Содержание:

ВВЕДЕНИЕ

Возникновение и развитие нового типа общества породило новые проблемы, а именно, проблемы обеспечения информационной безопасности.

Современные условия развития общества таковы, что компьютерные сети получили массовое распространение, сейчас уже никого не удивишь наличием компьютера дома, и тем более, в офисе. Однако подобное распространение информационных технологий привело к тому, что особенно острой стоит проблема обеспечения безопасности информации. Данная проблема весьма актуальна в наши дни, когда информация является одним из наиболее главных ресурсов современной экономики.

Мероприятия по обеспечению безопасности информации направлены, в первую очередь, на предотвращение несанкционированного доступа к информации, уничтожения, изменения, хищения информации.

Для того, чтобы идти в ногу со временем и быть защищенным от угроз важной информации предприятие должно соблюдать ряд следующих принципов:

Необходимо постоянно проводить обучающие мероприятия среди сотрудников, целью которых состоит донесение правил соблюдения конфиденциальности, режима коммерческой тайны на предприятии, воспитание ответственности к исполняемым обязанностям в части соблюдения конфиденциальности важной информации о деятельности предприятия.

Использование технических средств защиты, которые прошли технические испытания, аттестацию. Только в такой случае они могут гарантировать эффект в обеспечении информационной безопасности.

Борьба с текучестью кадров, которые владеют коммерческой тайной. Необходимо создавать самые благоприятные, в пределах разумного, условия для нормальной работы людей. В случае, если все таки увольнения избежать не удается, то расставаться с сотрудником необходимо в доброжелательном тоне.

То есть, из этого можно заключить, что угрозы информационной безопасности всегда легче предупредить, чем потом бороться с их последствиями.

Вышесказанное и определяет актуальность выбранной темы курсовой работы для исследования «Виды и состав угроз информационной безопасности».

Цель исследования состоит в исследовании видов угроз информационной безопасности, а также в анализе методов борьбы с угрозами информационной безопасность.

Для достижения данной цели необходимо решение следующих **задач:**

1) Рассмотреть сущность понятия информационной безопасности и ее угроз.

2) Рассмотреть виды угроз информационной безопасности и их источники.

3) Оценить преимущества физических методов борьбы с угрозой конфиденциальности информации.

4) Дать анализ криптографическим методам борьбы с угрозами целостности и доступности информации.

Объектом исследования является угроза информационной безопасности.

Предметом исследования является исследование методов борьбы и предотвращения угроз информационной безопасности предприятия.

Работа состоит из введения, двух глав («Теоретическая сущность информационной безопасности и состав ее угроз», «Анализ методов борьбы с угрозами информационной безопасности»), заключения и библиографии.

ГЛАВА 1. Теоретическая сущность информационной безопасности и состав ее угроз

1.1.Понятие информационной безопасности и ее угроз

Защита информации личного или производственного назначения занимает важное место в современной системе обеспечения безопасности. Ведь мировое сообщество вступило в такую фазу развития, где наиболее ценным ресурсом является информация во всех ее проявлениях. Информация является довольно специфическим ресурсом, которая не имеет материально выраженной формы. Однако нужная информация может помочь достичь небывалых успехов, может заставить человека опуститься «на дно», может помочь, а может и навредить. Информация может обладать уникальной ценностью, но становится ненужной, если нарушается ее конфиденциальность.

Особенностью информации является ее уязвимость. Вот почему обеспечение информационной безопасности является очень актуальной проблемой в наши дни.

Угроз безопасности информационных ресурсов предприятия много – это и компьютерные вирусы, которые могут уничтожить важные данные, и промышленный шпионаж со стороны конкурентов преследующих своей целью получение незаконного доступа к информации, представляющей коммерческую тайну, и много другое[1]. Поэтому особое место приобретает деятельность по защите информации, по обеспечению информационной безопасности[2].

Определение информационной безопасности звучит следующим образом.

Информационная безопасность (англ. «Information security») [3] – защищенность информации и соответствующей инфраструктуры от случайных или преднамеренных воздействий сопровождающихся нанесением ущерба владельцам или пользователям информации. Информационная безопасность – обеспечение конфиденциальности, целостности и доступности информации.

Целью защиты информации от несанкционированного вторжения состоит в том, чтобы сделать важную информацию недоступной для заинтересованных пользователей, независимо от того, преследуют ли они злой умысел, либо ими движет простое любопытство. В случае, если первая цель не достигнута, то тогда цель информационной безопасности направлена на то, чтобы минимизировать потери, которые могут быть вызваны нарушением целостности и конфиденциальности информативных данных.

Информационная безопасность – это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю[4].

Далее рассмотрим структуру проблем информационной безопасности. Итак, информационная безопасность включает в себя три направления: защиту информации, защиту от информации, добывание информации о потенциальных угрозах[5].

Защита информации в основном достигается при помощи технических средств.

Защита от информации достигается при помощи средств организационно-технического характера.

Добывание информации о потенциальных угрозах возможно посредством работы с человеком[6].

Структуру информационной безопасности рассмотрим в виде блок схемы.

