 2018 г.).
9. Кодекс РФ от 30 декабря 2001 г. № 195-ФЗ «Об административных правонарушениях» (в ред. от 3.08. 2018 г.).
10. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (в ред. от 29.07.2018 г.)

ст. 128.1 «Клевета»; ст. 137 «Нарушение неприкосновенности частной жизни»; ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»; ст. 140 «Отказ в предоставлении гражданину информации»; ст. 146 «Нарушение авторских и смежных прав»; ст. 155 «Разглашение тайны усыновления (удочерения)»; ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»; ст. 185.1 «Злостное уклонение от раскрытия или предоставления информации, определенной законодательством РФ о ценных бумагах»; ст. 187 «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов»; ст. 189 «Незаконные экспорт или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники»; ст. 237 «Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей»;

ст. 242 «Незаконные изготовление и оборот порнографических материалов или предметов»; ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационных телеком муникационных систем»; ст. 276 «Шпионаж»; ст. 283 «Разглашение государственной тайны»; ст. 287 «Отказ в предоставлении информации Федеральному Собранию РФ или Счетной палате РФ»; ст. 310 «Раз глашение данных предварительного расследования»; ст. 311 «Разглаше ние сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса»; ст. 320 «Разглашение сведений О мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа».

11. Национальный стандарт РФ ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. Приказом Федерального агенства по техническому регулированию и метрологии от 18 декабря 2008 г. №532-ст)

12. Иные нормативные правовые акты и организационно-распорядительные документы.

13. Положения, инструкции, нормативно-технические и методические документы.

2. Назначение, принципы и структура системы защиты информации

Система обеспечения информационной безопасности (СЗИ) - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

СЗИ основана на следующих принципах :

1. Комплексность — обеспечение безопасности обслуживающего персонала, материальных и финансовых ресурсов от всех возможных угроз всеми доступными законными средствами, методами и мероприятиями; обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, во всех технологических процессах и операциях их создания, обработки, использования и уничтожения; способность системы защиты информации к развитию и совершенствованию и соответствии с изменяющимися внешними и внутренними условиями.

2. Своевременность — упреждающий характер мер защиты ин формации предполагает постановку задач по комплексной защите информации на стадии проектирования (создания) системы ее защиты на основе анализа известных и прогнозирования возможных угроз безопасности информации, которые могут появиться в будущем после запуска системы защиты в эксплуатацию (реализацию).

3. Непрерывность — постоянное поддержание работоспособности и развитие СЗИ.

4. Активность — настойчивость в достижении целей и задач защиты информации. Предполагает постоянный маневр силами и средствами защиты информации, а также принятие нестандартных мер защиты.

5. Законность — разработка СЗИ на основе действующего законодательства, а также иных нормативных актов, регламентирующих безопасность информации. Входе последующей реализации СЗИ — применение всех законных методов и средств обнаружения и пресечения правонарушений в области безопасности информации.

6. Обоснованность — заключается в том, что все методы и средства защиты информации должны быть научно обоснованными и современными, соответствовать последним достижениям науки и техники. В своей совокупности они должны отвечать всем установленным требованиям и нормам по защите информации.

7. Экономическая целесообразность — затраты на разработку и ре ализацию (обеспечение заданных параметров) СЗИ не должны пре вышать размеры потенциального ущерба, который может наступить в результате нарушения безопасности защищаемой информации.

8. Специализация — предполагает привлечение к разработке и вне дрению методов и средств защиты информации специализированных субъектов, имеющих государственную лицензию на определенный вид деятельности в сфере оказания услуг по защите информации. Применя емые ими средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

9. Взаимодействие и координация деятельности — предусматривает организацию четкого взаимодействия между всеми субъектами защиты информации, действующими в рамках единой СЗИ, а также координа цию их усилий и осуществляемых работ в этой сфере для достижения общих целей. Заключается в интеграции и последовательности деятель ности по защите конкретных информационных ресурсов.

10. Совершенствование — предусматривает совершенствование и разработку новых законодательных, организационных и технических мер защиты информации под воздействием объективных и субъективных факторов.

11. Централизация управления — предполагает наличие единого координационного центра (субъекта), занимающегося общими вопро сами управления СЗИ, а также единых требований по обеспечению безопасности информации.

