Содержание:

ВВЕДЕНИЕ

Информация представляет собой результат отображения и обработки в человеческом сознании разнообразия окружающего мира, сведения об окружающих человека предметах, природных явлений, деятельности других людей. информационный безопасность угроза

Под защитой информации сейчас понимается сфера науки и техники, включающая комплекс средств, методов и способов человеческой деятельности, ориентированных на достижение защиты всех форм информации на предприятиях разных направлений деятельности и форм собственности.

Информация, которую необходимо защищать, способна быть представлена на разных носителях, способна храниться, обрабатываться и передаваться разнообразными способами и средствами.

Целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым данным; предотвращение противоправных действий по уничтожению, изменению, искажению, копированию, блокированию информации; предотвращение иных видов незаконного вмешательства в информационные ресурсы и системы; формирование правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, находящихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации; реализация прав субъектов в информационных процессах и при разработке, производстве и использовании информационных систем, технологии и средств их обеспечения.

Информационная безопасность - это положение защищенности информационной среды общества, реализующее применение информации в интересах граждан, предприятий, государств.

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности. Для эффективного противодействия угрозам информационной безопасности надо в полной мере знать их виды и состав. Это и актуализирует тему данной курсовой работы.

Цель курсовой работы заключается в исследовании видов угроз информационной безопасности и их состава.

Для реализации поставленной цели необходимо выполнить ряд задач, а именно:

- рассмотреть теоретические аспекты исследования видов угроз информационной безопасности;

- разработать план внедрения программно-аппаратного средства защиты информации от несанкционированного доступа «Secret Net LSP».

Предметом исследования курсовой работы является информационная безопасность.

Объектом исследования курсовой работы являются угрозы информационной безопасности.

Структура курсовой работы состоит из введения, двух глав – теоретической и практической, заключения, списка использованной литературы.

Глава 1. Теоретические аспекты исследования видов угроз информационной безопасности

1.1. Понятие и структура угроз защищаемой информации

Есть три разных подхода в определении угроз, включающие следующее:

1. Угроза понимается как возможно существующая ситуация (вероятность, опасность) нарушения безопасности информации, в данном случае безопасность информации означает, что информация состоит в защищённом виде, способном противодействовать всяким дестабилизирующим влияниям;

2. Угроза понимается как явление (событие, случай или вероятность их появления), чьим следствием способны являться нежелательные влияния на информацию;
3. Угроза трактуется как реальные или потенциально вероятные действия, или условия, ведущие к какой-либо форме выражения уязвимости информации[1].

Та или иная угроза не сводится к чему-то однозначному, она включает определенные взаимозависимые элементы, каждый из которых сам по себе не составляет угрозу, но является её составляющей. Непосредственно угроза появляется исключительно при комплексном их влиянии[2].

Угрозы защищаемой информации связаны с её уязвимостью, т.е. неспособностью информации самостоятельным образом противодействовать дестабилизирующим влияниям, нарушающим её статус. А нарушение статуса защищаемой информации заключается в нарушении её физической сохранности, логической структуры и содержания, доступности для правомочных пользователей, конфиденциальности (закрытости для посторонних лиц), и выражается по средствам реализации шести форм проявления уязвимости информации[3].

В первую очередь угроза должна иметь определенные сущностные проявления, а всяческое проявление именуется явлением, соответственно, одним из признаков и компонентов угроз должно быть явление.

В основе всякого явления находятся составляющие причины, являющиеся его движущей силой и аргументированные теми или иными обстоятельствами или предпосылками. Данные причины и обстоятельства принадлежат к факторам, формирующим вероятность дестабилизирующего влияния на информацию. Итак, факторы являются ещё одним признаком и компонентом угрозы.

Ещё одним выраженным признаком угрозы является её направленность, т.е. результат, к которому способно привести дестабилизирующее влияние на информацию.

Угроза защищаемой информации – сочетание явлений, факторов и условий, формирующих опасность нарушения статуса информации.

Для раскрытия структуры угроз требуется признаки угроз конкретизировать содержательной частью, которые должны раскрыть направленность явлений и факторов, определить состав условий.

К сущностным проявлениям угрозы целесообразно отнести следующее:

1. Источник дестабилизирующего влияния на информацию (от кого или чего исходят данные влияния);
2. Формы дестабилизирующего влияния на информацию (каким образом);
3. Способы дестабилизирующего влияния на информацию (какими приёмами, действиями осуществляются виды дестабилизирующего влияния)[4].

К факторам кроме причин и обстоятельств целесообразно отнести наличие каналов и методов несанкционированного доступа к конфиденциальной информации для влияния на информацию со стороны лиц, не имеющих к ней разрешённого доступа.

К источникам дестабилизирующего влияния на информацию относятся:

1. Люди;
2. Технические средства отображения, хранения, обработки, воспроизведения, передачи информации, средства связи;
3. Системы обеспечения работы технических средств;
4. Технологические процессы отдельных категорий промышленных объектов;
5. Природные явления[5].

Наиболее распространенным, разнообразным и опасным источником дестабилизирующего влияния на защищаемую информацию являются люди. Он таков, т.к. влияние на защищаемую информацию способны оказывать разные категории людей, как работающих, так и неработающих на предприятии.

К таком источнику относятся:

1. персонал организации;
2. лица, не работающие в организации, но обладающие доступом к защищаемой информации ввиду служебного положения;
3. работники государственных органов разведки других стран и конкурирующих организаций;
4. лица из криминальных структур[6].

Технические средства являются вторым по значению источником дестабилизирующего влияния на защищаемую информацию ввиду их разнообразия.

Сюда целесообразно отнести следующее:

1. электронно-вычислительная техника;
2. электрические и автоматические машинки и копировально-множительная техника;
3. средства видео- и звукозаписывающей и воспроизводящей техники;
4. средства телефонной, телеграфной, факсимильной, громкоговорящей техники;
5. средства радиовещания и телевидения;
6. средства кабельной связи и радиосвязи[7].

Третий источник дестабилизирующего влияния на информацию включает системы электро-, водо-, теплоснабжения, кондиционирования. Сюда также примыкают вспомогательные электрические и радиоэлектронные системы и средства.

К четвертому источнику принадлежат технологические процессы обработки разных объектов ядерной энергетики, химической промышленности, радиоэлектроники, объекты по изготовлению определенных видов вооружения и военной техники, изменяющие естественную структуру окружающей среды.

Пятый источник – это природные явления, включающие стихийные бедствия и атмосферные явления.