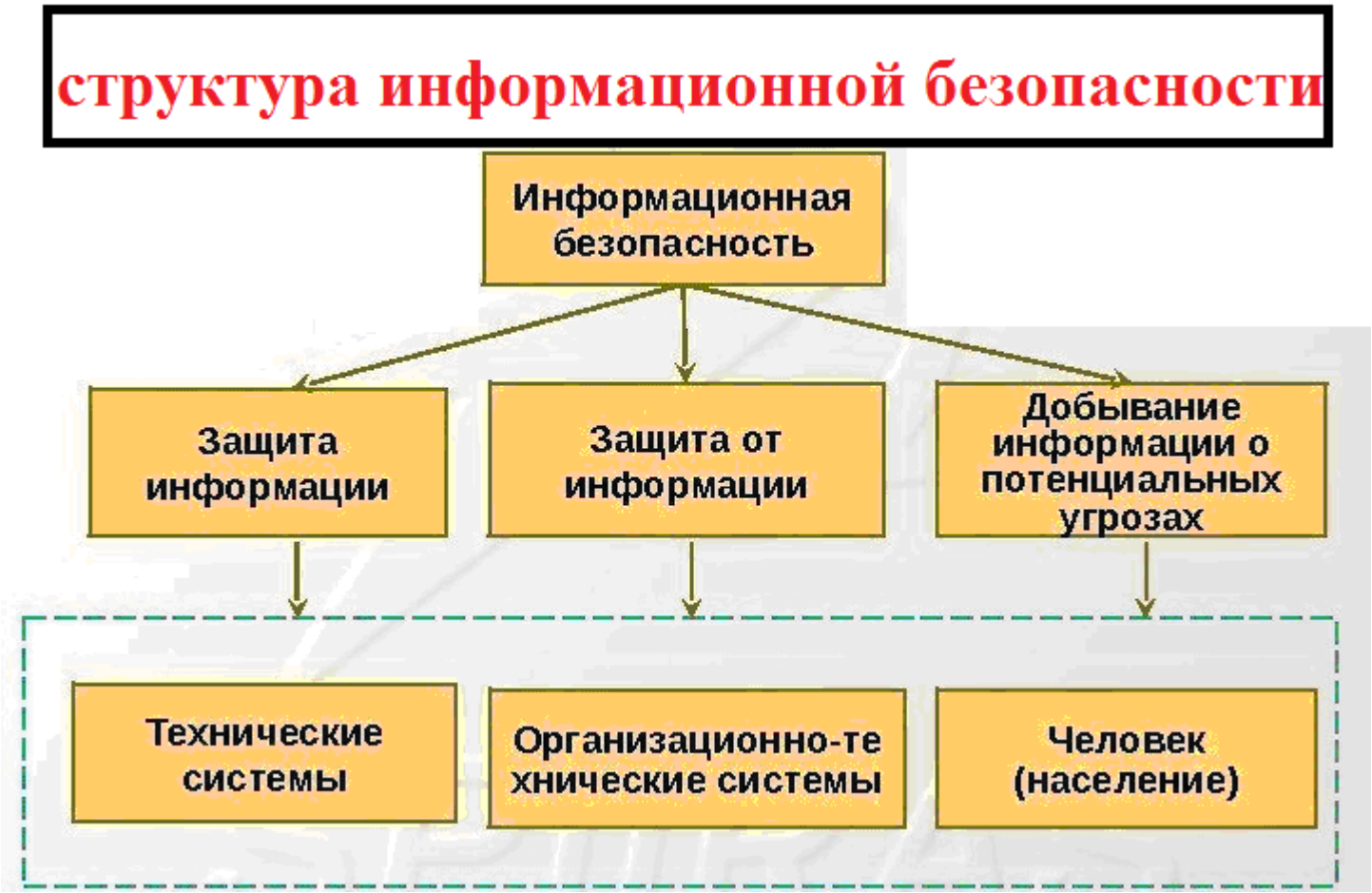

Рисунок 1. Структура информационной безопасности

Рассмотрим основные принципы информационной безопасности[7].

1. Целостность данных - такое свойство, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Создавать, уничтожать или изменять данные может только пользователь, имеющий право доступа[8].

2. Конфиденциальность — свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц.

Конфиденциальность информации гарантирует то, что в процессе обработки и передачи информации она останется доступной только тем пользователям, которые имеют право на доступ к ней.

3. Доступность информации - это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации[9].

4. Достоверность – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

Таким образом, обеспечение информационной безопасности направлено на предотвращение угроз целостности, доступности и конфиденциальности информации. Система защиты информации подразумевает целый комплекс мероприятий, направленных на предотвращение несанкционированного доступа со стороны недобросовестных пользователей. Также система защиты информации направлена на то, чтобы предотвратить действия по незаконному использованию, повреждению, искажению, копированию, блокированию информации[10].

Вопросы информационной безопасности становятся первоочередными в тех случаях, когда выход из строя или возникновение ошибки в конкретной компьютерной системе могут привести к тяжелым последствиям[11].

