Содержание:

ВВЕДЕНИЕ

Актуальность темы курсовой работы заключается в том, что современное общество каждый день накапливает и передает информацию с помощью разнообразных «гаджетов», облачных технологий. Объемы информации действительно колоссальны и их необходимо не только как-то упорядочить, систематизировать, но и защищать.

Если раньше любое предприятие хранило всю накопленную информацию в огромных папках, которых за годы накапливалось неприличное количество, то сейчас все хранится в электронном виде. Такая информация является лакомым куском для конкурентов, если мы говорим о сферах бизнеса, или для врагов, если мы говорим о государстве. Обеспечить защиту информации от угроз безопасности помогают системы криптографической защиты информации.

В настоящее время мы все чаще встречаем такие понятия как аутентификация, идентификация, электронная подпись, шифрование и другие. Все это применяется для защиты информации. Но несмотря на развитие информационных технологий в сфере защиты информации, уязвимостей, а значит и угроз безопасности появляется все больше.

Проблемы защиты информации являются очень важными и охватывают широкий круг задач:

- обеспечение конфиденциальности информации;

- обеспечение целостности информации;

- обеспечение доступа к информации средствами аутентификации и идентификации.

Объектом исследования курсовой работы являются виды и состав угроз информационной безопасности, а предметом исследования – меры противодействия угрозам безопасности и средства криптографической защиты информации.

Целью курсовой работы является изучение современных угроз информационной безопасности.

Для достижения поставленной цели в курсовой работе необходимо решить следующие задачи:

1) дать определения основным понятиям – информация, угроза, информационная безопасность, аутентификация, идентификация, шифрование, средство криптографической защиты информации;

2) рассмотреть проблемы информационной безопасности;

3) рассмотреть классификацию угроз информационной безопасности;

4) изучить меры противодействия угрозам информационной безопасности;

5) изучить современные средства криптографической защиты информации.

При написании курсовой работы использовались научные труды следующих авторов: Астахова Л.В. [1], Бондарев В.В. [2], Борисова С.Н. [3], Варлатая С.К. [4], Горбатов В.С. [5] и другие.

1. Информационная безопасность

1.1 Основные понятия

Реалии современного информационного общества однозначно показывают, что ни одна сфера жизни цивилизованного государства не может эффективно функционировать без развитой информационной инфраструктуры, широкого применения аппаратно-программных средств и сетевых технологий обработки информации.

По мере возрастания ценности информации, развития и усложнения средств ее обработки безопасность общества все в большей степени зависит от безопасности используемых информационных технологий.

Многочисленные публикации последних лет показывают, что способы злоупотреблений информацией, циркулирующей в системах, совершенствуются не менее интенсивно, чем меры защиты от них. Более того, объектами компьютерных

преступлений являются не только информационные ресурсы, но и сами компьютеры, программное обеспечение, телекоммуникационное оборудование и линии связи. [19]

Комплексное обеспечение информационной безопасности может быть реализовано, если создана и функционирует система защиты информации, охватывающая весь жизненный цикл прохождения информации – от идеи и разработки проекта до утилизации изделия – и всю технологическую цепочку сбора, хранения, обработки и выдачи информации. [15]

Понятие «безопасность» охватывает широкий круг интересов, как отдельных лиц, так и целых государств. Во все исторические времена существенное внимание уделялось проблеме информационной безопасности, обеспечению защиты конфиденциальной информации от ознакомления с ней конкурирующих групп. [7]

Перед тем, как рассматривать угрозы информационной безопасности, а также средства криптографической защиты информации более подробно, следует рассмотреть основные понятия.

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информация может быть представлена в совершенно разных формах (в виде символов, сигналов и т.д.) на носителях различных типов.

Защищаемая информация – это информация, которая является собственностью и должна быть защищена в соответствии с правовыми нормами и требованиями, устанавливаемыми собственником информации (физическим лицом, группой лиц, юридическим лицом или государством).

В настоящее время большие объемы важной информации хранятся, обрабатываются и передаются с использованием автоматизированных систем обработки информации. Система обработки информации представляет собой совокупность технических и программных средств, а также методов обработки информации и действий персонала с целью обработки информации.

Объектом информатизации называют совокупность информационных ресурсов, средств и систем обработки информации, которые используются в соответствии с определенной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и

системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

В зависимости от конкретных условий, может решаться задача обеспечения комплексной безопасности объекта информатизации или защиты отдельных ресурсов – информационных, программных и т. д.

Информационный ресурс представляет собой документы или массивы документов, которые содержаться в каких-либо информационных системах, будь то библиотеки, архивы, фонды, и т.д.).

Если рассматривать вопросы безопасности информационных систем, то надо говорить о наличии некоторых «желательных» состояний системы, через которые и описывается ее «защищенность» или «безопасность». Безопасность является таким же свойством системы, как надежность или производительность, и в последнее время ей уделяется все большее внимание.

Чтобы указать на причины выхода системы из безопасного состояния, вводятся понятия «угроза» и «уязвимость».

Угрозой безопасности информации называют совокупность факторов и условий, которые создают потенциальную или реально существующую опасность нарушения безопасности информации.

Источников угрозы безопасности информации является некий субъект (физическое лицо, материальный объект или физическое явление), который является непосредственной причиной возникновения угрозы безопасности информации. Угрозы делят на связанные и несвязанные с деятельностью человека. Примерами могут служить удаление пользователем файла с важной информацией и пожар в здании, соответственно. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

Свойство информационной системы, которое позволяет реализовать угрозу безопасности обрабатываемой информации называется уязвимостью информационной системы. Например, угроза потери информации из-за сбоя в сети электропитания реализуется, если в автоматизированной системе не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью). [16]

С понятием информационной безопасности тесно связано понятие защита информации.

Понятие информация достаточно широко, как и многозадачность понятия информационной безопасности, поэтому существует множество определений защиты информации.