Со стороны людей выделяются определенные формы дестабилизирующих влияний, а именно:

- 1. Непосредственное влияние на носители защищаемой информации;
  2. Несанкционированное распространение конфиденциальной информации;
  3. Нарушение режима функционирования технических средств хранения, обработки, воспроизведения, передачи информации, средств связи и технологий обработки информации;
  4. Вывод из нормальной эксплуатации технических средств и средств связи;
  5. Вывод из нормальной эксплуатации и нарушение режима функционирования систем обеспечения работы указанных средств[8].

Способами влияния на носители защищаемой информации являются:

1. физическое разрушение носителя информации;
2. возникновение аварийных ситуаций для носителей;
3. удаление информации с носителей;
4. возникновение искусственных магнитных полей для размагничивания носителей;

5. внесение фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может реализовываться с помощью:

1. словесной передачи информации;
2. передачи копий носителя информации;
3. показа носителей информации;
4. ввода информации в вычислительные сети и системы;
5. публикации информации в СМИ;
6. применения информации в открытых публичных выступлениях;
7. потери носителей информации[9].

Способами нарушения функционирования технических средств и обработки информации являются:

1. повреждения отдельных компонентом средств;
2. нарушение правил эксплуатации средств;
3. внесение изменений в порядок обработки информации;
4. заражение программ обработки информации вредоносными программами;
5. выдача ошибочных программных команд;
6. превышение расчетного числа запросов;
7. создание помех в радиоэфире при помощи дополнительного звукового или шумового фона, изменение (наложение) частот передачи информации;
8. передача ложных сигналов;
9. подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;
10. нарушение режима функционирования систем обеспечения работы соответствующих средств.

К четвертому виду относятся способы:

- 1. неправильный монтаж технических средств;
  2. разрушение средств, в том числе, повреждения кабельных линий связи;
  3. возникновение аварийных ситуаций для технических средств;
  4. отключение средств от сетей питания;
  5. вывод из нормальной эксплуатации или нарушения режима функционирования систем обеспечения работы средств;
  6. монтирование в электронно-вычислительную технику разрушающих радио- и программных закладок[10].

К стихийным бедствиям и вместе с тем формам влияния относятся землетрясения, наводнения, ураган (смерч), оползни, лавины, извержения вулканов.

К атмосферным явлениям (видам влияния) относятся: гроза, дождь, снег, град, мороз, жара, изменения влажности воздуха и магнитные бури.

1.2. Виды угроз информационной безопасности РФ

По общей направленности угрозы информационной безопасности РФ делятся на определенные виды, а именно:

1. Угрозы конституционным правам и свободам человека и гражданина в сфере духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
2. Угрозы информационному обеспечению государственной политики РФ;
3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и проникновению такой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного применения отечественных информационных ресурсов;
4. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и образующихся на территории РФ[11].

Угрозами конституционным правам и свободам человека и гражданина в сфере духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России способны быть:

1. Принятие федеральными органами государственной власти, органами государственной власти субъектов РФ нормативных правовых актов, ущемляющих конституционные права и свободы граждан в соответствующей сфере;
2. Формирование монополий на получение и распространение информации в РФ, в том числе с применением телекоммуникационных систем;
3. Противодействие, в том числе со стороны криминальных структур, реализации гражданами собственных конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и прочих сообщений;
4. Нерациональное, слишком жесткое ограничение доступа к соответствующей информации;

5. Противоправное использование специальных средств влияния на индивидуальное, групповое и общественное сознание;
6. Неисполнение федеральными органами государственной власти, органами государственной власти субъектов РФ, органами местного самоуправления, организациями и гражданами требований законодательства, определяющего отношения в информационной сфере;
7. Неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, к открытым архивным материалам, к иной открытой социально важной информации[12];
8. Дезорганизация системы накопления и сохранения культурных ценностей, включая архивы;
9. Нарушение конституционных прав и свобод человека и гражданина в сфере массовой информации;
10. Вытеснение отечественных информационных агентств, СМИ с внутреннего информационного рынка и наращивание зависимости духовной, экономической и политической областей общественной жизни России от зарубежных информационных структур;
11. Разрушение духовных ценностей, пропаганда образцов массовой культуры, базирующихся на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, установленным в социуме РФ;
12. Упадок духовного, нравственного и творческого потенциала граждан РФ, что значительным образом затрудняет подготовку трудовых ресурсов для внедрения и применения новейших технологий, включая информационные;
13. Манипулирование информацией (дезинформация, сокрытие или изменение информации).

Угрозами информационному обеспечению государственной политики РФ способны быть:

- 1. Монополизация информационного рынка РФ, его обособленных секторов отечественными и иностранными информационными структурами;
  2. Блокирование функционирования государственных СМИ по информированию российской и иностранной аудитории;
  3. Недостаточная эффективность информационного обеспечения государственной политики РФ ввиду нехватки квалифицированных кадров, отсутствия системы формирования и проведения государственной

информационной политики[13].

Под угрозой безопасности информации понимается потенциально возможное событие, процесс или явление, которое может привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Всё множество потенциальных угроз безопасности информации в автоматизированных информационных системах (АИС) или в компьютерных системах (КС) может быть разделено на два класса: случайные угрозы и преднамеренные угрозы. Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называются случайными или непреднамеренными.

К случайным угрозам относятся: стихийные бедствия и аварии, сбои и отказы технических средств, ошибки при разработке АИС или КС, алгоритмические и программные ошибки, ошибки пользователей и обслуживающего персонала.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным – до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом может происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию. Согласно тем же статистическим данным только в результате ошибок пользователей и обслуживающего персонала происходит до 65% случаев нарушения безопасности информации[14].

Следует отметить, что механизм реализации случайных угроз изучен достаточно хорошо и накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации автоматизированных информационных систем, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

Угрозы, связанные со злоумышленными действиями людей, являются непредсказуемыми, преднамеренными. Сюда целесообразно отнести следующие угрозы:

- традиционный или универсальный шпионаж и диверсии;

- несанкционированный доступ к информации;

- электромагнитные излучения;

- несанкционированная модификация структур;

- вредительские программы.

Источниками нежелательного влияния на информационные ресурсы являются методы и средства шпионажа и диверсий. Сюда целесообразно отнести: подслушивание, визуальное наблюдение, хищение документов и машинных носителей информации, хищение программ и атрибутов систем защиты, подкуп и шантаж персонала и пр.

Несанкционированный доступ к информации – это нарушение правил разграничения доступа с применением штатных средств вычислительной техники или автоматизированных систем. Несанкционированный доступ вероятен:

• при отсутствии системы разграничения доступа;

• при сбое в компьютерных системах;

• при ошибочных действиях пользователей;

• при ошибках в системе распределения доступа;

• при фальсификации полномочий[15].

Процесс обработки и передачи информации техническими средствами компьютерных систем сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и иных проводниках. В совокупности эти называется «побочные электромагнитные излучения и наводки» (ПЭМИН). Электромагнитные излучения и наводки могут быть применены злоумышленниками, как для получения информации, так и для её уничтожения.