В заключении раздела можно прийти к следующим выводам:

- защита информации личного или производственного назначения занимает важное место в современной системе обеспечения безопасности. Особенностью информации является ее уязвимость. Вот почему обеспечение информационной безопасности является очень актуальной проблемой в наши дни.

- информационная безопасность представляет собой степень защищенности информации от случайного и преднамеренного доступа к ней, который является

несанкционированным. Информационная безопасность предполагает обеспечение конфиденциальности, целостности и доступности информации.

- целью защиты информации от несанкционированного вторжения состоит в том, чтобы сделать важную информацию недоступной для заинтересованных пользователей, независимо от того, преследуют ли они злой умысел, либо ими движет простое любопытство. В случае, если первая цель не достигнута, то тогда цель информационной безопасности направлена на то, чтобы минимизировать потери, которые могут быть вызваны нарушением целостности и конфиденциальности информативных данных.

- были рассмотрены основные принципы информационной безопасности: это конфиденциальность, доступность, целостность и достоверность данных.

- были рассмотрены проблемы информационной безопасности, включающие в себя три направления: защиту информации, защиту от информации, добывание информации о потенциальных угрозах.

1.2.Виды угроз информационной безопасности и их источники

Угроза информационной безопасности предполагает возможность влияния на автоматизированную систему, результатом которой может стать нанесение моральное и материального ущерба собственникам данной автоматизированной системы и информации, находящейся в ней.

Рассмотрим виды угроз информационной безопасности, которые разделены согласно различным классификационным признакам[12].

1) По рангу преднамеренности выражения:

-угрозы, спровоцированы ошибками или небрежностью сотрудников, например неграмотное использование методов защиты, ввод не верных данных и т.п.;

-угрозы преднамеренного влияния, например методы мошенников.

2) По характеру возникновения:

-искусственные угрозы безопасности автоматизированных систем, вызванные руками человека.

-природные угрозы, созданные воздействиями на автоматизированные системы объективных физических действий или стихийных природных явлений[13];

3) По непосредственной причине угроз:

- человек, к примеру, нанятые путем подкупа сотрудников, выбалтывание конфиденциальной информации и т.п.; [14];

- форс – мажорные обстоятельства природного стихийного характера;

- несанкционированные программно-аппаратные фонды, например заражение ПК вирусами с разрушающими функциями;

- санкционированные программно-аппаратные фонды, отказ в работе, к примеру, удаление данных.

4) По степени зависимости от активности автоматизированной системы:

-только в ходе обработки данных, к примеру, угрозы реализации и рассылке программных вирусов;

-независимо от активности автоматизированной системы, к примеру, вскрытие шифров[15].

Рассмотрим классификацию угроз информационной безопасности в виде рисунка.

Рисунок 2. Виды угроз информационной безопасности

Угроза информационной безопасности не появляется из ниоткуда. Она всегда идет от источника угроз информации.

1) В зависимости от состояния источника угроз выделяют:

- угрозы, возникшие непосредственно в автоматизированной системе. Например, неточная реализация ресурсов автоматизированной системы.

- угрозы, которые возникли в пределах автоматизированной системы. Например, установка подслушивающих, пишущих устройств, хищение носителей данных и прочее.

- угрозы, которые возникли вне зоны автоматизированной системы. Примером может послужить захват информации, которая передается по путям связи, перехват электромагнитных излучений.

2) В зависимости от степени воздействия различают следующие виды угроз:

- активные угрозы, которые при реакции вносят изменения и модифицированной автоматизированной системы, к примеру, ввод вирусов и троянских коней;

- пассивные угрозы, которые при исполнении не модифицируют и не изменяют автоматизированной системы, к примеру, угроза копирования секретной информации.

3) В зависимости от способа пути к ресурсам автоматизированной системы.

- угрозы, реализуемые с использованием маскированного нестандартного каналу пути к ресурсам автоматизированной системы, к примеру, несанкционированный путь к ресурсам автоматизированной системы путем использования каких либо возможностей;

- угрозы, реализуемые с использованием стандартного каналу доступа к ресурсам АС, к примеру, незаконное обретение паролей и других параметров разграничения доступа с последующей маскировкой под зарегистрированного сотрудника[16].

4) В зависимости от шагов доступа сотрудников или программ к ресурсам.

- угрозы, которые реализуются после согласия на доступ к ресурсам автоматизированной системы. Например, это может быть угроза некорректного и несанкционированного применения ресурсов автоматизированной системы[17];.

- угроза, которая реализуется на шаге доступа к ресурсам автоматизированной системы. Например, это угроза несанкционированного доступа к ресурсам автоматизированной системы.

5) В зависимости от места размещения информации, которая хранится в данной автоматизированной системе, различают:

- угрозы проходу к информации, которая находится внутри программных аппаратных средств.

- угрозу проходу информации, которые находятся на внешних носителях.

- угрозы проходу к информации, видимой на терминале, например запись отображаемых данных на видеокамеру;

- угрозы проходу к информации, проходящих в каналах связи, например незаконное подсоединение к каналам связи с задачей прямой подмены законного сотрудника с следующим вводом дезинформации и навязыванием ложных данных, незаконное подсоединение к каналам связи с следующим вводом ложных данных или модификацией передаваемых данных[18].