Под защитой информации в узком смысле следует понимать совокупность мероприятий и действий, которые направленны на обеспечение ее безопасности информации, то есть конфиденциальности и целостности - в процессе сбора, передачи, обработки и хранения. Это определение подразумевает тождественность понятий защита информации и обеспечение безопасности информации. Безопасность информации – это свойство (или текущее состояние) передаваемой, накапливаемой, обрабатываемой и хранимой информации, которое характеризует ее степень защищенности от негативного воздействия внешней среды (человека и природы) и внутренних угроз, то есть ее конфиденциальность (секретность, смысловая или информационная скрытность), сигнальная скрытность (энергетическая и структурная) и целостность – устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам.

Если говорить и защите информации в более широком смысле, то следует понимать комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий. [8]

Криптология – наука, изучающая математические методы защиты информации путем ее преобразования. Криптологию можно разделить на два направления – криптографию и криптоанализ.

Если криптография изучает методы преобразования информации с помощью шифрования, то криптоанализ изучает методы дешифрования информации без знания ключа.

Существует ряд смежных, но не входящих в криптологию отраслей знания, например, стенография – обеспечение скрытности информации в информационных массивах. Обеспечение целостности информации в условиях случайного воздействия находится в ведении теории помехоустойчивого кодирования. Наконец, смежной областью по отношению к криптологии являются математические методы сжатия информации.

Шифрование - это процесс преобразования открытого текста в шифротекст с помощью определенных правил, содержащихся в шифре. Цель шифрования - сделать содержимое открытого текста непонятным для посторонних лиц. При шифровании, в отличие от кодирования, самостоятельному преобразованию подвергается каждый символ защищаемых данных. [3]

1.2 Проблемы информационной безопасности

Проблема обеспечения конфиденциальности информации при передаче сообщений по контролируемому противником каналу связи является традиционной задачей информационной безопасности. В простейшем случае эта задача описывается взаимодействием трех субъектов (сторон). Отправитель (владелец информации) осуществляет преобразование (шифрование) исходной (открытой) информации в форму передаваемых получателю по открытому каналу связи шифрованных сообщений, чтобы защитить ее от противника.

Противником можно называть абсолютно любой субъект, который не имеет права ознакомления с содержанием передаваемой информации. В качестве противника может выступать криптоаналитик, который владеет методами раскрытия шифров. Получатель информации может расшифровать информацию из полученных сообщений на законных основаниях. Противник в свою очередь, пытается овладеть защищаемой информацией (его действия обычно называют атаками). Его действия могут быть как пассивными, например, подслушивание, анализ трафика, перехват, запись зашифрованных сообщений с последующим дешифрованием, то есть попытками "взломать" защиту с целью овладения информацией.

В процессе активной атаки, противник может прерывать процесс передачи сообщений, модифицировать передаваемые шифрованные сообщения или вообще создавать поддельные (сфабрикованные) сообщения. Такие действия принято называть попыткой имитации и подмены соответственно.

Шифр – это некоторая совокупность обратимых преобразований, каждое из которых определяется некоторым параметром, который называется ключом, а также режимом шифрования, то есть порядком применения данного преобразования.

Ключ является важнейшим компонентом шифра, который отвечает за выбор преобразования, применяемого для зашифрования конкретного сообщения.

Обычно ключ представляет собой некоторую буквенную или числовую последовательность, которая задает алгоритм шифрования.

Каждое преобразование описывается некоторым криптографическим алгоритмом и однозначно определяется ключом. Для шифрования может применяться один и тот же криптографический алгоритм, но в различных режимах. Таким образом реализуются различные способы шифрования, будь то простая замена, гаммирование или иные способы. Каждому режиму шифрования присущи как свои преимущества, так и недостатки. Поэтому для каждой конкретной ситуации выбирается свой режим. При расшифровании полученной информации используется криптографический алгоритм, который может отличаться от алгоритма, который применяется для зашифрования информации. Соответственно ключи зашифрования и расшифрования могут различаться. Пару алгоритмов зашифрования и расшифрования обычно называют криптосистемой (шифрсистемой), а реализующие их устройства — шифртехникой.

Обеспечение целостности информации или неизменности ее в процессе передачи и хранения, наряду с конфиденциальностью, является не менее важной задачей. Для решения данной задачи разрабатываются средства, которые позволяют обнаружить не столько случайные искажения, сколько целенаправленное навязывание противником ложной информации. В этом случае в передаваемую информацию вносится избыточность. Обычно в этом случае к сообщению добавляется некоторая проверочная комбинация, вычисляемая с помощью специального алгоритма и играющая роль контрольной суммы для проверки целостности полученного сообщения.

Главным отличием данного метода от методов теории кодирования состоит в том, что алгоритм выработки проверочной комбинации является "криптографическим", другими словами, он зависит от секретного ключа. Если секретный ключ противнику не известен, то вероятность успешного навязывания противником искаженной или ложной информации очень мала. Такая вероятность служит мерой имитостойкости шифра, то есть способности самого шифра противостоять активным атакам со стороны противника.

Итак, для проверки целостности к сообщению M добавляется проверочная комбинация S, называемая кодом аутентификации сообщения (сокращенно — КАС) или имитовставкой. В этом случае по каналу связи передается пара C = (M, S). При получении сообщения M пользователь вычисляет значение проверочной комбинации и сравнивает его с полученным контрольным значением S

Несовпадение говорит о том, что данные были изменены.

Как правило, код аутентификации является значением некоторой (зависящей от секретного ключа) криптографической хеш-функции от данного сообщения: hk(M) = S. К кодам аутентификации предъявляются определенные требования. К ним относятся:

— невозможность вычисления значения hk(M) = S для заданного сообщения M без знания ключа k,

— невозможность подбора для заданного сообщения M с известным значением hk(M)=S другого сообщения M1 с известным значением hk (M1) = S1, без знания ключа k. Первое требование направлено против создания поддельных (сфабрикованных) сообщений при атаках типа имитация; второе — против модификации передаваемых сообщений при атаках типа подмена. [10]

Аутентификация – проверка подлинности. Она бывает односторонней, когда клиент доказывает свою подлинность серверу и двусторонней, когда процедура взаимна. [6]

В общем случае этот термин «аутентификация» может относиться к сеансу связи, сторонам, передаваемым сообщениям или к иным аспектам информационного взаимодействия.