Существенную угрозу безопасности информации в компьютерных системах представляет несанкционированная модификация алгоритмической, программной и технической структуры системы.

Одним из ключевых источников угроз безопасности информации является применение специальных программ, называющихся вредительскими. Исходя из механизма действия они делятся на 4 класса:

• «логические бомбы»;

• «черви»;

• «троянские кони»;

• «компьютерные вирусы»[16].

Логические бомбы – это программы или их компоненты, постоянно состоящие в ЭВМ и реализуемые исключительно при соблюдении соответствующих условий. Примерами подобных условий способны являться: наступление определенной даты, наступление некоторых событий определенное количество раз и пр.

Черви – программы, выполняющиеся всякий раз при загрузке системы, могут перемещаться в вычислительных системах или в сети и самовоспроизводить копии. Лавинообразное размножение программ ведет к перегрузке каналов связи, памяти и блокировке системы.

Троянские кони – программы, полученные с помощью явного изменения или добавления команд в пользовательские программы. При дальнейшем выполнении пользовательских программ вместе с заданными функциями реализуются несанкционированные, измененные или новые функции.

Компьютерные вирусы – это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются с помощью образования собственных копий.

Организация обеспечения безопасности информации должна иметь комплексный характер и базироваться на всестороннем анализе вероятных отрицательных последствий. В данном случае важно не упустить те или иные важные аспекты. Анализ отрицательных последствий подразумевает обязательную идентификацию вероятных источников угроз, факторов, способствующих их проявлению и, соответственно, определение актуальных угроз безопасности информации.

Угроз безопасности информации не так уж и много. Угроза, как следует из определения, это опасность нанесения ущерба, т.е. в данном случае проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Формы вероятного ущерба могут быть различны:

- моральный и материальный ущерб деловой репутации компании;

- моральный, физический или материальный ущерб, связанный с разглашением персональных сведений отдельных лиц;

- материальный (финансовый) ущерб от разглашения защищаемой информации;

- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;

- моральный и материальный ущерб от дезорганизации деятельности компании;

- материальный и моральный ущерб от нарушения международных отношений[17].

Ущерб может быть причинен каким-либо субъектом (тогда налицо правонарушение), а также явиться следствием независящих от субъекта проявлений (например, стихийных случаев). В первом случае налицо вина субъекта, определяющая причиненный вред как состав преступления, совершенного по злому умыслу или по неосторожности, и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом.

Во втором случае ущерб имеет вероятностный характер и должен быть сопоставлен как минимум с тем риском, который оговаривается гражданским, административным или арбитражным правом как предмет рассмотрения.

В теории права под ущербом понимаются невыгодные для собственника имущественные последствия, появившиеся в результате правонарушения. Ущерб выражается в уменьшении имущества или в недополучении дохода, который был бы получен при отсутствии правонарушения[18].

При рассмотрении в качестве субъекта, причинившего ущерб той или иной личности, категория «ущерб» справедлива тогда, когда можно доказать, что он причинен, т.е. деяния личности нужно квалифицировать в терминах правовых актов, как состав преступления. Ввиду этого при классификации угроз безопасности информации в такой ситуации нужно принимать во внимание требования актуального уголовного права, определяющего состав преступления [19].

Ниже приведены некоторые примеры составов преступления, определяемых УК РФ.

Хищение - осуществленные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.

Копирование компьютерной информации - повторение и устойчивое запечатление информации на машинном или ином носителе.

Уничтожение - внешнее воздействие на имущество, по итогам которого оно прекращает физическое существование или приводится в полную непригодность для применения по целевому назначению. Уничтоженное имущество не может быть восстановлено с помощью ремонта или реставрации и полностью выводится из хозяйственного оборота.

Уничтожение компьютерной информации - стирание ее в памяти ЭВМ.

Повреждение - изменение свойств имущества, при котором значительным образом ухудшается его состояние, теряется большая часть его полезных свойств, и оно становится целиком или частично непригодным для целевого применения.

Модификация компьютерной информации - внесение любых изменений, за исключением связанных с адаптацией программы для ЭВМ или баз данных.

Блокирование компьютерной информации - искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

Несанкционированное уничтожение, блокирование, модификация, копирование информации - всяческие неразрешенные законом, собственником или компетентным пользователем соответствующие действия с информацией[20].

Итак, обобщая изложенное, целесообразно утверждать, что угрозами информационной безопасности являются:

• хищение информации;

• уничтожение информации;

• модификация информации;

• нарушение доступности информации;

• отрицание подлинности информации.

Носителями угроз безопасности информации являются источники угроз. Источниками угроз могут являться как субъекты, так и объективные проявления. Причем источники угроз способны быть как внутренними, так и внешними. Деление на субъективные и объективные оправдано с учетом рассуждений по поводу вины или риска ущерба информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников способны отличаться.

Глава 2. План внедрения программно-аппаратного средства защиты информации от несанкционированного доступа «Secret Net LSP»

В контексте выполнения второй главы данной курсовой работы после изучения видов и угроз информационной безопасности в первой главе предлагается разработать план внедрения программно-аппаратного средства защиты информации.

СЗИ «Secret Net LSP» предназначено для выполнения определенных типовых задач, а именно:

– защита информации на рабочих станциях и серверах в соответствии с требованиями регулирующих органов;

– контроля утечек и каналов распространения защищаемой информации[21].

Возможности:

– аутентификация пользователей;

– разграничение доступа пользователей к информации и ресурсам АС;

– доверенная информационная среда;

– контроль утечек и каналов распространения конфиденциальной информации;

– контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной

информации;

– централизованное управление системой защиты, оперативный мониторинг и аудит безопасности;

– масштабируемая система защиты, возможность использования «Secret Net LSP» (сетевой вариант) в организации со множеством филиалов;

– защита терминальной инфраструктуры и поддержка технологий виртуализации рабочих столов (VDI)[22].

СЗИ «Secret Net LSP» реализует гибкое управление контролем устройств и разграничение доступа пользователей к ним, а также возможность назначения устройствам категорий конфиденциальности.

2.1. Требования перед началом установки ПО «Secret Net LSP»

СЗИ «Secret Net LSP» устанавливается на компьютеры, соответствующие определенным системным требованиям, а именно:

– ОС: Альт Линукс СПТ 6.0.0/6.0.2 x 86/x 64; ALT Linux 6.0.0 Centaurus x86/x64; CentOS 6.2/6.5 x86/x64; ContinentOS 4.2 x64; Debian 6.0.3/7.6 x86/x64; Red Hat Enterprise Linux 6.2/6.3/6.5 Desktop/Server x86/x64.