Угрозы информационной безопасности также делят на случайные и преднамеренные.

Источниками случайных угроз выступают различные сбои в работе аппаратуры, безответственность работников, форс- мажорные обстоятельства природного стихийного характера и прочие.

Преднамеренные угрозы всегда направлены на достижение целей преступника. Поэтому, угрозы преднамеренной атаки на информацию всецело и неразрывно связаны с намерениями злоумышленника.

Методы преступника могут быть объяснены следующими факторами: конкурентной борьбой, любопытством, недовольством сотрудника своей карьерой, материальным интересом (взятка), стремлением самоутвердиться любыми методами и т.п. [19];

Делая вывод из вероятности становление наиболее опасных условий, обусловленной методами злоумышленника, можно прикинуть гипотетическую модель потенциального злоумышленника:

-злоумышленнику известны данные о методах и параметрах работы системы;

-квалификация злоумышленника может позволять делать несанкционированные действия на уровне разработчика;

- злоумышленник может выбрать наиболее слабое место в системе защите;

- злоумышленником может быть кто угодно, как и законный пользователь системы, так и постороннее лицо[20].

В заключении раздела можно сделать следующие выводы:

- угроза информационной безопасности предполагает возможность влияния на автоматизированную систему, результатом которой может стать нанесение моральное и материального ущерба собственникам данной автоматизированной системы и информации, находящейся в ней.

- были рассмотрены основные виды угроз информационной безопасности.

- были рассмотрены виды источников угроз в зависимости от видов угроз информационной безопасности.

- для того, чтобы достичь необходимый уровень информационной безопасности на предприятии необходимо создать мощную систему защиты информации. Необходимо реализовать противодействие информационным угрозам, как можно более снизить влияние человеческого фактора. На предприятии данные мероприятия должны реализовываться специальной службой безопасности, которая разрабатывает политику безопасности, в том числе и информативных технологий предприятия.

Выводы по главе 1.

В первой главе данной работы была раскрыта теоретическая сущность информационной безопасности и состав ее угроз.

- защита информации личного или производственного назначения занимает важное место в современной системе обеспечения безопасности. Особенностью информации является ее уязвимость. Вот почему обеспечение информационной безопасности является очень актуальной проблемой в наши дни.

- информационная безопасность представляет собой степень защищенности информации от случайного и преднамеренного доступа к ней, который является несанкционированным. Информационная безопасность предполагает обеспечение конфиденциальности, целостности и доступности информации.

- целью защиты информации от несанкционированного вторжения состоит в том, чтобы сделать важную информацию недоступной для заинтересованных пользователей, независимо от того, преследуют ли они злой умысел, либо ими движет простое любопытство. В случае, если первая цель не достигнута, то тогда цель информационной безопасности направлена на то, чтобы минимизировать потери, которые могут быть вызваны нарушением целостности и конфиденциальности информативных данных.

- были рассмотрены основные принципы информационной безопасности: это конфиденциальность, доступность, целостность и достоверность данных.

- были рассмотрены проблемы информационной безопасности, включающие в себя три направления: защиту информации, защиту от информации, добывание информации о потенциальных угрозах.

- угроза информационной безопасности предполагает возможность влияния на автоматизированную систему, результатом которой может стать нанесение

моральное и материального ущерба собственникам данной автоматизированной системы и информации, находящейся в ней.

- были рассмотрены основные виды угроз информационной безопасности.

- были рассмотрены виды источников угроз в зависимости от видов угроз информационной безопасности.

- для того, чтобы достичь необходимый уровень информационной безопасности на предприятии необходимо создать мощную систему защиты информации. Необходимо реализовать противодействие информационным угрозам, как можно более снизить влияние человеческого фактора. На предприятии данные мероприятия должны реализовываться специальной службой безопасности, которая разрабатывает политику безопасности, в том числе и информативных технологий предприятия.

ГЛАВА 2. Анализ методов борьбы с угрозами информационной безопасности

2.1 Преимущества физических методов борьбы с угрозой конфиденциальности информации

Угрозы информационной безопасности необходимо пресекать для того, чтобы избежать пагубных последствий несанкционированного вторжения в конфиденциальную информацию. Существуют разные методы борьбы с угрозами информационной безопасности, которые призваны защитить информацию.

Особое внимание необходимо уделить анализу преимуществ физических методов борьбы с угрозами конфиденциальности информации.

Рассмотрим в виде рисунка физические методы защиты конфиденциальности информации.

Рисунок 3. Физические методы борьбы с угрозой конфиденциальности информации

Физические средства защиты - это разного рода механические, электронно-механические устройства, специально предназначенные для образования физических препятствий на возможных путях проникновения и доступа возможных нарушителей к компонентам автоматической системы и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации[21].

Физическая безопасность связана с введением мер защиты, которые защищают от стихийных бедствий, например, таких как пожар, наводнение, ураган, землетрясение[22].