Важной составной частью проблемы обеспечения достоверности получаемой информации является проверка и подтверждение, то есть установление подлинности всех аспектов информационного взаимодействия.

Эта проблема стоит особенно остро, если участвующие стороны друг другу не доверяют. В этом случае источником угроз может служить не только третья сторона (противник), но и сторона, с которой осуществляется взаимодействие.

Если говорить о сеансе связи (транзакции) аутентификация обеспечивает проверку: своевременности передачи данных, невозможности повторной передачи данных противником и целостности соединения. Для этого, как правило, используют дополнительные параметры, позволяющие "сцепить" передаваемые данные в легко проверяемую последовательность. Это достигается, например, путем вставки в сообщения некоторых специальных чисел или меток времени. Они позволяют предотвратить попытки повторной передачи, изменения порядка следования или обратной отсылки части переданных сообщений. При этом такие

вставки в передаваемом сообщении необходимо защищать (например, с помощью шифрования) от возможных подделок и искажений.

Применительно к сторонам взаимодействия аутентификация означает проверку одной из сторон того, что взаимодействующая с ней сторона — именно та, за которую она себя выдает. Часто аутентификацию сторон называют также идентификацией.

Основным средством для проведения идентификации являются протоколы идентификации. Они позволяют осуществлять идентификацию (и аутентификацию) каждой из участвующих во взаимодействии и не доверяющих друг другу сторон. Бывают протоколы односторонней и взаимной идентификации.

Протокол представляет собой распределенный алгоритм, который определяет последовательность действий каждой из сторон. Процесс выполнения протокола идентификации предполагает отсутствие передачи какой-либо информации о своем секретном ключе. Каждая сторона хранит его у себя и использует для формирования ответных сообщений на запросы, поступающие при выполнении протокола.

Наконец, применительно к самой информации аутентификация означает проверку того, что информация, передаваемая по каналу, является подлинной по содержанию, источнику, времени создания, времени пересылки и т. д.

Суть проверки подлинности содержания информации сводится к установлению ее неизменности (с момента создания) в процессе передачи или хранения, то есть проверке целостности. Подтверждением того, что исходный документ был создан именно заявленным источником и является аутентификация.

Стоит отметить, что если стороны доверяют друг другу и обладают общим секретным ключом, то аутентификацию сторон можно обеспечить с помощью кода аутентификации. В действительности, каждое успешно декодированное получателем сообщение может быть создано только отправителем, так, как только он знает их общий секретный ключ. В случае, если стороны не доверяют друг другу, то решение подобных задач с использованием общего секретного ключа становится невозможным. Для этих случаев аутентификации источника данных используют цифровую подпись.

Вообще, аутентификация источника данных и протокол идентификации выполняют одну и ту же роль. Но в них есть отличие: в случае аутентификации, имеется

некоторая передаваемая информация, авторство которой требуется установить, а в случае идентификации - требуется просто установить сторону, с шторой осуществляется взаимодействие.

В некоторых ситуациях отдельные лица могут отказаться от ранее принятых обязательств, это может произойти в связи с изменившимися обстоятельствами. В данном случае, необходим некоторый механизм, который препятствует подобным попыткам.

Если предполагается, что стороны не доверяют друг другу, то значит использование общего секретного ключа для решения поставленной проблемы становится невозможным. Отправитель может отказаться от факта передачи сообщения, утверждая, что его создал сам получатель (отказ от авторства). Получатель легко может модифицировать, подменить или создать новое сообщение, а затем утверждать, что оно получено от отправителя (приписывание авторства).

Ясно, что в такой ситуации арбитр при решении спора не будет иметь возможность установить истину.

В данной ситуации на помощь приходит иной механизм - цифровая подпись.

Цифровая подпись во многом аналогична обычной "ручной" подписи и имеет существенные отличия, связанные с возможностью отделения от документа и независимой передачей, а также возможностью подписывания одной подписью всех копий документа.

В состав цифровой подписи входит два алгоритма, один — для вычисления, а второй — для проверки подписи. Вычислить подпись может только ее автор. Проверку правильности подписи должен иметь возможность осуществить каждый, а значит алгоритм проверки должен быть общедоступным.

Для создания схемы цифровой подписи применяют симметричные шифрсистемы. В этом случае подписью может служить само зашифрованное на секретном ключе сообщение. Однако основной недостаток таких подписей состоит в том, что они являются одноразовыми: после каждой проверки секретный ключ становится известным.

Но в рамках использования симметричных шифрсистем из этой ситуации есть выход - это введение доверенной третьей стороны, выполняющей функции

посредника, которому доверяют обе стороны. В этом случае вся информация пересылается через посредника, а он в свою очередь осуществляет перешифрование сообщений с ключа одного из абонентов на ключ другого. Однако, эта схема является очень неудобной.

При использовании шифрсистем с открытым ключом возможны два подхода к построению системы цифровой подписи:

1. Преобразование сообщения в форму, по которой можно восстановить само сообщение, а значит и проверить правильность "подписи". В данном случае подписанное сообщение имеет, как правило, ту же длину, что и исходное сообщение. Для создания такого "подписанного сообщения" можно, например, произвести зашифрование исходного сообщения на секретном ключе автора подписи. Тогда каждый может проверить правильность подписи путем расшифрования подписанного сообщения на открытом ключе автора подписи.

2. Подпись вычисляется и передается вместе с исходным сообщением. Вычисление подписи заключается в преобразовании исходного сообщения в некоторую цифровую комбинацию (которая и является подписью). Алгоритм вычисления подписи должен зависеть от секретного ключа пользователя. Это необходимо для того, чтобы воспользоваться подписью мог бы только владелец ключа. В свою очередь, алгоритм проверки правильности подписи должен быть доступен каждому.

Этот алгоритм зависит от открытого ключа пользователя, а длина подписи не зависит от длины подписываемого сообщения.