– процессор: в соответствии с требованиями ОС, установленной на компьютере.

– оперативная память: минимум 512 Мб.

– жесткий диск: минимум 600 Мб.

Перед началом установки «Secret Net LSP» на компьютер нужно убедиться в выполнении определенных требований, а именно:

1. На компьютере установлена лишь одна поддерживаемая ОС с одним ядром.

2. Ядро ОС должно входить в список ядер, заявленных как поддерживаемые компанией-разработчиком СЗИ, и соответствовать устанавливаемому дистрибутиву «Secret Net LSP»[23].

Установку системы «Secret Net LSP» осуществляет администратор, который должен обладать правами суперпользователя компьютера и правами на запуск приложения.

2.2. Установка программы «Secret Net LSP». Руководство администратора

1. Вставьте установочный компакт-диск системы Secret Net LSP, запустите эмулятор терминала и введите команду запуска программы установки с указанием пути к файлу дистрибутива. Программа установки проверит целостность дистрибутива, распакует архив с дистрибутивом и начнет выполнение 1-го этапа – сбора информации о системе. На экране появятся название версии системы и обнаруженные версии ядра. Затем программа установки перейдет ко 2-му этапу установки и предложит ознакомиться с текстом лицензионного соглашения и ввести серийный номер продукта.

2. Для просмотра текста лицензии в окне эмулятора терминала введите «Да». Появится текст лицензионного соглашения.

Для продолжения установки без просмотра лицензионного соглашения введите «Нет». Появится запрос на принятие положений лицензии. Перейдите к п. 4.

3. Ознакомьтесь с текстом лицензии. Для выхода из режима просмотра текста лицензии нажмите клавишу. В окне эмулятора терминала появится запрос на принятие положений лицензии.

4. Если вы принимаете положения лицензии, введите «Да». Появится запрос на ввод серийного номера.

Если вы не принимаете положения лицензии, введите «Нет». Программа установки завершит работу.

5. Введите серийный номер[24].

Для установочных пакетов RPM и DEB файл лицензии для демонстрационной версии включен. Для пакетов SH при установке необходимо указывать файл лицензии.

После успешной проверки файла лицензии появится запрос на выбор варианта установки: полная версия или консольная версия продукта (рисунок 1).

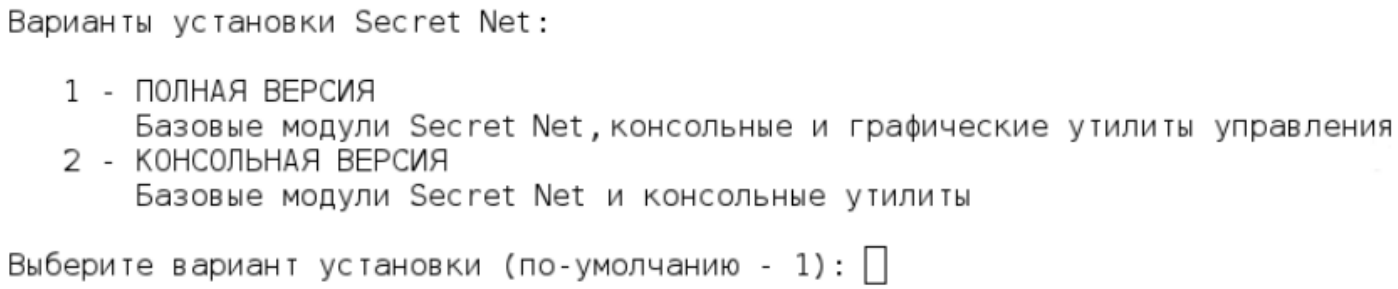

Рисунок 1. Варианты установки

6. Введите вариант установки. Целесообразно устанавливать полную версию. Программа установки перейдет к 3-му этапу – копированию файлов в каталог /opt/secretnet. По окончании копирования программа установки перейдет к 4-му этапу – настройке конфигурации системы (рисунок 2).

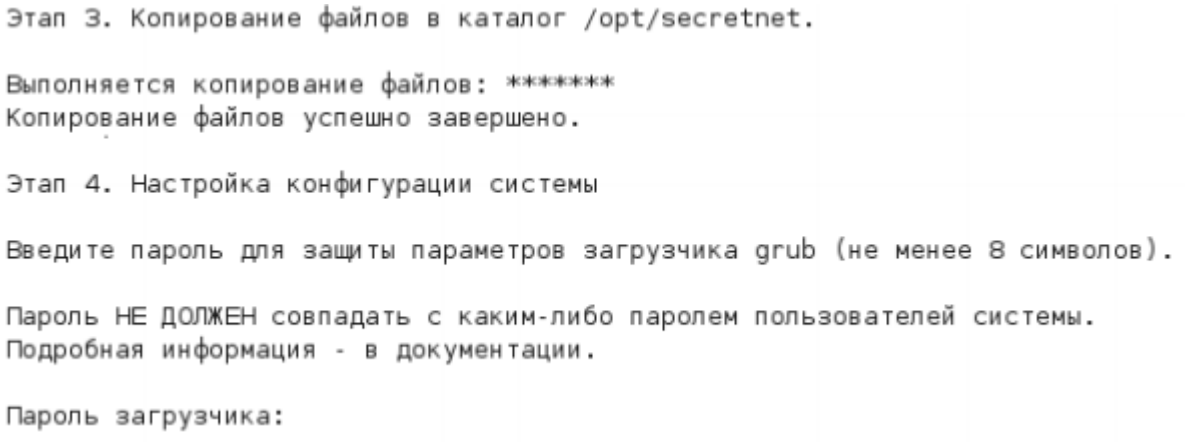

Рисунок 2. Копирование файлов в каталог /opt/secretnet, настройка конфигурации системы

7. Введите и подтвердите пароль загрузчика. Пароль должен содержать минимум 8 символов и не должен совпадать с каким-либо паролем пользователей системы.

Пароль загрузчика обеспечивает защиту от изменений пользователем параметров ядра при старте системы. Для изменения параметров ядра при старте системы нужно в grub ввести имя пользователя и указанный пароль загрузчика[25].

После ввода пароля возникнет сообщение о выполненном обновлении модулей и настроек системы аутентификации PAM и запрос на ввод нового пароля суперпользователя root (рисунок 3).