Таким образом, можно отметить, что физические средства защиты информации представляют собой устройства и аппараты различной модификации и конфигурации, которые преследуют цель воспрепятствовать недобросовестным действиям злоумышленникам.

Это могут быть средства механического, электромеханического, радиотехнического и электрического характера и назначения. Они устроены таким образом, что препятствуют доступ к информации преступника, а также препятствуют выноса материальных средств носителей информации.

Физические средства борьбы с угрозами конфиденциальности информации призваны решить следующие цели:

-охрана территории предприятия и наблюдение за ней;

-охрана зданий, внутренних помещений и контроль их;

-охрана оборудования, продукции, финансов и информации;

-осуществление контролируемого доступа в здания и помещение[23].

Все физические средства защиты объектов можно разделить на три категории:

-средства предупреждения,

-средства обнаружения

-системы ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

-охранные и охранно-пожарные системы;

-охранное телевидение;

-охранное освещение;

-средства физической защиты.

К средствам физической защиты относятся:

-ограждение и физическая изоляция,

-запирающие устройства,

-системы контроля доступа[24].

К системам контроля доступа относятся:

-системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце,

-системы опознавания по отпечаткам пальцев,

-системы опознавания по голосу,

-системы опознавания по почерку,

-система опознавания по геометрии рук[25].

Также следует отметить, что для достижения наилучшего результата все вышеуказанные средства должны работать в комплексе. Только в таком случае

можно говорить о каком - то положительном эффекте в достижении целей обеспечения информационной безопасности.

Особое внимание следует уделить защите рабочего места лица, который владеет доступом к конфиденциальной информации. Высокий уровень защиты можно обеспечить также при помощи физических средств защиты.

При организации рабочего места данного сотрудника необходимо строго придерживаться некоторых правил.

1) На рабочем месте должно быть установлено только самое необходимое оборудование, которое жизненно необходимо для реализации должностных обязанностей данного сотрудника. Ничего лишнего из аппаратуры быть не должно, так как избыточное количество различной аппаратуры повышает в раз риск несанкционированного проникновения по различным каналам связи.

2) Установка всего оборудования и элементов интерьера должна предельно затруднять их перемещение и замену или внедрение посторонних предметов.

На случай, если нарушение размещения, замена или внедрение нового предмета произойдет, должны быть приняты меры, делающие это изменение выявляемым, и определены действия, следующие за таким выявлением[26].

3) Должны быть созданы такие рабочие условия, которые максимальным образом затруднят потенциальное наблюдение за рабочим процессом сотрудника со стороны преступника. Также необходимо создать наиболее трудные условия для наблюдения со стороны преступника и за системой аппаратуры защиты информации.

Несмотря на простоту предлагаемых вариантов действий, к данной проблеме необходимо подойти с тщательным анализом и контролем.

Особую эффективность при обеспечении защиты информации физическими методами имеет защита по периметру.

Любая физическая система защиты по периметру должна отвечать и соответствовать следующим требованиям.

1)Возможность раннего обнаружения нарушителя — еще до его проникновения на объект. Это обеспечивается камерами наблюдения и постоянным мониторингом.

2) Строгая проверка точно по периметру, избегания возникновения так называемых «мертвых зон».

3) Скрытая установка датчиков системы.

4) Независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т.д.), то есть отсутствие влияния фактора форс – мажорных обстоятельств. [27]

5) Невосприимчивость к факторам внешней среды.

6) Устойчивость к электромагнитным помехам — грозовые разряды, источники мощных электромагнитных излучений и т.п. [28]

Таким образом, можно отметить, что система охраны по периметру должна обладать высочайшим уровнем чувствительности. Наряду с этим, данная система должна обеспечивать низкий уровень вероятности ложных срабатываний. Ложные тревоги могут быть вызваны самыми различными факторами. Более того, преступник может иногда и провоцировать ложные тревоги, чтобы усыпить бдительность охранников.

Необходимо отметить, что любая система защиты по периметру должна легко и качественно интегрироваться с другими система защиты, особенно с системой видеонаблюдения на предприятии или другом объекте. [29]

В заключении раздела можно сделать следующие выводы:

- были рассмотрены физические методы защиты и борьбы с угрозами конфиденциальности информации.

- физические средства защиты информации представляют собой устройства и аппараты различной модификации и конфигурации, которые преследуют цель воспрепятствовать недобросовестным действиям злоумышленникам.

- необходимо тщательно исследовать рабочее место на предмет доступности и потенциального наблюдения к нему со стороны злоумышленника.

- особую эффективность при обеспечении защиты информации физическими методами имеет защита по периметру. Система охраны по периметру должна обладать высочайшим уровнем чувствительности. Наряду с этим, данная система должна обеспечивать низкий уровень вероятности ложных срабатываний. Ложные

тревоги могут быть вызваны самыми различными факторами. Более того, преступник может иногда и провоцировать ложные тревоги, чтобы усыпить бдительность охранников.

- физические системы защиты должны легко и качественно интегрироваться с другими система защиты.