Основными целями защиты информации являются:

- предотвращение утечки, хищения, утраты, искажения и подделки информации;
- локализация угроз безопасности личности, общества и государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, а также предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;
- обеспечение правового режима документированной информации как объекта собственности

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с действующим законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Задачи защиты информации:

- проведение единой политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;
- исключение или существенное затруднение добывания информации средствами разведки (промышленного шпионажа);
- предотвращение утечки информации по техническим каналам и несанкционированного доступа к ней;
- предупреждение вредоносных воздействий на информацию, ее носителей, а также технические средства ее создания, обработки, использования, передачи и защиты;

- принятие правовых актов, регулирующих общественные отношения в области защиты информации;
- анализ состояния и прогнозирование возможностей технических средств разведки, а также способов их применения;
- формирование системы информационного обмена сведениями об осведомленности иностранных разведок о силах, методах, средствах и мероприятиях, обеспечивающих защиту информации внутри страны и за ее пределами;
- организация сил, разработка научно обоснованных методов, создание средств защиты информации и контроля за ее эффективностью;
- контроль состояния защиты информации в органах государственной власти, учреждениях, организациях и на предприятиях всех форм собственности, использующих в своей деятельности охраняемую законом информацию.

На государственном уровне к субъектам СЗИ относятся:

- палаты Федерального Собрания — осуществляют законодательное регулирование отношений в сфере защиты информации; рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в этой области; определяют полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания;

своих полномочий решение иных вопросов, возникающих в связи с отнесением сведений к тому или иному виду тайны, их засекречиванием или рассекречиванием и их защитой;

- Президент Российской Федерации — анализ состояния и прогно зирование возможностей технических средств разведки, а также способов их применения; утверждение государственных программ в области защиты информации; утверждение по представлению правительства РФ состава, структуры межведомственной комиссии по защите государственной тайны и положения о ней; утверждение по представлению правительства РФ перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также перечня сведений, отнесенных к государственной тайне; заключение международных договоров России о совместном использовании и защите сведений, составляющих государственную тайну; определение полномочий должностных лиц по обеспечению защиты информации в своей Администрации; в пределах своих полномочий решение иных вопросов, возникающих в связи с отнесением сведений к тому или иному виду тайны, их засекречиванием или рассекречиванием и их защитой;

- Правительство РФ — организует исполнение законов и международных соглашений в области защиты информации; представляет на утверждение президенту состав и структуру межведомственной комиссии по защите государственной тайны, а также положение о ней; представляет на утверждение президенту перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к тому или иному виду тайны; организует разработку и выполнение государственных программ в области защиты информации; определяет полномочия должностных лиц по обеспечению защиты информации в аппарате правительства; устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны; устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания; заключает межправительственные соглашения, принимает меры по выполнению международных договоров России о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам; в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к тому или иному виду тайны, их засекречиванием или рассекречиванием и их защитой;

• органы государственной власти РФ, органы государственной власти субъектов РФ и органы МСУ во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий — обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями охраняемой законом информации, а также сведений, засекречиваемых ими; обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организация в соответствии с требованиями законодательства РФ; обеспечивают в пределах своей компетенции проведение проверочных мероприятии в отношении граждан, допускаемых к тайне; реализуют предусмотренные законодательством меры по ограничению конституционных прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну; внося в полномочные органы государственной власти предложения по совершенствованию системы защиты информации;

- органы судебной власти — рассматривают уголовные и гражданские дела о нарушениях законодательства в области защиты информации; обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите охраняемой законом информации; обеспечивают в входе рассмотрения указанных дел защиту отдельных видов тайны; определяют полномочия должностных лиц по обеспечению защиты охраняемой законом информации в органах судебной власти;

• органы защиты информации:

1 — Межведомственная комиссия по защите государственной тайны — это коллегиальный орган, координирующий работу по защите информации в РФ;

2 — органы федеральной исполнительной власти. К ним относятся: Федеральная служба безопасности, Министерство обороны, Министерство внутренних дел, Служба внешней разведки, Федеральная служба охраны, Государственная техническая комиссия при Президенте РФ (Гостехкомиссия[1]);

3 — органы государственной власти, предприятия, учреждения, организации и их структурные подразделения по защите охраняемой законом информации.