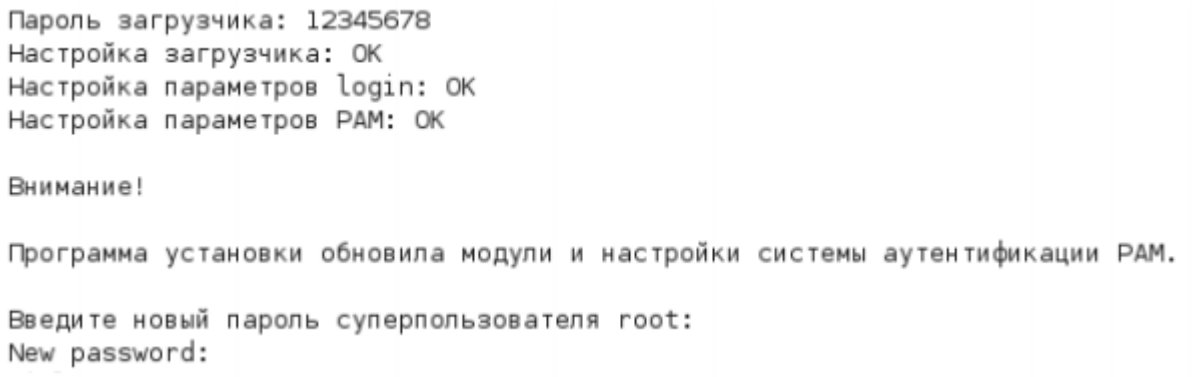

Рисунок 3. Ввод нового пароля суперпользователя root

8. Введите и подтвердите новый пароль суперпользователя root.

По общему требованию к стойкости пароль должен содержать минимум 6 символов и включать буквы и цифры. Если при вводе пароля суперпользователя root указанное требование не выполнено, то программа установки выведет соответствующее предупреждение и после повторного ввода выведет сообщение об успешном обновлении пароля.

После успешного обновления пароля суперпользователя root программа установки создаст группу системных учетных записей snlogger и осуществит настройку параметров системы.

9. Для завершения установки нажмите клавишу ENTER.

10. Перезагрузите компьютер.

После установки ПО и перезагрузки компьютера администратор должен войти в систему и выполнить начальные настройки. Первый вход в систему администратор выполняет под учетной записью суперпользователя root. Начальные настройки включают в себя: смену паролей пользователей, зарегистрированных на компьютере.

2.3. Начало работы. Руководство администратора

При первой загрузке ОС, защищаемой СЗИ Secret Net LSP, вступают в действие защитные механизмы. В данном случае действуют настройки, установленные по умолчанию.

После входа в систему администратор может просмотреть и, если требуется, изменить настройки по умолчанию, а также ознакомиться с журналами, где были зафиксированы события, связанные со входом администратора в систему.

Настройки по умолчанию. К настройкам по умолчанию относятся параметры учетных записей пользователей, добавляемых в систему средствами Secret Net LSP, и параметры политик. Значения параметров определяются при установке Secret Net LSP и могут быть изменены администратором.

Параметры учетных записей. К ним относятся:

– оболочка;

– шаблон домашнего каталога;

– создание личной группы пользователя;

– создание группы по умолчанию;

– создание домашнего каталога[26].

Для просмотра/изменения параметров учетных записей:

1. Вызовите панель безопасности и в группе «Управление пользователями» перейдите на страницу «Установки по умолчанию». Будет осуществлен переход на соответствующую страницу (рисунок 4).

Для вызова панели безопасности вызовите панель безопасности стандартным способом с помощью ярлыка Secret Net LSP на рабочем столе. На экране появится панель безопасности Secret Net LSP (рисунок 5).

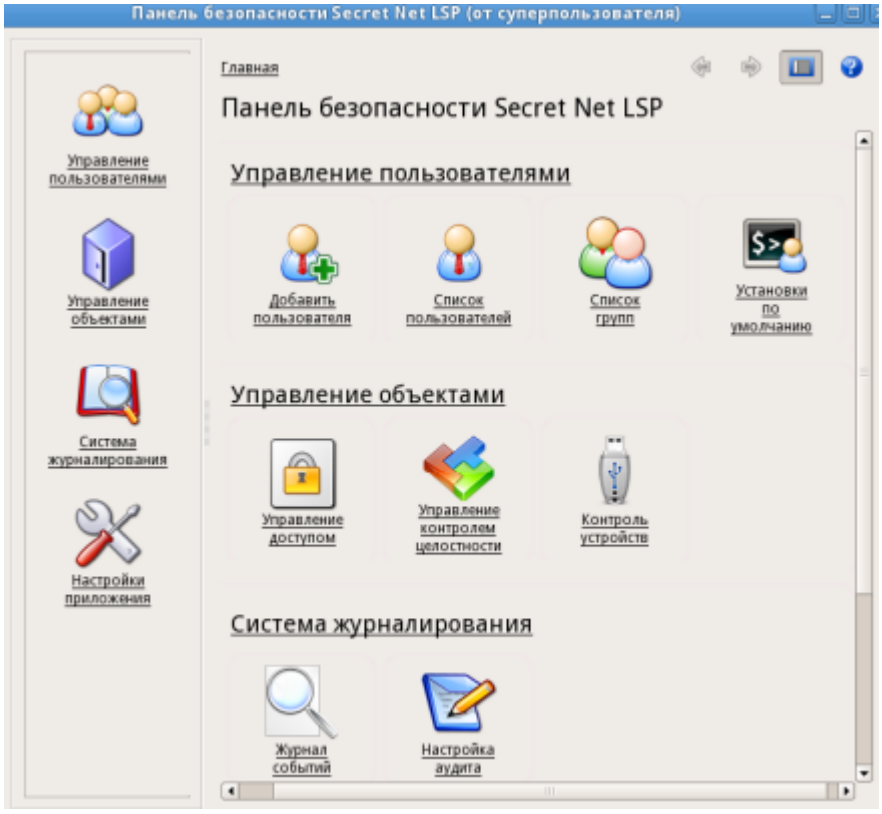

Рисунок 4. Панель безопасности Secret Net LSP

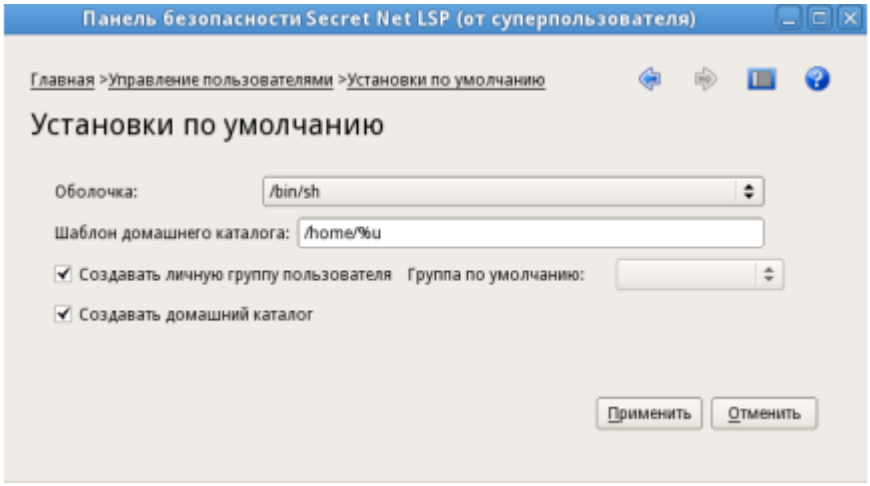

Рисунок 5. Страница «Установка по умолчанию»

1. При необходимости измените значения параметров (рисунок 6).