2.2 Анализ криптографических методов борьбы с угрозой целостности и доступности информации

В борьбе с угрозой целостности и сохранности информации особое место следует выделить криптографическим методам защиты. Криптография, как форма ее зарождения, была известна еще избранным древнего Египта. Криптография – это специальный набор шифра, который определенным образом засекречивает необходимую информацию.

Криптографические методы защиты информации — это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования[30].

Следует отметить, что криптографический метод защиты является самым надежным методом защиты, так как охраняется именно сама информация, а не доступ к ней. То есть, если даже и злоумышленник сможет взломать защиту на доступе к информации, он все равно не сможет воспользоваться данной информацией. Так как данная информация защищена криптографическим шифрованием. Криптографический метод защиты можно реализовать посредством специального набора и пакета программных средств[31].

Криптография призвана решить следующие задачи:

1) Обеспечить конфиденциальность данных. Это одна из основных задач криптографии, для ее решения применяется шифрование данных, т.е. такое их преобразование, при котором прочитать их могут только законные пользователи, обладающие соответствующим ключом.

2) Обеспечение целостности данных— гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это

права. Под модификацией понимается вставка, удаление или подмена информации, а также повторная пересылка перехваченного ранее текста.

3) Обеспечение аутентификации. Под аутентификацией понимается проверка подлинности субъектов (сторон при обмене данными, автора документов, и т.д.) или подлинности самой информации. Во многих случаях субъект X должен не просто доказать свои права, но сделать это так, чтобы проверяющий субъект (Y) не смог впоследствии сам использовать полученную информацию для того, чтобы выдать себя за X. Подобные доказательства называются «доказательствами с нулевым разглашением».

4) Обеспечение невозможности отказа от авторства— предотвращение возможности отказа субъектов от совершенных ими действий (обычно — невозможности отказа от подписи под документом). Эта задача неотделима от двойственной — обеспечение невозможности приписывания авторства[32].

Самым ярким примером реализации данной задачи является применение цифровой или электронной подписи. Рассмотрим ситуацию. В подписании договора участвуют два или группа лиц, которые не доверяют друг другу и сомневаются в добросовестности каждого. Каждая сторона, которая подписывает контракт или договор, должна быть уверена в том, что подпись контрагента будет подлинна, и что в будущем он не откажется от того, что это подпись его, и она является подлинной. Для этого используется цифровая подпись.

Современная криптография включает в себя четыре крупных раздела:

1)Симметричные криптосистемы. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. Шифрование представляет собой следующий процесс. Исходный текст, который носит название открытого текста, преобразовывается в набор шифрованного текста. Соответственно, дешифрование представляет собой обратный процесс, который подразумевает преобразование шифрованного текста в исходный текст. Данные процессы реализовываются при помощи одного ключа. Ключ представляет собой информацию, с помощью которой можно либо зашифровать, либо расшифровать информацию. Зная ключ, при помощи которого можно зашифровать текст, без труда можно его и расшифровать.

2) Криптосистемы с открытым ключом. Криптосистема с открытым ключом предполагает использование двух ключей открытого и закрытого. Данные ключи

связаны друг с другом математическими связями. Информация шифруется при помощи открытого ключа. Открытый ключ имеется в свободном доступе всем желающим. А расшифровывается информация при помощи закрытого ключа, которым обладает тот, кому данная информация непосредственно адресована.

3) Электронная подпись. Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения[33].

4) Управление ключами. Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями[34].

Основное направление использования криптографического метода состоит в том, чтобы передавать, сохраняя целостность и конфиденциальность, информацию соответствующему получателю. Также криптографические методы защиты используются тогда, когда необходимо сохранить важную информацию, установить подлинность информации.

Процесс криптографического закрытия данных может осуществляться 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 более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования[35]:

-зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

-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);

-знание алгоритма шифрования не должно влиять на надежность защиты;

-незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа [36];

-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 шифрованного текста должна быть равной длине исходного 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.

В заключении раздела можно прийти к следующим выводам:

- были рассмотрены криптографические методы борьбы с угрозами целостности и доступности информации.

- криптографический метод защиты является самым надежным методом защиты, так как охраняется именно сама информация, а не доступ к ней. То есть, если даже и злоумышленник сможет взломать защиту на доступе к информации, он все равно не сможет воспользоваться данной информацией. Так как данная информация защищена криптографическим шифрованием.

Выводы по главе 2.

Во второй главе данной работы были проанализированы основные методы борьбы с угрозами информационной безопасности.

- были рассмотрены физические методы защиты и борьбы с угрозами конфиденциальности информации.

- физические средства защиты информации представляют собой устройства и аппараты различной модификации и конфигурации, которые преследуют цель воспрепятствовать недобросовестным действиям злоумышленникам.

- необходимо тщательно исследовать рабочее место на предмет доступности и потенциального наблюдения к нему со стороны злоумышленника.

- особую эффективность при обеспечении защиты информации физическими методами имеет защита по периметру. Система охраны по периметру должна обладать высочайшим уровнем чувствительности. Наряду с этим, данная система должна обеспечивать низкий уровень вероятности ложных срабатываний. Ложные тревоги могут быть вызваны самыми различными факторами. Более того, преступник может иногда и провоцировать ложные тревоги, чтобы усыпить бдительность охранников.