Наряду с проблемой цифровой подписи возникла проблема построения бесключевых криптографических хеш-функций. При вычислении цифровой подписи сначала проводится хеширование, а затем уже подписание полученной комбинации с помощью секретного ключа. При этом функция хеширования должна быть "криптографической", хотя и не зависит от ключа и является открытой.

Имеется в виду свойство односторонности этой функции: по значению комбинации-свертки никто не должен иметь возможность подобрать соответствующее сообщение. В настоящее время имеются стандарты на криптографические хеш-функции, утверждаемые независимо от стандартов на криптографические алгоритмы и схемы цифровой подписи. [10]

1.3 Методы защиты информации

Метод – в самом общем значении это способ достижения цели, определенным образом упорядоченная деятельность.

В защите информации используются следующие методы: скрытие, ранжирование, дезинформация, дробление, страхование, морально-нравственные, учет, кодирование, шифрование.

Скрытие – предполагает наличие максимально ограниченного числа лиц, которые допущены к секретной информации. Это один из основных организационных принципов защиты информации. Реализация этого метода достигается обычно путем:

а) засекречивания информации. Информацию относят к разряду секретной или конфиденциальной. Существуют различные степени секретности и ограничение в связи с этим доступа к этой информации в зависимости от ее важности для собственника. На носителе информации проставляется соответствующий гриф секретности информации;

б) 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.

Следующим методов защиты информации является ранжирование. Этот метод позволяет, во-первых, поделить засекречиваемую информацию по степени секретности, и, во-вторых, регламентировать допуск 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 определяется матрицей доступа: может осуществляться по тематическому признаку или по признаку секретности информации.

Ранжирование – метод защиты информации, который является частным случаем метода скрытия. В данном случае пользователь не допускается к информации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и иных посторонних лиц.

Дезинформация является одним из методов защиты информации, который предполагает распространение заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности, положении дел на предприятии и т. д.

Расчленение или дробление – позволяет разбить информации на части с таким условием, что знание какой-то одной части информации не позволяет восстановить всю картину, всю технологию в целом (например, технология производства конечного продукта подразумевает знание всей цепочки операций, однако знание только одной операции технологии производства не позволить раскрыть всю цепочку и получить целевой продукт).

Применяется достаточно широко при производстве средств вооружения и военной техники, а также при производстве товаров народного потребления. Менее известен пример по членению технологии при изготовлении денег; например, на фабрике Гознака.

Страхование – достаточно «молодой» метод защиты информации и пока еще только получает признание. Его смысл состоит в том, чтобы защитить права и интересы собственника информации или средства информации как от традиционных угроз (кражи, стихийные бедствия), так и от угроз безопасности информации, а именно: защита информации от утечки, хищения, модификации (подделки), разрушения и др.

Страховые методы защиты информации применяются, прежде всего, для защиты коммерческих секретов от промышленного шпионажа. Особенно страховые методы эффективны в независимом секторе экономики, где административные методы и формы управления, а особенно контроля, плохо применимы.

Данный метод предполагает проведение аудиторского обследования с последующим заключением о сведениях, которые предприятие будет защищать как коммерческую тайну, надежность средств защиты.

Морально-нравственные методы играют очень важную роль в защите информации Их можно отнести к группе тех методов, которые, исходя из известного выражения, что «тайну хранят не замки, а люди». Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и 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 методы защиты информации предполагают проведение специальной работы с сотрудником, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), а также обучение сотрудника, осведомленного в сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Учет – также один из важнейших методов защиты информации. Он обеспечивает возможность получения данных о любом носителе защищаемой информации в любой промежуток времени, а также данных о всех пользователях этой информации. Без учета решать проблемы было бы невозможно, особенно когда количество носителей превысит какой-то минимальный объем.

Кодирование – метод защиты информации, который позволяет скрыть от соперника содержание защищаемой информации. Он заключается в преобразовании открытого текста в условный с помощью кодов при передаче информации по каналам связи.

Шифрование – метод защиты информации, который используется в случае опасность перехвата сообщений противником. Метод применяется при передаче сообщений с помощью различной радиоаппаратуры, письменных сообщений и в других случаях. Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра. [1]

2. Угрозы информационной безопасности

2.1 Основные понятия об угрозах безопасности

Под угрозой безопасности информации следует понимать потенциальную возможность возникновения такого явления или события, следствием которого могут быть негативные воздействия на информацию, нарушающие доступность, целостность или конфиденциальность информации. [5]

Угрозы информационной безопасности могут возникать на различных этапах жизненного цикла информационных систем и со стороны разных источников. Попытки реализации угроз информации называются информационными атаками на системы. [13]

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Существует такое понятие, как окно опасности. Это промежуток времени от момента, когда появляется возможность использовать слабое место, и до того момента, когда слабое место ликвидируется. Пока существует окно опасности, возможны успешные атаки на ИС.

Если говорить об ошибках в программном обеспечении, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при установке исправлений.

Для большинства уязвимых мест время существования окна опасности определяются следующими событиями:

1. Появляется информация об использовании уязвимостей в защите;

2. Разрабатываются так называемые «патчи» (или заплаты), закрывающие проблему;

3. Патчи устанавливаются в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно, а значит окна опасности существуют почти всегда, что в свою очередь подразумевает проведение постоянного мониторинга уязвимостей и оперативный выпуск заплат.

Некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС.

Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Стоит подчеркнуть, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым). [14]

2.2 Классификация угроз безопасности

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, которые приводят к неправомерному овладению защищаемыми сведениями. Такими действиями являются:

- ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;

- модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;

- разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба. В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации. [20]

По общей направленности угрозы информационной безопасности подразделяются на:

- угрозы конституционным правам и свободам граждан в области духовной жизни и информационной деятельности, духовному возрождению России;

- угрозы развитию отечественной индустрии средств информатизации, телекоммуникаций и связи, обеспечению потребностей внутреннего рынка, выходу ее продукции на мировые рынки, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- угрозы безопасности информационных ресурсов, нормальному функционированию информационных и телекоммуникационных систем как развернутых, так и создаваемых на территории России.

