# Введение

Информационная безопасность предприятия – это защищенность информации, которой располагает предприятие (производит, передает или получает) от несанкционированного доступа, разрушения, модификации, раскрытия и задержек при поступлении. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью комплексной информационной безопасности является сохранение информационной системы предприятия в целости и сохранности, защита и гарантирование полноты и точности выдаваемой ею информации, минимизация разрушений и модификация информации, если таковые случаются.

Компьютеризация, развитие телекоммуникаций предоставляют сегодня широкие возможности для автоматизированного доступа к различным конфиденциальным, персональным и другим важным, критическим данным в обществе (его граждан, организаций и т.д.).

Проблема создания и поддержания защищенной среды информационного обмена, реализующая определенные правила и политику безопасности современной организации, является весьма актуальной. Информация давно уже перестала играть эфемерную, чисто вспомогательную роль, превратившись в весьма важный и весомый, чуть ли не материальный, фактор со своими стоимостными характеристиками, определяемыми той реальной прибылью, которую можно получить от ее (информации) использования. В то же время, вполне возможен сегодня и вариант ущерба, наносимого владельцу информации (предприятию) путем несанкционированного проникновения в информационную структуру и воздействия на ее компоненты.[[1]](#footnote-1)

Объектом исследования являются: информационная безопасность.

Предмет исследования: защита информации.

Таким образом, цель данной работы изучение информационной безопасности.

Для достижения поставленной цели необходимо выполнить следующие задачи: рассмотреть оценку безопасности информационных систем, виды, методы и средства защиты информации; проанализировать структуру системы защиты информации.

# **1. Оценка безопасности информационных систем**

В условиях использования автоматизированной информационной технологии (АИТ) под безопасностью понимается состояние защищенности информационных систем (далее ИС) от внутренних и внешних угроз.

Показатель защищенности ИС – характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности.[[2]](#footnote-2)

Для оценки реального состояния безопасности ИС могут применяться различные критерии. Анализ отечественного и зарубежного опыта показал определенную общность подхода к определению состояния безопасности ИС в разных странах. Для предоставления пользователю возможности оценки вводится некоторая система показателей и задается иерархия классов безопасности. Каждому классу соответствует определенная совокупность обязательных функций. Степень реализации выбранных критериев показывает текущее состояние безопасности. Последующие действия сводятся к сравнению реальных угроз с реальным состоянием безопасности.

Если реальное состояние перекрывает угрозы в полной мере, система безопасности считается надежной и не требует дополнительных мер. Такую систему можно отнести к классу систем с полным перекрытием угроз и каналов утечки информации. В противном случае система безопасности нуждается в дополнительных мерах защиты.

Политика безопасности – это набор законов, правил и практического опыта, на основе которых строится управление, защита и распределение конфиденциальной информации.

Анализ классов безопасности показывает, что чем он выше, тем более жесткие требования предъявляются к системе.

Руководящие документы в области зашиты информации разработаны Государственной технической комиссией при Президенте Российской Федерации. Требования этих документов обязательны для исполнения только организациями государственного сектора либо коммерческими организациями, которые обрабатывают информацию, содержащую государственную тайну. Для остальных коммерческих структур документы носят рекомендательный характер.

#

# **2. Методы и средства построения систем информационной безопасности (СИБ)**

Создание систем информационной безопасности в ИС и ИТ основывается на следующих принципах: системный подход, принцип непрерывного развития системы, разделение и минимизация полномочий, полнота контроля и регистрация попыток, обеспечение надежности системы защиты, обеспечение контроля за функционированием системы защиты, обеспечение всевозможных средств борьбы с вредоносными программами, обеспечение экономической целесообразности.[[3]](#footnote-3)

В результате решения проблем безопасности информации современные ИС и ИТ должны обладать следующими основными признаками:

* наличием информации различной степени конфиденциальности;
* обеспечением криптографической защиты информации различной степени конфиденциальности при передаче данных;
* иерархичностью полномочий субъектов доступа к программам и компонентам ИС и ИТ (к файл-серверам, каналам связи и т.п.);
* обязательным управлением потоками информации, как в локальных сетях, так и при передаче по каналам связи на далекие расстояния;
* наличием механизма регистрации и учета попыток несанкционированного доступа, событий в ИС и документов, выводимых на печать;
* обязательной целостностью программного обеспечения и информации в ИТ;
* наличием средств восстановления системы защиты информации;
* обязательным учетом магнитных носителей;
* наличием физической охраны средств вычислительной техники и магнитных носителей;
* наличием специальной службы информационной безопасности системы.