Работа по защите информации осуществляется по следующим на правлениям:

- подготовка и принятие законодательных и иных нормативных правовых актов в области защиты информации;
- обеспечение контроля за их исполнением;
- финансовое и кадровое обеспечение мероприятий по защите информации;
- обеспечение эффективного управления СЗИ;
- определение сведений, подлежащих охране, и демаскирующих признаков, раскрывающих эти сведения;
- анализ и оценка угроз безопасности охраняемой законом ин формации;
- разработка организационно-технических мероприятий по защите информации и их реализация;
- организация и проведение контроля состояния защиты инфор мации;
- анализ и оценка эффективности СЗИ, ее своевременная кор ректировка.

К числу основных организационно-технических мероприятий по защите информации относятся:

- лицензирование деятельности предприятий в области защиты информации;
- аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;
- сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;
- категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;
- обеспечение условий защиты информации при подготовке и ре ализации международных договоров и соглашений;

- оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват ин формации, подлежащей защите), расположенных на территории России;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использовании технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- разработка и внедрение технических решений и элементов за щиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;
- разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;
- применение специальных методов, технических мер и средств за щиты, исключающих перехват информации, передаваемой по каналам электросвязи.

Средства защиты информации подразделяются на физические; аппаратные; программные; криптографические.

Объектами защиты являются:

- лица, допущенные к работе с охраняемой законом информацией либо имеющие доступ в помещения, где эта информация обрабатывается.
- объекты информатизации — средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров;
- охраняемая законом информация — информация, доступ к которой ограничен в соответствии с законодательством России (конфиденциальная информация);
- материальные носители охраняемой законом информации;
- средства защиты информации;
- технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации.

Угрозы безопасности информации делятся на следующие виды:

1. Естественные угрозы:

- стихийные бедствия, природные явления (пожары, землетрясения, наводнения, ураганы, смерчи, тайфуны, циклоны и т. п.);
- самопроизвольное разрушение элементов, из которых состоит средство электронно-вычислительной техники, электросвязи и защиты

2. Искусственные угрозы (деятельность человека):

2.1. Умышленные (правонарушения):

- пассивный (бесконтактный) несанкционированный доступ к информации: а) визуальное наблюдение за объектами информатизации (невооруженным глазом; с помощью оптических и оптико-электронных приборов и устройств); б) перехват речевой информации (с помощью остро направленных микрофонов, электронных стетоскопов, лазерного луча, устройств дистанционного съема речевой информации с проводных линий электросвязи, радиомикрофонных закладок, телефонных закладок, микрофонных закладок, минимагнитофонов и диктофонов); и) электромагнитный перехват информации (в радиосетях связи, побочных электромагнитных излучений, побочных электромагнитных наводок, паразитных модуляций ВЧ-сигналов, паразитных информативных токов и напряжений во вспомогательных сетях технических средств передачи информации);
- активный (контактный) несанкционированный доступ к информации: а) с использованием физического доступа путем непосредственного воздействия на материальные носители, иные средства обработки и защиты информации;

б) с использованием штатных и специально разработанных (приспособленных, запрограммированных) средств для негласного получения, уничтожения, модификации и блокирования информации.

2.2. Неумышленные (ошибки деятельности человека — непреодолимые факторы): а) ошибки при создании (изготовлении) средств электронно-вычислительной техники, электросвязи и защиты информации (ошибки проектирования, кодирования информации, изготовления элементов технических средств и систем); б) ошибки, возникающие в процессе работы (эксплуатации) средств электронно-вычислительной техники, электросвязи и защиты информации (неадекватность концепции обеспечения безопасности; ошибки управления системой защиты; ошибки персонала; сбои и отказы оборудования и программного обеспечения; ошибки при производстве пуско-наладочных и ремонтных работ. Под материальным носителем информации понимается любое техническое устройство либо физическое поле, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации.

Элементами системы защиты информации являются:

- правовой;
- организационный;
- инженерно-технический;
- программно-аппаратный;
- криптографический.