По уровням угрозы ИБ могут быть классифицированы следующим образом:

а) для личности:

- нарушение конституционных прав и свобод граждан на поиск, получение, передачу, производство и распространение объективной информации;

- лишение права граждан на неприкосновенность частной жизни;

- нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации;

- посягательства на объекты интеллектуальной собственности;

б) для общества:

- препятствия в построении информационного общества;

- лишение права на духовное обновление общества, сохранение его нравственных ценностей, утверждение в обществе идеалов высокой нравственности, патриотизма и гуманизма, развитие многовековых духовных традиций Отечества, пропаганду национального, культурного наследия, норм морали и общественной нравственности;

- манипулирование массовым сознанием;

- создание атмосферы, препятствующей приоритетному развитию современных телекоммуникационных технологий, сохранению и развитию отечественного научного и производственного потенциала;

в) для государства:

- защита интересов личности и общества;

- построение правового государства;

- формирование институтов общественного контроля за органами государственной власти;

- формирование системы подготовки, принятия и реализации решений органами государственной власти, обеспечивающей баланс интересов личности, общества и государства;

- защита государственных информационных систем и государственных информационных ресурсов;

- защита единого информационного пространства страны.

По происхождению основные угрозы жизненно важным интересам личности, общества и государства в информационной сфере включают:

а) внутренние:

- отставание России от ведущих стран мира по уровню информатизации;

- ослабление роли русского языка как государственного языка Российской Федерации;

- размывание единого правового пространства страны вследствие принятия субъектами Российской Федерации нормативных правовых актов, противоречащих Конституции Российской Федерации и федеральному законодательству;

- разрушение единого информационного и духовного пространства России, активизация различного рода религиозных сект, наносящих значительный ущерб духовной жизни общества, представляющих прямую опасность для жизни и здоровья граждан;

- отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам;

б) внешние:

- целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем Российской Федерации;

- стремление сократить использование русского языка как средства общения за пределами России;

- попытки не допустить участия России на равноправной основе в международном информационном обмене;

- подготовка к информационным войнам и использование информационного оружия. [18]

Меры противодействия угрозам безопасности

Угроза безопасности информации – потенциально возможное воздействие на информацию, которое прямо или косвенно может нанести урон пользователям или владельцам информации. [9]

Рассмотрим основные меры противодействия современным угрозам информационной безопасности.

Законодательные меры. Они включают в себя:

- указы,

- постановления,

- законы,

- руководящие документы,

- иные нормативно-правовые акты.

Все эти документы определяют нормы обращения с информацией, права и обязанности участников информационных отношений и устанавливают ответственность за несоблюдение данных норм.

Морально-этические меры предполагают соблюдение норм поведения, которые традиционно сложились в обществе или формируются по мере распространения информационных технологий. Обычно эти нормы не обязательны к применению, как требования нормативных актов, однако, их несоблюдение может нередко привести к снижению престижа компании.

Организационные меры — это меры административного характера, которые устанавливают правила функционирования системы обработки данных и деятельности обслуживающего персонала, а также порядок их взаимодействия для снижения вероятности осуществления угроз безопасности или потерь в случае их реализации. К организационным мерам можно отнести соблюдение требований разграничения доступа, надлежащую охрану территории объекта, формирование дисциплины и ответственности сотрудников и др.

Технологические меры предусматривают такие технологические решения и приемы, которые основаны на принципе избыточности (структурной, функциональной, информационной, временной и т. п.) и направлены на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках мандатного доступа (например, двойной ввод ответственной информации, инициализация ответственных операций только при наличии разрешений от нескольких должностных лиц, процедура проверки соответствия реквизитов исходящих и входящих сообщений в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т. п.).

Физические меры защиты основаны на применении разного рода механических, электро-или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов АС (пломбы, наклейки и т.п.).

Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

Таким образом, в арсенале специалистов по информационной безопасности имеется широкий спектр защитных мер: законодательных, морально-этических, административных (организационных), физических и технических (аппаратурных и программных) средств. Все они обладают своими достоинствами и недостатками, которые необходимо знать и правильно учитывать при создании систем защиты. [2]

3. Средства криптографической защиты информации

3.1 Виды средств криптографической защиты информации

Еще с незапамятных времен проблемы защиты информации волновали человечество. Например, первые системы шифров ученые встречают в Древней Греции, Древнем Египте, Спарте и Риме. Даже правители Венеции еще в XVI веке заботились о секретности информации. Ученые средневековья боялись преследования инквизиции, заботились о пальме первенства или же хотели, чтобы их знания достались только ученикам. Примеры достаточно сложных зашифрованных текстов археологи встречают и в русских памятниках XII–XIII веков. Первые технические системы начали разрабатываться сразу после изобретения телефона. Так, в США уже в 1875 году была подана заявка на изобретение, относящееся к закрытию телефонной связи. Да и по сегодняшний день радикальной мерой защиты каналов связи остается использование криптографических методов закрытия информации. [11]

Средства криптографической защиты информации (СКЗИ) – совокупность аппаратных и(или) программных компонентов, которые обеспечивают возможность шифрования информации с использованием одного или нескольких криптографических методов защиты.

Из определения следует, что существует ряд возможных реализаций методов криптографической защиты информации:

- программные, которые представляют собой реализацию одного или нескольких криптоалгоритмов на языке программирования высокого или низкого уровня, в виде отдельных библиотек, модулей, или выделенных программ с функцией криптографической защиты;

- аппаратные, которые реализуют криптоалгоритмы или их отдельные участки в микросхемах, процессорах и специализированных блоках (системы встроенной защиты) и аппаратных модулях (системы наложенной защиты), совмещенные со средствами вычислительной техники или встраиваемые в автоматизированные

системы;

- программно-аппаратные, которые представляют собой комплексы, состоящие из взаимосвязанных аппаратной и программной части с функциями криптографической защиты.

Программные средства шифрования представляют собой реализацию криптографического алгоритма на высокоуровневом или низкоуровневом языке программирования. Обычно функционирование таких средств криптографической защиты требует выполнения ряда вычислительных операций стандартными аппаратными средствами компьютерной системы.