информационный безопасность криптографический система

# **3. Структура системы информационной безопасности**

При рассмотрении структуры системы информационной безопасности (СИБ) возможен традиционный подход – выделение обеспечивающих подсистем. Система информационной безопасности, как и любая ИС, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет способна выполнить свою целевую функцию. С учетом этого, СИБ должна иметь следующие виды (элементы) обеспечения: правовое, организационное, нормативно-методическое, информационное, техническое (аппаратное), программное, математическое, лингвистическое.[[4]](#footnote-4)

**Правовое обеспечение** СИБ основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные собственником информации ограничительные и технологические меры защитного характера, а также ответственности персонала за нарушение порядка защиты информации. Этот вид обеспечения включает:

• наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, в должностных и рабочих инструкциях положений и обязательств по защите конфиденциальной информации;

• формулирование и доведение до сведения всех сотрудников фирмы (в том числе не связанных с конфиденциальной информацией) положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;

• разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.[[5]](#footnote-5)

Следует отметить, что из всех мер зашиты в настоящее время ведущую роль играют **организационные мероприятия**. Поэтому следует выделить вопрос организации службы безопасности. Реализация политики безопасности требует настройки средств защиты, управления системой зашиты и осуществления контроля функционирования ИС. Как правило, задачи управления и контроля решаются административной группой, состав и размер которой зависят от конкретных условий. Очень часто в эту группу входят администратор безопасности, менеджер безопасности и операторы.

Обеспечение и контроль безопасности представляют собой комбинацию технических и административных мер. По данным зарубежных источников, у сотрудников административной группы обычно 1/3 времени занимает техническая работа и около 2/3 – административная (разработка документов, связанных с защитой ИС, процедуры проверки системы защиты и т.д.). Разумное сочетание этих мер способствует уменьшению вероятности нарушений политики безопасности.[[6]](#footnote-6)

Административную группу иногда называют группой информационной безопасности. Она обособлена от всех отделов или групп, занимающихся управлением самой ИС, программированием и другими относящимися к системе задачами, во избежание возможного столкновения интересов.

Организационное обеспечение включает в себя регламентацию:

• формирования и организации деятельности службы безопасности и службы конфиденциальной документации (или менеджера по безопасности, или референта первого руководителя), обеспечения деятельности этих служб (сотрудника) нормативно – методическими документами по Организации и технологии защиты информации;

• составления и регулярного обновления состава (перечня, списка, матрицы) защищаемой информации фирмы, составления и ведения перечня (описи) защищаемых бумажных, машиночитаемых и электронных документов фирмы;

• разрешительной системы (иерархической схемы) 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 фирмы (делопроизводственной, автоматизированной и смешанной технологий); 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 рекламных агентств, средств массовой информации;

• оборудования и аттестации помещений и рабочих зон, выделенных для работы с конфиденциальной информацией, лицензирования технических систем и средств защиты информации и охраны, сертификации информационных систем, предназначенных для обработки защищаемой информации;

• пропускного режима на территории, в здании и помещениях фирмы, идентификации персонала и посетителей;

• системы охраны территории, здания, помещений, оборудования, транспорта и персонала фирмы;

• действий персонала в экстремальных ситуациях;

• организационных вопросов приобретения, установки и эксплуатации технических средств защиты информации и охраны;

• организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;

• работы по управлению системой защиты информации;

• критериев и порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации.

Организационный элемент защиты информации является стержнем, основной частью комплексной системы элементов системы защиты – «элемент организационно-правовой защиты информации».

**Нормативно-методическое** обеспечение может быть слито с правовым, куда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации; различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований соблюдения конфиденциальности.

Нормативы и стандарты по защите информации накладывают требования на построение ряда компонентов, которые традиционно входят в обеспечивающие подсистемы самих информационных систем, т.е. можно говорить о наличии тенденции к слиянию обеспечивающих подсистем ИС и СИБ.