Поле	Описание
Оболочка	Выберите оболочку из раскрывающегося списка
Шаблон домашнего каталога	Введите вручную шаблон
Создавать личную группу пользователя	Для создания личной группы пользователя установите отметку. Имя личной группы будет соответствовать имени пользователя. Если создание личной группы пользователя не требуется, удалите отметку
Группа по умолчанию	Поле доступно, если не создается личная группа пользователя. Выберите из раскрывающегося списка группу. Если поле оставлено незаполненным, новый пользователь будет автоматически включен в виртуальную группу Users
Создавать домашний каталог	Установите отметку, если требуется автоматическое создание домашнего каталога пользователя. Если создание домашнего каталога не требуется, удалите отметку

Рисунок 6. Параметры

1. Для сохранения внесенных изменений нажмите кнопку «Применить».

Для отмены выполненных изменений нажмите кнопку «Отменить».

Для возврата на предыдущую страницу нажмите соответствующую ссылку в строке навигации.

Политики. При помощи политик реализуются определенные настройки СЗИ, а именно:

– управление режимом работы подсистемы разграничения доступа к устройствам;

– включение/выключение системных сервисов;

– управление режимом входа в систему;

– настройки параметров паролей, назначаемых новым пользователям по умолчанию.

Настройки осуществляются изменением параметров политик[27].

Для просмотра/изменения параметров политик:

1. Вызовите панель безопасности и в группе «Настройки приложения» перейдите на страницу «Политики». Будет осуществлен переход на страницу «Настройка

политик» (рисунок 7).

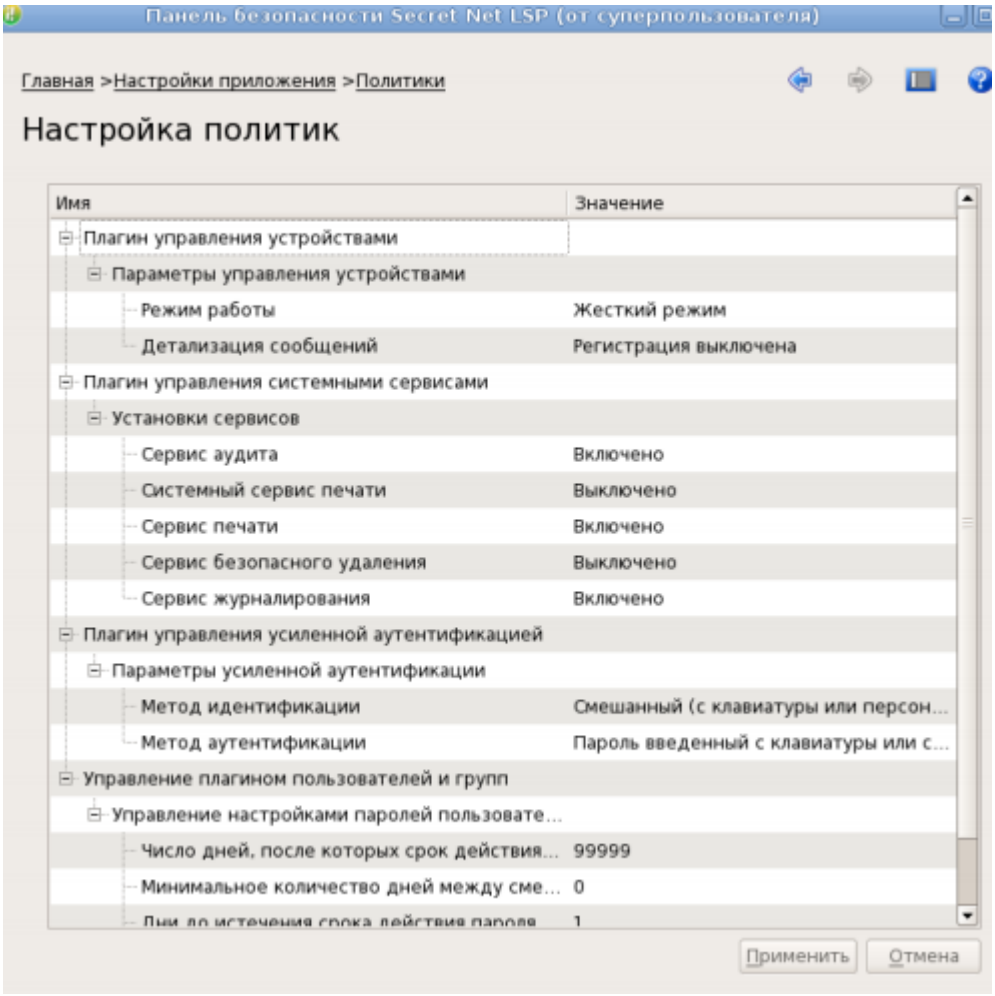

Рисунок 7. Настройка политик

2. Для изменения политики выберите необходимый параметр, активируйте поле «Значение» и выберите требуемое значение из раскрывающегося списка.

3. Для сохранения изменений нажмите кнопку «Применить».

Просмотр журналов. При первом входе в систему администратор может просмотреть результаты работы механизма регистрации событий и подсистемы ведения журналов. Также администратор может просмотреть события, зафиксированные подсистемами контроля целостности и идентификации, и аутентификации в журналах событий и аудита[28].

Для просмотра журналов вызовите панель управления безопасностью и в группе «Система журналирования» перейдите на страницу «Журнал событий».

Будет осуществлен переход на страницу «Журнал событий».

На странице на вкладках «Журнал» и «Аудит» представлено содержимое журнала событий и журнала аудита соответственно (рисунок 8).