Технология реализации криптоалгоритмов программными средствами имеет ряд отличий и особенностей. Кроме очевидного факта, что при использовании программного СКЗИ применение аппаратного расширения не является обязательным условием, можно отметить и ряд других особенностей:

- в общем случае работу программного СКЗИ нарушить легче, чем его аппаратного аналога, поэтому необходим дополнительный контроль за качеством функционирования;

- возможность контроля ошибок в закрытом тексте при шифровании путем внедрения избыточности;

- чтобы обеспечить надежное хранение ключей, создается мастер-ключ (ключа для шифрования файла, содержащего базу данных ключей) и других технологий, которые не требуют обычно при использовании аппаратного СКЗИ;

- необходимо иметь возможность масштабировать СКЗИ новыми программными блоками и модификациями используемых;

- принципиальная возможность использования программного СКЗИ с открытым кодом, что допускается при шифровании информации в частных целях и облегчает общую схему защиты.

Таким образом, программное СКЗИ отличает способность использования в распределенных и глобальных информационно-телекоммуникационных системах, более гибкая реализация, способность масштабирования и высокая мобильность.

Аппаратное средство криптографической защиты информации представляет собой специализированный блок, компонент средства вычислительной техники или

отдельное устройство, выполняющее шифрование информации.

Собственно, шифрование, согласно определению, представляет собой криптографическое преобразование данных для получения шифртекста (закрытого текста). Дополняя это определение, можно заметить на основании первого раздела данной книги, что шифрование в аппаратных средствах криптографической защиты также требует взаимодействия различных специализированных компонентов автоматизированной системы или средства вычислительной техники для реализации криптоалгоритмов.

Устройство криптографической защиты данных (УКЗД) – аппаратное СКЗИ, выполняющее также дополнительные функции по защите информации, например, защищающий от НСД.

Кроме того, аппаратное средство криптографической защиты содержит ряд дополнительных блоков, которые не требуются в программной реализации:

- блок управления криптографическими ключами;

- постоянная и оперативная память;

- блок синхронизации времени;

- генератор случайных чисел;

- устройство хранения и проверки хэш-значений и контрольных сумм.

Программно-аппаратные комплексы криптографической защиты информации являют собой наиболее сложную и эффективную разновидность средств обеспечения информационной безопасности с использованием криптоалгоритмов.

Под программно-аппаратными средствами криптографической защиты информации следует понимать комплексы, организованные специальным образом, и содержащие взаимосвязанные программные и аппаратные блоки, и реализующие следующий набор функций:

- аутентификацию и идентификацию пользователей;

- криптографическое преобразование данных;

- обеспечение целостности информации.

Усиление или замещение существующих функций защиты компьютерных систем для обеспечения требуемого уровня защищенности является основной целью применения программно-аппаратных средств обеспечения информационной безопасности.

Кроме этого стоит сказать о возможности реализации комплексного метода защиты информации. Это метод криптографической защиты как конфиденциальности информации, так и целостности. При использовании данного метода основную роль играют электронная цифровая подпись, шифрование и криптографические ключи. [10]

Цифровые сертификаты позволяют установить, было ли сообщение действительно создано конкретным лицом или организацией, а цифровые подписи позволяют узнавать было ли сообщение случайно или преднамеренно изменено. [4]

3.2 Требования к криптографическим системам

Процесс криптографического закрытия данных может осуществляться двумя способами: как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация допускает гибкость в использовании, поэтому более практична.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- только при наличии ключа зашифрованное сообщение можно прочитать;

- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

- на надежность защиты знание алгоритма шифрования никак не должно влиять;

- даже при использовании одного и того же ключа, незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения;

- структурные элементы алгоритма шифрования должны быть неизменными;

- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

- длина исходного текста должна быть равной длине шифрованного текста;

- не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

- любой ключ из множества возможных должен обеспечивать надежную защиту информации;

- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования. [17]

Современные аппаратно-программные комплексы СКЗИ

СКЗИ Verba-OW

Средство криптографической защиты информации "Верба-OW" разработано ЗАО "Московское отделение Пензенского научно-исследовательского электротехнического института" (МО ПНИЭИ) и решает следующие задачи:

- шифрование/расшифрование информации на уровне файлов;

- генерация электронной цифровой подписи (ЭЦП);

- проверка ЭЦП;

- обнаружение искажений, которые вносят злоумышленники или вирусы в защищаемую информацию.

Средства криптографической защиты информации серии "Верба" представляют собой автономное рабочее место или модули, встраиваемые в программное обеспечение заказчика.

Классификация программных продуктов и аппаратно-программных средств "Верба":

- файловый криптоменеджер представляет собой средства криптографической защиты данных пользователя, предназначенные для электронной подписи и шифрования данных пользователей на рабочих местах с последующим хранением и передачей по каналам связи;

- программный модуль "VCrypt" представляет собой набор библиотечных модулей, позволяющих вызвать криптографические функции непосредственно из приложения, осуществляющего обработку конфиденциальной информации, а также обеспечивают шифрование и создание ЭЦП.

- средства криптографической защиты клиент-серверных технологий, которые предназначены для использования в системах типа "клиент-сервер", таких как – доступ к базам данных, системы Банк-Клиент и т.п., и имеющие в своей основе принцип раздельного функционирования систем обработки запросов и систем криптографической защиты информации ("Криптографический сервер");

- защищенные почтовые технологии, которые предназначены как для организации собственных защищенных почтовых систем на базе X.400, так и для организации защищенного документооборота через Internet приложения. Применение шифрования и электронной цифровой подписи самого письма и его вложения позволяет обеспечить конфиденциальность, целостность и авторство передаваемых сообщений (Средства защиты электронной почты "Дионис").

- средства криптографической защиты каналов связи, которые предназначенны для защиты информации в каналах связи в режиме online по протоколам IP, X.25, Fray Relay и т.д.