Примером может служить использование операционных систем (ОС). В разных странах выполнено множество исследований, в которых анализируются и классифицируются изъяны защиты ИС. Выявлено, что основные недостатки зашиты ИС сосредоточены в ОС. Использование защищенных ОС является одним из важнейших условий построения современных ИС. Особенно важны требования к ОС, ориентированным на работу с локальными и глобальными сетями. Развитие Интернета оказало особенно сильное влияние на разработку защищенных ОС. Развитие сетевых технологий привело к появлению большого числа сетевых компонентов (СК). Системы, прошедшие сертификацию без учета требований к сетевому программному обеспечению, в настоящее время часто используются в сетевом окружении и даже подключаются к Интернету. Это приводит к появлению изъянов, не обнаруженных при сертификации защищенных вычислительных систем, что требует непрерывной доработки ОС.

**Инженерно-техническое обеспечение** системы защиты информации предназначено для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств. При защите информационных систем этот элемент имеет важное значение, хотя стоимость средств технической защиты и охраны велика. Элемент включает в себя:

• сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здание и помещения (заборы, решетки, стальные двери, кодовые замки, идентификаторы, сейфы и др.);

• средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и других приборов и офисного оборудования, при проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов и т.п.;

• 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 и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т.п.);

• технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг и т.п.

**Программно-аппаратное обеспечение** системы защиты предназначено для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах. Однако фрагменты этой защиты могут применяться как сопутствующие средства в инженерно-технической и организационной защите. Элемент включает в себя:

• автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;

• программы защиты информации, работающие в комплексе с программами обработки информации;

• программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающие данные при несанкционированном входе в базу данных и др.).[[7]](#footnote-7)

# 4. Методы и средства обеспечения безопасности информации

Методы и средства обеспечения безопасности информации в АИС в обобщенном и упрощенном виде отражает схема на нижепредставленном рисунке.

Противодействие атакам вредоносных программ

Препятствия

Управление доступом

Шифрование

Регламентация

Принуждение

Побуждение

Организационные

Законодательные

Морально-этические

***Неформальные***

Физические

Аппаратные

Программные

***Технические***

***Формальные***

Методы и средства обеспечения безопасности информации

Рассмотрим неформальные методы защиты информации.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Кроме того, управление доступом включает следующие функции защиты:

* идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
* аутентификацию для опознания, установления подлинности пользователя по предъявленному им идентификатору;
* проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
* разрешение и создание условий работы в пределах установленного регламента;
* регистрацию (протоколирование) обращений к защищаемым ресурсам;
* реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

В настоящее время для исключения неавторизованного проникновения в компьютерную сеть стал использоваться комбинированный подход: пароль плюс идентификация пользователя по персональному ключу. Ключ представляет собой пластиковую карту (магнитная или со встроенной микросхемой – смарт-карта) или различные устройства для идентификации личности по биометрической информации – по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д. Серверы и сетевые рабочие станции, оснащенные устройствами чтения смарт-карт и специальным программным обеспечением, значительно повышают степень защиты от несанкционированного доступа.

Шифрование – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ – комплекс разнообразных мер организационного характера и по использованию антивирусных программ. Цели принимаемых мер: уменьшение вероятности инфицирования АИС; выявление фактов заражения системы; уменьшение последствий информационных инфекций; локализация или уничтожение вирусов; восстановление информации в ИС.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – такой метод зашиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – такой метод защиты, который побуждает пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – специализированные программы и программные комплексы, предназначенные для защиты информации в ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем руководителя организации.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил,

Морально-этические средства зашиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например, честность) либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения. Характерным примером таких предписаний является «Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США».[[8]](#footnote-8)

#

# **5. Криптографические методы защиты информации**

***Криптология*** – наука, состоящая из двух направлений: криптографии и криптоанализа. ***Криптоанализ*** – это наука (и практика ее применения) о методах и способах вскрытия шифров. Соотношение криптографии и криптоанализа очевидно: криптография – это защита, т.е. разработка шифров, а криптоанализ – нападение, т.е. вскрытие шифров.[[9]](#footnote-9)

Сущность криптографических методов заключается в следующем. Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым преобразуется в шифрограмму, т.е. в закрытый текст или графическое изображение документа. В таком виде сообщение и передается по каналу связи, пусть даже и незащищенному. Санкционированный пользователь после получения сообщения дешифрует его (т.е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям. Таким образом, даже в случае перехвата сообщения взломщиком текст сообщения становится недоступным для него.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (последовательностью бит), обычно называемым шифрующим ключом.