- физические системы защиты должны легко и качественно интегрироваться с другими система защиты.

- были рассмотрены криптографические методы борьбы с угрозами целостности и доступности информации.

- криптографический метод защиты является самым надежным методом защиты, так как охраняется именно сама информация, а не доступ к ней. То есть, если даже и злоумышленник сможет взломать защиту на доступе к информации, он все равно не сможет воспользоваться данной информацией. Так как данная информация защищена криптографическим шифрованием.

- были рассмотрены основные задачи криптографических методов защиты информации.

ЗАКЛЮЧЕНИЕ

В заключении данной курсовой работы следует отметить следующие выводы:

В первой главе данной работы была раскрыта теоретическая сущность информационной безопасности и состав ее угроз.

- защита информации личного или производственного назначения занимает важное место в современной системе обеспечения безопасности. Особенностью

информации является ее уязвимость. Вот почему обеспечение информационной безопасности является очень актуальной проблемой в наши дни.

- информационная безопасность представляет собой степень защищенности информации от случайного и преднамеренного доступа к ней, который является несанкционированным. Информационная безопасность предполагает обеспечение конфиденциальности, целостности и доступности информации.

- целью защиты информации от несанкционированного вторжения состоит в том, чтобы сделать важную информацию недоступной для заинтересованных пользователей, независимо от того, преследуют ли они злой умысел, либо ими движет простое любопытство. В случае, если первая цель не достигнута, то тогда цель информационной безопасности направлена на то, чтобы минимизировать потери, которые могут быть вызваны нарушением целостности и конфиденциальности информативных данных.

- были рассмотрены основные принципы информационной безопасности: это конфиденциальность, доступность, целостность и достоверность данных.

- были рассмотрены проблемы информационной безопасности, включающие в себя три направления: защиту информации, защиту от информации, добывание информации о потенциальных угрозах.

- угроза информационной безопасности предполагает возможность влияния на автоматизированную систему, результатом которой может стать нанесение моральное и материального ущерба собственникам данной автоматизированной системы и информации, находящейся в ней.

- были рассмотрены основные виды угроз информационной безопасности.

- были рассмотрены виды источников угроз в зависимости от видов угроз информационной безопасности.

- для того, чтобы достичь необходимый уровень информационной безопасности на предприятии необходимо создать мощную систему защиты информации. Необходимо реализовать противодействие информационным угрозам, как можно более снизить влияние человеческого фактора. На предприятии данные мероприятия должны реализовываться специальной службой безопасности, которая разрабатывает политику безопасности, в том числе и информативных технологий предприятия.

Во второй главе данной работы были проанализированы основные методы борьбы с угрозами информационной безопасности.

- были рассмотрены физические методы защиты и борьбы с угрозами конфиденциальности информации.

- физические средства защиты информации представляют собой устройства и аппараты различной модификации и конфигурации, которые преследуют цель воспрепятствовать недобросовестным действиям злоумышленникам.

- необходимо тщательно исследовать рабочее место на предмет доступности и потенциального наблюдения к нему со стороны злоумышленника.

- особую эффективность при обеспечении защиты информации физическими методами имеет защита по периметру. Система охраны по периметру должна обладать высочайшим уровнем чувствительности. Наряду с этим, данная система должна обеспечивать низкий уровень вероятности ложных срабатываний. Ложные тревоги могут быть вызваны самыми различными факторами. Более того, преступник может иногда и провоцировать ложные тревоги, чтобы усыпить бдительность охранников.

- физические системы защиты должны легко и качественно интегрироваться с другими система защиты.

- были рассмотрены криптографические методы борьбы с угрозами целостности и доступности информации.

- криптографический метод защиты является самым надежным методом защиты, так как охраняется именно сама информация, а не доступ к ней. То есть, если даже и злоумышленник сможет взломать защиту на доступе к информации, он все равно не сможет воспользоваться данной информацией. Так как данная информация защищена криптографическим шифрованием.

БИБЛИОГРАФИЯ

1. «Гражданский кодекс Российской Федерации» от 30 ноября 1994 года N 51-ФЗ.

2. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017).

3. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ.

4. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

5. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.

6. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.

7. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.

8. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с.

9. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

10. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. - 392 с.

11. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. - 256 с.

12. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.

13. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

14. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

15. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. - 352 с.

16. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.