Применение этих средств позволяет создавать виртуальные частные сети (*VPN*) и обеспечивать конфиденциальность передаваемых между ними данных, защищенный выход в Internet, и защищенный on-line доступ в частную сеть удаленных (мобильных) пользователей (Аппаратно-программный комплекс "Шип"). [12]

3.3 Программный комплекс VCERT PKI

Программный продукт VCERT PKI является результатом совместной работы компаний ЗАО "МО ПНИЭИ" и ООО "ВАЛИДАТА". Система управления сертификатами VCERT PKI – это многокомпонентная система, использующая инфраструктуру открытых ключей для обеспечения конфиденциальности информации, контроля целостности и подтверждения авторства электронных документов на основе использования криптографических процедур, реализованных в соответствии с российскими стандартами и международными рекомендациями.

VCERT PKI условно можно разделить на два компонента: программный интерфейс к криптографическим функциям для PKI приложений и систему управления сертификатами – инфраструктуру открытых ключей (PKI).

Система VCERT PKI реализована на платформах Windows и призвана обеспечить защиту информации на основе реализации инфраструктуры открытых ключей с использованием международного стандарта X.509.

Программное обеспечение VCERT PKI реализовано по модульному принципу, в его состав входят следующие основные программные комплексы и модули:

- VCA (VCERT Certification Authority) – программный комплекс Центр Сертификации (ЦС), предназначенный для создания на основе информации, предоставляемой Центром Регистрации, сертификатов открытых ключей, списков аннулированных сертификатов и их бумажных копий, а также хранения эталонной базы сертификатов и списков аннулированных сертификатов.

- VRA (VCERT Registration Authority) – программный комплекс Центр Регистрации (ЦР), предназначенный для регистрации пользователей и обеспечения взаимодействия пользователя с Центром Сертификации.

- VCS (VCERT Certificates Store) – программный комплекс Справочник Сертификатов, обеспечивающий администрирование справочника сертификатов, формирование служебных сообщений на рабочем месте пользователя, а также генерацию секретных и открытых ключей на рабочем месте пользователя и запись их на ключевые носители.

- VCrypt – программный модуль реализации криптографических функций и генерации ключевой информации (из состава СКЗИ "Верба-OW").

Цифровая подпись соответствует требованиям ГОСТ Р 34.10–94 "Информационная технология. Криптографическая защита информации. Система электронной

цифровой подписи на базе асимметричного криптографического алгоритма". Функция хэширования выполнена в соответствии с требованиями ГОСТ Р 34.11–94 "Информационная технология. Криптографическая защита информации. Функция хэширования", а алгоритм шифрования реализован в соответствии с требованиями ГОСТ 28147–89 "Системы обработки информации. Защита криптографическая".

Длины секретного и открытого ключей электронной цифровой подписи составляют соответственно 256 бит и 512 бит (или 1024 бита), такие же длины имеют секретный и открытый ключи шифрования. Секретные ключи подписи могут храниться на ключевых носителях – дискетах 3.5", носителях Touch-Memory или смарт-картах.

Система VCERT PKI обеспечивает:

- генерацию и верификацию электронных цифровых подписей под файлом или областью памяти в соответствии с ГОСТ Р34.10–94 и ГОСТ Р34.11–94;

- конфиденциальность и контроль целостности информации посредством ее шифрования и имитозащиты в соответствии с ГОСТ 28147–89;

- регистрацию электронных запросов пользователей на сертификаты открытых ключей подписи;

- формирование электронных сертификатов открытых ключей подписи пользователей.

Клиентское программное обеспечение VCERT PKI позволяет пользователям на своих рабочих местах формировать запросы на сертификаты открытых ключей, генерировать секретные и открытые ключи подписи и шифрования, а также получать сообщения о компрометации секретных ключей и информацию из справочника сертификатов.

Инструментарий разработчика дает возможность встраивать в прикладное программное обеспечение криптографические функции генерации/верификации цифровой подписи, шифрования/расшифрования информации. [12]

- ○ 1. СКЗИ КРИПТОПРО CSP

Средство криптографической защиты информации КриптоПро CSP, разработанное совместно компанией "Крипто-Про" и ФГУП "НТЦ "Атлас", реализовано в соответствии с криптографическим интерфейсом корпорации Microsoft – CSP

(Cryptographic Service Provider) и российскими криптографическими алгоритмами электронной цифровой подписи (ГОСТ Р34.10–94), шифрования и имитозащиты данных (ГОСТ 28147–89) и хэширования (ГОСТ Р34.11–94).

Программный комплекс Удостоверяющий центр – КриптоПро УЦ позволяет в полном объеме реализовать инфраструктуру открытых ключей.

В состав КриптоПро УЦ входят следующие компоненты:

- Центр сертификации (ЦС),

- Центр регистрации (ЦР),

- АРМ администратора ЦР,

- АРМ пользователя, программный интерфейс взаимодействия с УЦ.

Центр сертификации – базовый компонент системы. Он предназначен не только для формирования сертификатов открытых ключей пользователей и администраторов Удостоверяющего центра, но и для хранения эталонной базы сертификатов и списков аннулированных сертификатов. Центр сертификации взаимодействует только с Центром регистрации на базе защищенного сетевого протокола и реализован на платформе Microsoft Windows Server.

Центр регистрации также работает на платформе Microsoft Windows Server и использует базу данных Microsoft SQL. АРМ пользователя позволяет взаимодействовать пользователю с Удостоверяющим центром. ЦР является единственной точкой входа (регистрации) пользователей в системе. Только зарегистрированный пользователь может получить сертификат открытого ключа в Удостоверяющем центре.

Компонент АРМ Администратора ЦР обеспечивает выполнение организационно-технических мероприятий, которые связанны с регистрацией пользователей, генерацией ключей и сертификатов пользователей и взаимодействием с Центром регистрации. АРМ администратора ЦР функционирует в ОС Microsoft Windows. АРМ администратора взаимодействует с Центром регистрации в отдельном сегменте локальной сети на базе защищенного сетевого протокола.