Каждый используемый ключ может производить различные шифрованные сообщения, определяемые только этим ключом. Для большинства систем закрытия схема генератора ключа может представлять собой набор инструкций и команд либо узел аппаратуры, либо компьютерную программу, либо все вместе взятое, но в любом случае процесс шифрования (дешифрования) определяется только этим специальным ключом. Чтобы обмен зашифрованными данными проходил успешно, как отправителю, так и получателю необходимо знать правильную ключевую установку и хранить ее в тайне.

Стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее, этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации принятой информации. Взломщик в случае перехвата сообщения будет иметь дело только с зашифрованным текстом, а истинный получатель, принимая закрытые известным только ему и отправителю ключом сообщения, будет надежно защищен от возможной дезинформации.

Современная криптография знает два типа криптографических алгоритмов: классические алгоритмы, основанные на использовании закрытых, секретных ключей, и новые алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключи (эти алгоритмы называются также асимметричными). Кроме того, существует возможность шифрования информации и более простым способом – с использованием генератора псевдослучайных чисел.

Метод криптографической защиты с открытым ключом реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию и поэтому неприменим для таких серьезных информационных систем, каковыми являются, например, банковские системы.

Наиболее перспективными системами криптографической защиты данных сегодня считаются асимметричные криптосистемы, называемые также системами с открытым ключом. Их суть состоит в том, что ключ, используемый для зашифровывания, отличен от ключа расшифровывания. При этом ключ зашифровывания не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа зашифровывания невозможно. Для расшифровывания используется специальный, секретный ключ. При этом знание открытого ключа не позволяет определить ключ секретный. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом.

Специалисты считают, что системы с открытым ключом больше подходят для шифрования передаваемых данных, чем для защиты данных, хранимых на носителях информации. Существует еще одна область применения этого алгоритма – цифровые подписи, подтверждающие подлинность передаваемых документов и сообщений. Асимметричные криптосистемы наиболее перспективны, так как в них не используется передача ключей другим пользователям, и они легко реализуются как аппаратным, так и программным способом.

В системах передачи и обработки информации все чаще возникает вопрос о замене рукописной подписи, подтверждающей подлинность того или иного документа, ее электронным аналогом – электронной цифровой подписью (ЭЦП). Сформулируем три свойства ЭЦП:

1. Подписать документ может только «законный» владелец подписи.

2. Автор подписи не может от нее отказаться.

3. В случае возникновения спора, возможно, участие третьих лиц (например, суда) для установления подлинности подписи.[[10]](#footnote-10)

Ею могут скрепляться всевозможные электронные документы, начиная с различных сообщений и кончая контрактами. ЭЦП может применяться также для контроля доступа к особо важной информации. К ЭЦП предъявляются два основных требования: высокая сложность фальсификации и легкость проверки.

Для реализации ЭЦП можно использовать как классические криптографические алгоритмы, так и асимметричные, причем именно последние обладают всеми свойствами, необходимыми для ЭЦП.

ЭЦП чрезвычайно подвержена действию обобщенного класса «троянских» программ с преднамеренно заложенными в них потенциально опасными последствиями, активизирующимися при определенных условиях. Например, в момент считывания файла, в котором находится подготовленный к подписи документ, эти программы могут изменить имя подписывающего лица, дату, какие-либо данные (например, сумму в платежных документах) и т.п.

Практика использования систем автоматизированного финансового документооборота показала, что программная реализация ЭЦП наиболее подвержена действию «троянских» программ, позволяющих проводить заведомо ложные финансовые документы, а также вмешиваться в порядок разрешения споров по факту применения ЭЦП. Поэтому при выборе системы ЭЦП предпочтение безусловно должно быть отдано ее аппаратной реализации, обеспечивающей надежную защиту информации от несанкционированного доступа, выработку криптографических ключей и ЭЦП. Следовательно, надежная криптографическая система должна удовлетворять следующим требованиям:

* процедуры зашифровывать и расшифровывания должны быть прозрачны» для пользователя;
* дешифрование закрытой информации должно быть максимально затруднено;
* содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма;
* надежность криптозащиты не должна зависеть от содержания в секрете самого алгоритма шифрования.