17. Криптографические способы защиты - [онлайн] URL: https://www.ronl.ru/stati/gosudarstvo-i-pravo/720005/

ПРИЛОЖЕНИЕ 1

Рисунок. Физические методы борьбы с угрозой конфиденциальности информации

ПРИЛОЖЕНИЕ 2

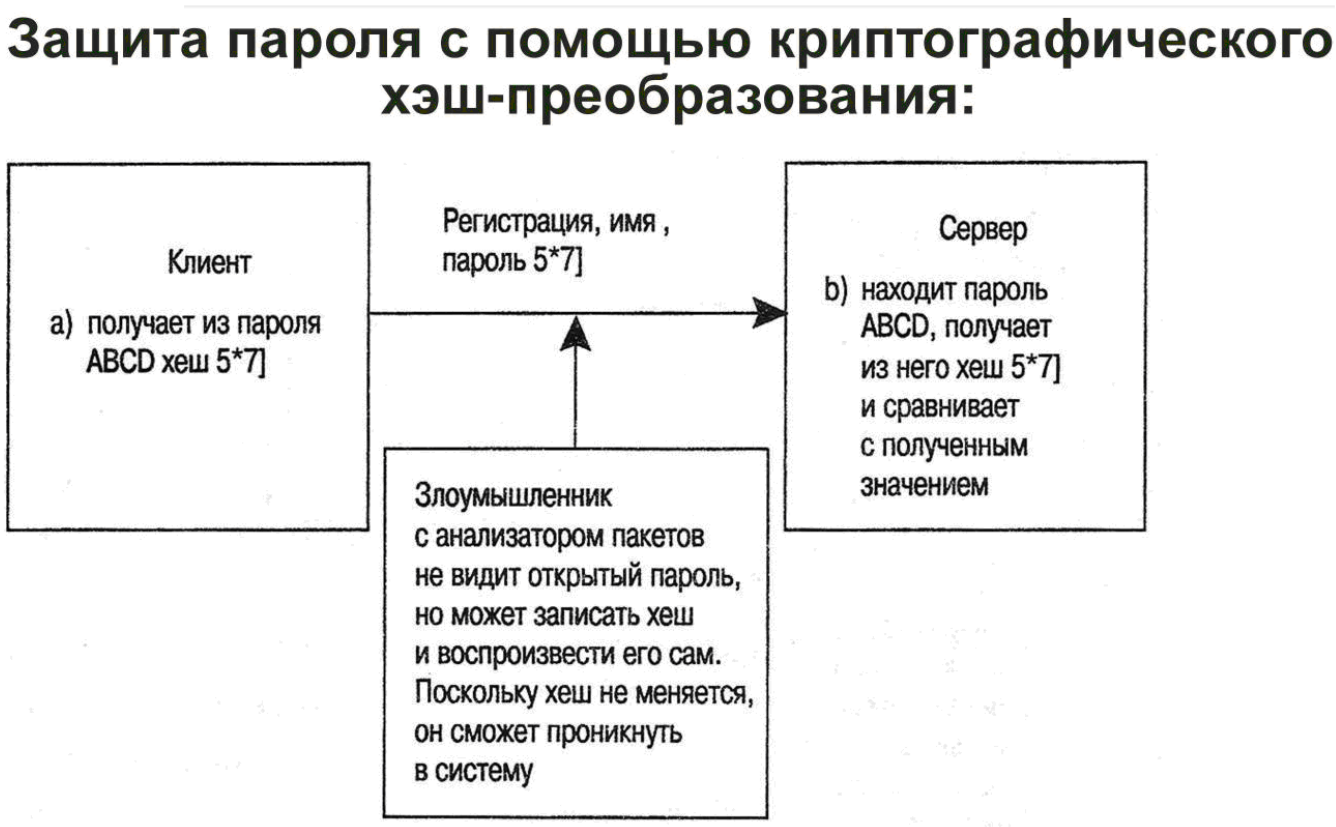

Рисунок. Использование криптографических методов

1. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. – С. 105. ↑

2. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. – С. 205. ↑

3. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. – С. 456. ↑

4. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. – С. 205. ↑

5. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. – С. 105. ↑

6. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. – С. 456. ↑

7. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. – С. 205. ↑

8. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. – С. 105. ↑

9. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. – С. 456. ↑

10. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. – С. 205. ↑

11. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. – С. 105. ↑

12. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. – С. 153. ↑

13. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с. ↑

14. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с. ↑

15. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. – С. 153. ↑

16. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. – С. 153. ↑

17. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с. ↑

18. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. – С. 153. ↑

19. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с. ↑

20. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. – С. 153. ↑

21. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. – С. 230. ↑

22. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. – С. 250. ↑

23. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. – С. 230. ↑

24. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. – С. 250. ↑

25. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. – С. 230. ↑

26. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. – С. 230. ↑

27. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. – С. 230. ↑

28. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. – С. 250. ↑

29. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. – С. 250. ↑

30. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. – С. 265. ↑

31. Криптографические способы защиты - [онлайн] URL: https://www.ronl.ru/stati/gosudarstvo-i-pravo/720005/ ↑

32. Криптографические способы защиты - [онлайн] URL: https://www.ronl.ru/stati/gosudarstvo-i-pravo/720005/ ↑

33. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. – С. 265. ↑

34. Криптографические способы защиты - [онлайн] URL: https://www.ronl.ru/stati/gosudarstvo-i-pravo/720005/ ↑

35. Криптографические способы защиты - [онлайн] URL: https://www.ronl.ru/stati/gosudarstvo-i-pravo/720005/ ↑

36. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. – С. 265. ↑