АРМ администратора ЦР предназначен для проверки состояния и обработки запросов пользователей на регистрацию, выдачу и аннулирование сертификатов открытых ключей, а также на поиск информации в базе данных ЦР, на просмотр

протоколов работы ЦР.

АРМ пользователя – это web-приложение, которое размещается на сервере ЦР и функционирует в ОС Microsoft Windows. Он обеспечивает шифрование информации, передаваемой ЦР с использованием протокола TLS (протокол TLS обеспечивает конфиденциальность и целостность данных при коммутации двух приложений и позволяет приложениям "клиент-сервер" взаимодействовать защищенным способом, предотвращающим перехват информации и подделку сообщений).

Основные функции АРМ пользователя:

- обеспечивает взаимодействие пользователя с центром регистрации;

- позволяет заполнить формы запросов на сертификаты;

- позволяет выбрать тип сертификата;

- позволяет проверить состояние запросов на сертификаты и статус сертификатов;

- обеспечивает генерацию секретных ключей;

- обеспечивает получение сертификатов.

Программный интерфейс пользователя позволяет просмотреть персональную информацию из базы данных центра регистрации, список сертификатов, которые получены пользователем, а также запросы на сертификаты для загрузки, получения и аннулирования сертификатов.

Конфиденциальность, авторство и целостность информации достигается за счет интеграции средств криптографической защиты информации со средствами операционной системы и приложениями, с использованием инфраструктуры открытых ключей.

Применяя средство криптографической защиты информации КриптоПро CSP, пользователи операционной системы MS Windows могут воспользоваться стандартными программными средствами корпорации Microsoft для реализации решений, основанных на инфраструктуре открытых ключей. [12]

ЗАКЛЮЧЕНИЕ

В первом разделе данной курсовой работы были даны основные определения, касающиеся информации, защищаемой информации, криптологии, систем обработки информации, шифрования.

Защищаемая информация – это информация, которая является собственностью и должна быть защищена в соответствии с правовыми нормами и требованиями, устанавливаемыми собственником информации (физическим лицом, группой лиц, юридическим лицом или государством).

В настоящее время большие объемы важной информации хранятся, обрабатываются и передаются с использованием автоматизированных систем обработки информации в зашифрованном виде.

Шифрование - это процесс преобразования открытого текста в шифротекст с помощью определенных правил, содержащихся в шифре.

Во втором разделе была рассмотрена классификация угроз безопасности по общей направленности:

- угрозы конституционным правам и свободам граждан;

- угрозы развитию отечественной индустрии средств информатизации, телекоммуникаций и связи;

- угрозы безопасности информационных ресурсов, нормальному функционированию информационных и телекоммуникационных систем.

Также были рассмотрены меры противодействия угрозам безопасности:

- Законодательные меры;

- Морально-этические меры;

- Организационные меры;

- Технологические меры;

- Физические меры;

- Технические меры.

В третьем разделе данной курсовой работы изучены особенности современных средств криптографической защиты информации:

- СКЗИ Verba-OW;

- Программный комплекс VCERT PKI;

- СКЗИ КРИПТОПРО CSP.

В процессе выполнения курсовой работы решены следующие задачи:

1) даны определения основным понятиям – информация, угроза, информационная безопасность, аутентификация, идентификация, шифрование, средство криптографической защиты информации;

2) рассмотрены проблемы информационной безопасности;

3) рассмотрены классификацию угроз информационной безопасности;

4) изучены меры противодействия угрозам информационной безопасности;

5) изучены современные средства криптографической защиты.

Считаю, что все поставленные задачи курсовой работы, как теоретические, так и практические, решены, следовательно, главная цель исследования – достигнута.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск: Издательский центр ЮУрГУ, 2014. – 137 с.
2. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. — М. : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.
3. Борисова, С.Н. Методы и средства криптографической защиты данных в вычислительных системах. Часть 2 : Учебное пособие. – Пенза : Изд-во Пенз.гос. технол. акад., 2013. – 107 с.
4. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения безопасности: учебно-методический комплекс. – Москва: Проспект, 2015. – 152 с.
5. Введение в информационную безопасность: Учебное пособие для вузов / А. А. Малюк, В. С. Горбатов, В. И. Королев и др.; Под ред. В. С. Горбатова. − М.: Горячая линия – Телеком, 2011. – 288 с.

6. Галатенко В.А. Основы информационной безопасности: курс лекций: учебное пособие /Издание третье / Под ред. Академика РАН В.Б. Бетелина. – М.: ИНТУИТ.РУ, 2006. – 208 с.
7. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. – СПб: НИУ ИТМО, 2012. – 142 с.
8. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб:Университет ИТМО, 2018. – 100 с.
9. Девянин П.Н. Модели безопасности компьютерных систем: Учебное пособие для студ. высш. учеб. Заведений. – М.: Издательский центр «Академия», 2005. – 144 с.
10. Жданов, О. Н., Золотарев, В. В. Методы и средства криптографической защиты информации: Учебное пособие / О.Н. Жданов, В. В. Золотарев; СибГАУ. – Красноярск, 2007. – 217 с.
11. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.
12. Криптографическая защита информации : учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.
13. Куприянов А.И. Основы защиты информации: учеб. пособие для студ. Высш. Учеб. заведений. – М.: Издательский центр «Академия», 2006. – 256 с.
14. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
15. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие. Для студ. Учреждений высш. проф. образования; под ред. С.А. Клейменова. – 6-е изд., стер. – М.: Издательский центр «Академия», 2012, - 336 с.
16. Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.
17. Основы защиты информации: учебное пособие/ Шелупанов А.А, Зайцев А.П. и др./. – Изд. 5-е, перер. и доп. – Томск: В-Спектр, 2011. – 244 с.
18. Партыка Т. JL, Попов И. И. Информационная безопасность : учебное пособие / Т. Jl. Партыка, И. И. Попов. — 3-е изд., перераб. и доп. — М. : ФОРУМ, 2010. — 432 с.
19. Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. — СПб.: Питер, 2008. — 272 с.

20. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Гаудеамус, 2-е изд.— 2004. — 544 с.