Процессы защиты информации, шифрования и дешифрования связаны с кодируемыми объектами и процессами, их свойствами, особенностями перемещения. Такими объектами и процессами могут быть материальные объекты, ресурсы, товары, сообщения, блоки информации, транзакции (минимальные взаимодействия с базой данных по сети). Кодирование кроме целей защиты, повышая скорость доступа к данным, позволяет быстро определять и выходить на любой вид товара и продукции, страну производителя и т.д. Таким образом, связываются в единую логическую цепочку операции, относящиеся к одной сделке, но географически разбросанные по сети.

Например, штриховое кодирование используется как разновидность автоматической идентификации элементов материальных потоков, например товаров, и применяется для контроля за их движением в реальном времени. При этом достигается оперативность управления потоками материалов и продукции, повышается эффективность управления предприятием. Штриховое кодирование позволяет не только защитить информацию, но и обеспечивает высокую скорость чтения и записи кодов. Наряду со штриховыми кодами в целях защиты информации используют голографические методы.

Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением. Голография представляет собой раздел науки и техники, занимающийся изучением и созданием способов, устройств для записи и обработки волн различной природы. Оптическая голография основана на явлении интерференции волн. Интерференция волн наблюдается при распределении в пространстве волн и медленном пространственном распределении результирующей волны. Возникающая при интерференции волн картина содержит информацию об объекте. Если эту картину фиксировать на светочувствительной поверхности, то образуется голограмма. При облучении голограммы или ее участка опорной волной можно увидеть объемное трехмерное изображение объекта. Голография применима к волнам любой природы и в настоящее время находит все большее практическое применение для идентификации продукции различного назначения.

В совокупности кодирование, шифрование и защита данных предотвращают искажения информационного отображения реальных производственно-хозяйственных процессов, движения материальных, финансовых и других потоков и тем самым способствуют повышению обоснованности формирования и принятия управленческих решений.

# Заключение

В настоящее время *организация режима информационной безопасности* становится критически важным *стратегическим фактором* развития любой отечественной компании. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей российской нормативно-методической базы в области защиты информации.[[11]](#footnote-11)

Главными требованиями к организации эффективного функционирования системы защиты информации являются: персональная ответственность руководителей и сотрудников за сохранность носителя и конфиденциальность информации, регламентация состава конфиденциальных сведений и документов, подлежащих защите, регламентация порядка доступа персонала к конфиденциальным сведениям и документам, наличие специализированной службы безопасности, обеспечивающей практическую реализацию системы защиты и нормативно-методического обеспечения деятельности этой службы.

Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

Практической реализацией концепции информационной безопасности организации является технологическая система защиты информации. Защита информации представляет собой жестко регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ценных информационных ресурсов и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности фирмы.

# Список используемых источников

1. Белов Е.Б., Лось В.П., Мещеряков Р.В. Основы информационной безопасности: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2006. 544 с.
2. Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд. перераб. и доп. М.: Изд-во ЮНИТИ-ДАНА, 2008. 463 с.
3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2004. 280 с.
4. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Изд-во ДМК Пресс, 2004. 384 с.
5. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2005. 229 с.
6. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. М.: Издательско-торговая корпорация Дашков и К°, 2005. 336 с.
7. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие. М.: Изд-во ИНФРА-М, 2001. 304 с.
8. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Украина: Изд-во Юниор, 2003. 504 с.
1. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. М.: Издательско-торговая корпорация Дашков и К°, 2005. [↑](#footnote-ref-1)
2. Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд., доп. и перераб. М.: Изд-во ЮНИТИ-ДАНА, 2008. 463 с. [↑](#footnote-ref-2)
3. Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд. перераб. и доп. М.: Изд-во ЮНИТИ-ДАНА, 2008. с.218. [↑](#footnote-ref-3)
4. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2004. с. 202. [↑](#footnote-ref-4)
5. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие. М.: Изд-во ИНФРА-М, 2001. с.23-24 [↑](#footnote-ref-5)
6. Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд.М.: Изд-во ЮНИТИ-ДАНА, 2008. с.219. [↑](#footnote-ref-6)
7. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие. М.: Изд-во ИНФРА-М, 2001. 304 с. [↑](#footnote-ref-7)
8. Белов Е. Б., Лось В. П., Мещеряков Р. В. Основы информационной безопасности: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2006. с.248 [↑](#footnote-ref-8)
9. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Украина: Изд-во Юниор, 2003. с. 338. [↑](#footnote-ref-9)
10. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2005. с. 52. [↑](#footnote-ref-10)
11. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: Изд-во ДМК Пресс, 2004. с.7. [↑](#footnote-ref-11)