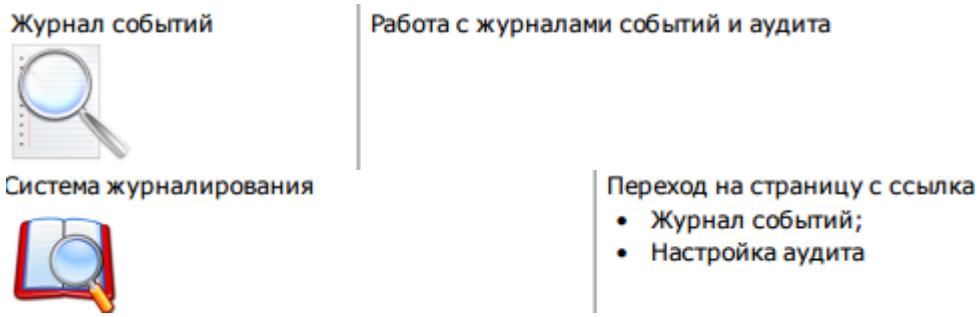

Рисунок 8. Журнал событий

2.4. Требования для пользователя перед началом работы

Перед началом работы в системе администратор должен предоставить пользователям все необходимые права для выполнения должностных обязанностей и проинформировать о предоставленных правах, разъяснить особенности работы в рамках действующих защитных механизмов. Если для входа в систему применяется персональный идентификатор, нужно получить его у администратора и ознакомиться с порядком его использования.

Перед началом работы на защищенном компьютере требуется:

1. Получить у администратора имя пользователя и пароль для входа в систему. Администратор также может выдать персональный идентификатор, который потребуется для входа в систему и входа в режиме усиленной аутентификации. Персональным идентификатором может быть Rutoken S, Rutoken S RF и iButton.

Имя: для идентификации пользователя.

Пароль: для проверки подлинности пользователя.

Персональный идентификатор: для идентификации пользователя, хранения пароля и ключевой информации, необходимой для входа в систему, когда включен режим усиленной аутентификации

2. Выяснить у администратора, какими правами и привилегиями вы сможете пользоваться при работе, а также какие ограничения имеют место в Secret Net LSP

в соответствии с настройками защитных механизмов[29].

Для начала сеанса работы на компьютере пользователь должен пройти процедуру входа в систему. В данном случае указываются учетные данные пользователя, нужные для его идентификации. После ввода учетных данных система аутентифицирует пользователя, и при успешном завершении аутентификации пользователю можно работать в системе. На рисунке приведено окно приглашения на вход в систему (рисунок 9).

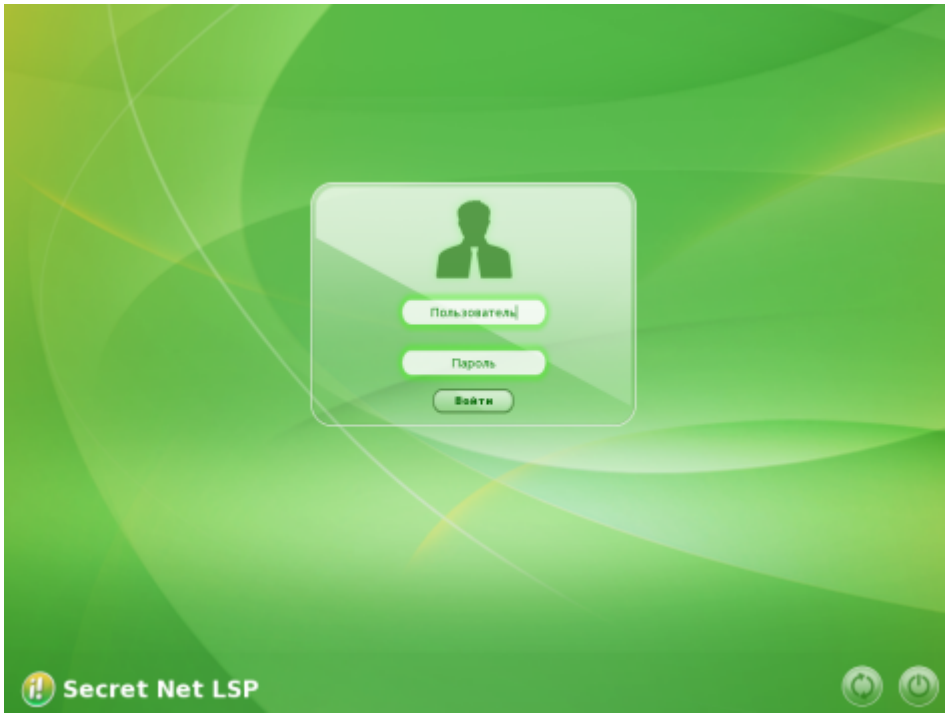

Рисунок 9. Окно приглашения на вход в систему

1. При появлении экрана приветствия (приглашение на вход в систему) введите имя и пароль пользователя.

2. Нажмите кнопку «Войти». Если учетные данные введены верно, будет осуществлен вход в систему.

Вход по идентификатору. При применении для входа в систему персонального идентификатора система автоматически определяет имя пользователя, которому присвоен идентификатор.

Для входа по идентификатору:

1. При появлении экрана приветствия (приглашение на вход в систему) предъявите собственный персональный идентификатор.

2. Реакция системы защиты находится в зависимости от информации о пароле пользователя, имеющейся в персональном идентификаторе, и наличия закрытого ключа (если включен режим усиленной аутентификации)[30]. Возможны следующие варианты:

– идентификатор включает актуальный пароль пользователя;

– в идентификаторе не записан пароль или идентификатор включает другой пароль, не совпадающий с паролем пользователя (например, ввиду того, что срок действия пароля истек, и он был заменен, но не записан в персональный идентификатор);

– в идентификаторе нет ключа или записанный в идентификаторе ключ не соответствует открытому ключу пользователя.

Если в идентификаторе имеется актуальный пароль, то после успешной проверки прав пользователя осуществляется вход в систему без запроса пароля.

Если в идентификаторе нет пароля или содержится другой пароль, появится сообщение об ошибке входа в систему.

Если в идентификаторе нет ключа или он не соответствует открытому ключу пользователя, появится сообщение об ошибке аутентификации.

Для выхода из системы:

1. Выберите в меню «Система» команду «Завершить сеанс пользователя». Появится окно предупреждения (рисунок 10).

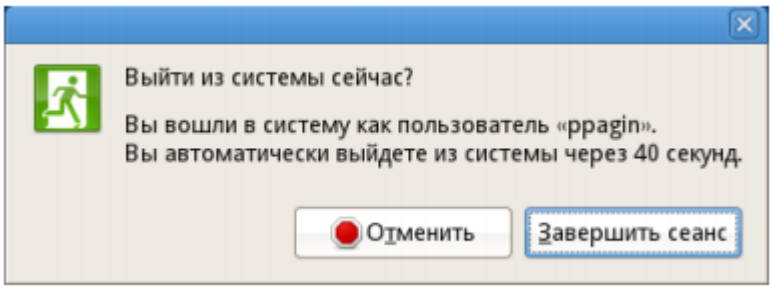

Рисунок 10. Окно выхода из системы

1. Нажмите кнопку «Завершить сеанс». Будет осуществлен выход пользователя из системы и на экране появится окно приветствия СЗИ Secret Net LSP[31].