Правовой элемент системы основывается на нормах информаци онного права и предполагает юридическое закрепление взаимоотно шений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязан ности персонала соблюдать установленные меры защитного характера, ответственности персонала за нарушение порядка защиты информации. Этот элемент включает:

- наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, трудовых контрактах, в должностных инструкциях положений и обязательств по защите конфиденциальном информации;
- формулирование и доведение до сведения всех сотрудников положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;
- разъяснение лицам, принимаемым на работу, положения о до бровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Элемент включает в себя регламентацию:

- формирования и организации деятельности СБ и службы конфиденциальной документации, обеспечения деятельности этих служб нормативно-методическими документами по организации и технологии защиты информации;
- составления и регулярного обновления состава защищаемой информации фирмы, составления и ведения перечня защищаемых бумажных, машиночитаемых и электронных документов;
- разрешительной системы разграничения доступа персонала к защищаемой информации;
- методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования сотрудников;
- направлений и методов воспитательной работы с персоналом, контроля соблюдения сотрудниками порядка защиты информации;

- технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов; внемашинной технологии защиты электронных документов;
- порядка защиты ценной информации фирмы от случайных или умышленных несанкционированных действий персонала;
- ведения всех видов аналитической работы;
- порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями СМИ;
- оборудования и аттестации помещений и рабочих зон, выделенных для работы с конфиденциальной информацией;
- пропускного режима на территории, в здании, помещениях, идентификации транспорта и персонала фирмы;
- системы охраны территории;
- действий персонала в экстремальных ситуациях;
- организационных вопросов приобретения, установки и эксплуатации технических средств защиты информации и охраны;
- работы по управлению системой защиты информации;
- критериев и порядка проведения оценочных мероприятий по уста новлению степени эффективности системы защиты информации.

Элемент организационной защиты является стержнем, основной частью рассматриваемой комплексной системы. Меры по организационной защите информации составляют 50-60% в структуре большинства СЗИ. Это связано с тем, что важной составной частью организационной защиты информации являются подбор, расстановка и обучение персонала, который будет реализовывать на практике СЗИ. Организационные меры защиты отражаются в нормативно-методических документах СБ, службы конфиденциальной документации учреждения или фирмы.

Инженерно-технический элемент СЗИ предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств**.** Элемент включает в себя:

- сооружения физической защиты от проникновения посторонних лиц на территорию, в здание, помещение (заборы, решетки, стальные двери...);
- средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов, других приборов и офисного оборудования, при проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов и т. д.;
- средства защиты помещений от визуальных способов технической разведки;
- средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализирования, информирования и идентификации);
- средства противопожарной охраны;
- средства обнаружения приборов и устройств технической разведки (подслушивающих устройств, тайно установленной звукозаписывающей и телевизионной аппаратуры);
- технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг и т. д.

Программно-аппаратный элемент СЗИ предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей, и различных информационных системах. Элемент включает в себя:

- автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;
- программы защиты информации, работающие в комплексе с про граммами обработки информации;
- программы защиты информации, работающие в комплексе с тех ническими устройствами защиты информации (прерывающими работу с ЭВМ при нарушении системы доступа, стирающие данные при не санкционированном входе в базу данных и др.).

Криптографический элемент СЗИ предназначен для защиты конфиденциальной информации методами криптографии. Элемент включает:

- регламентацию использования различных криптографических методов в ЭВМ и локальных сетях;
- определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи;
- регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радиосвязи;
- регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;
- регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров.

Кодирование и шифрование — основные методы криптографической защиты. Наряду с ними к криптографическим методам относят методы рассечения (разнесения) и сжатия (расширения) информации. Рассечение (разнесение) информации заключается в том, что массив защищенных данных делится на части, каждая из которых в отдельно сти не позволяет раскрыть содержание защищаемой информации. Эти фрагменты можно передавать по нескольким источникам. Разносить по времени и по месту записи на дискете или любом другом запоми нающем устройстве. Сжатие (расширение) информации представляет собой замену часто встречающихся одинаковых последовательностей символов некоторыми заранее выбранными символами или же под мешивание дополнительной информации.

В каждом элементе защиты могут быть реализованы на практике только составные части в зависимости от поставленных задач зашиты в крупных и некрупных фирмах различного профиля, в малом бизнесе. Структура системы, состав и содержание элементов, их взаимосвязь зависят от объема и ценности защищаемой информации, характера возникающих угроз безопасности информации, требуемой надежности защиты и стоимости системы[1].