Итак, можно сказать, что СЗИ Secret Net LSP предназначен для решения следующих типовых задач: защита информации на рабочих станциях и серверах под управлением ОС Linux в соответствии с требованиями регулирующих органов; контроль доступа пользователей к защищаемым файлам и устройствам. Secret Net LSP является сертифицированным средством защиты информации от несанкционированного доступа и дает возможность привести автоматизированные системы на платформе Linux в соответствие требованиям регулирующих документов.

ЗАКЛЮЧЕНИЕ

Угроза защищаемой информации – комплекс явлений, факторов и условий, формирующих опасность нарушения статуса информации.

Наиболее опасным источником дестабилизирующего влияния на информацию является человек, т.к. на защищаемую информацию способны влиять разные категории людей.

Многообразие видов и способов дестабилизирующего влияния на защищаемую информацию говорит о необходимости комплексной системы защиты информации.

Актуальная Доктрина информационной безопасности РФ максимально полно раскрывает виды и источники угроз информационной безопасности, а также методы ее обеспечения.

Целесообразно утверждать, что угрозами информационной безопасности являются:

• хищение информации;

• уничтожение информации;

• модификация информации;

• нарушение доступности информации;

• отрицание подлинности информации.

Носителями угроз безопасности информации являются источники угроз. Источниками угроз могут являться как субъекты, так и объективные проявления. Причем источники угроз способны быть как внутренними, так и внешними. Деление

на субъективные и объективные оправдано с учетом рассуждений по поводу вины или риска ущерба информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников способны отличаться.

Можно сказать, что СЗИ Secret Net LSP предназначен для решения следующих типовых задач: защита информации на рабочих станциях и серверах под управлением ОС Linux в соответствии с требованиями регулирующих органов; контроль доступа пользователей к защищаемым файлам и устройствам. Secret Net LSP является сертифицированным средством защиты информации от несанкционированного доступа и дает возможность привести автоматизированные системы на платформе Linux в соответствие требованиям регулирующих документов.

Цель курсовой работы достигнута - исследованы виды угроз информационной безопасности и их состав.

Для реализации поставленной цели был выполнен ряд задач, а именно:

- рассмотрены теоретические аспекты исследования видов угроз информационной безопасности;

- разработан план внедрения программно-аппаратного средства защиты информации от несанкционированного доступа «Secret Net LSP».

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Андрианов, В.И. «Шпионские штучки» и устройства для защиты объектов и информации. Справочное пособие / В.И. Андрианов, В.А. Бородин, А.В. Соколов. - М.: СПб: Лань, 2017. – С.199.

2. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

4. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2018. - 400 с.

5. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2017. - 474 с.

6. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2018. - 324 с.

7. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

8. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.

9. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2015. - 384 с.

10. Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2014. – С.225.

11. Запечников, С.В. Информационная безопасность открытых систем. Том 1. Угрозы, уязвимости, атаки и подходы к защите: Учебник для вузов. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2016. - 536 с.

12. Запечников, С.В. Информационная безопасность открытых систем. Том 2. Средства защиты в сетях: Учебник для вузов. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2016. - 558 с.

13. Ищейнов, В. Я. Защита конфиденциальной информации / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2014. – С.114.

14. Кадомцев, Б.Б. Динамика и информация / Б.Б. Кадомцев. - М.: [не указано], 2015. – С.499.

15. Ковалев, А.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов: Монография / А.А. Ковалев, В.А. Шамахов. - М.: Риор, 2018. - 32 с.

16. Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2013. - 136 с.

17. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. - М.: Русайнс, 2017. - 64 с.

18. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. / А.А. Малюк. - М.: Горячая линия -Телеком , 2014. - 280 с.

19. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. - 448 с.

20. Одинцов, А.А. Экономическая и информационная безопасность предпринимательства / А.А. Одинцов. - М.: Academia, 2014. - 384 с.

21. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.

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

23. Семененко, В.А. Информационная безопасность / В.А. Семененко. - М.: МГИУ, 2011. - 277 с.

24. Сергеева, Ю. С. Защита информации. Конспект лекций / Ю.С. Сергеева. - Москва: ИЛ, 2015. – С.11.

25. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. - 336 с.

26. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.

27. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. - М.: Академический проект, 2018. - 544 с.

1. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. - М.: Академический проект, 2018. – С.145. ↑

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. – С.99. ↑

3. Андрианов, В.И. «Шпионские штучки» и устройства для защиты объектов и информации. Справочное пособие / В.И. Андрианов, В.А. Бородин, А.В. Соколов. - М.: СПб: Лань, 2017. – С.78. ↑

4. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. – С.85. ↑

5. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. – С.90. ↑

6. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. – С.315. ↑

7. Сергеева, Ю. С. Защита информации. Конспект лекций / Ю.С. Сергеева. - Москва: ИЛ, 2015. – С.11. ↑

8. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2018. – С.218. ↑

9. Семененко, В.А. Информационная безопасность / В.А. Семененко. - М.: МГИУ, 2011. – С.155. ↑

10. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2017. – С.338. ↑

11. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. – С.190. ↑

12. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. – С.65. ↑

13. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. – С.46. ↑

14. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. – С.77. ↑

15. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2018. – С.156. ↑

16. Одинцов, А.А. Экономическая и информационная безопасность предпринимательства / А.А. Одинцов. - М.: Academia, 2014. – С.226. ↑

17. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. / А.А. Малюк. - М.: Горячая линия -Телеком , 2014. – С.177. ↑

18. Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2014. – С.91. ↑

19. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2015. – С.60. ↑

20. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. – С.194. ↑

21. Запечников, С.В. Информационная безопасность открытых систем. Том 2. Средства защиты в сетях: Учебник для вузов. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2016. – С.454. ↑

22. Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2013. - 136 с. ↑

23. Сергеева, Ю. С. Защита информации. Конспект лекций / Ю.С. Сергеева. - Москва: ИЛ, 2015. – С.11. ↑

24. Кадомцев, Б.Б. Динамика и информация / Б.Б. Кадомцев. - М.: [не указано], 2015. – С.499. ↑

25. Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2014. – С.225. ↑

26. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. – С.25. ↑

27. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. – С.144. ↑

28. Андрианов, В.И. «Шпионские штучки» и устройства для защиты объектов и информации. Справочное пособие / В.И. Андрианов, В.А. Бородин, А.В. Соколов. - М.: СПб: Лань, 2017. – С.199. ↑

29. Кадомцев, Б.Б. Динамика и информация / Б.Б. Кадомцев. - М.: [не указано], 2015. – С.550. ↑

30. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. – С.234. ↑

31. Ищейнов, В. Я. Защита конфиденциальной информации / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2014. – С.88. ↑