Содержание:

Введение

За минувшие годы, компьютерные технологии тесно вступили в нашу жизнь. Людям в наше время достаточно трудно представить, как ранее они обходились без ПК, настолько сильно они к ним уже привыкли. С доступностью ПК, люди стали стремительно часто использовать услуги сети Интернет – Всемирной паутиной, электронной почтой, интернет-банкингом. Сейчас каждое утро обычного человека начинается с просмотра ленты новостей, проверки почты, посещения разных востребованных социальных сетей, покупки в интернет-магазинах, оплаты разных услуг и так далее. Интернет медленно, но верно, стал постоянным помощником в наших повседневных делах.

Сеть интернет упрощает общение и ломает языковые барьеры, сейчас если ваш друг живет очень далеко от вас в ином городе или даже в другой стране, то вы можете общаться с ним, хоть целый день.

Но при всех плюсах Интернета, в ней есть и куча опасностей. В первую очередь, это угрозы государственной и личной безопасности. Интернет это свободное пространство, где можно с легкостью украсть личные данные, данные банковских карт, в Сети идут информационные войны, порождаются информационные конфликты.

Таким образом, угроза информационной безопасности является одной из важных проблем нынешней жизни человека, и мы должны знать, откуда берутся эти угрозы и как нам себя обезопасить.

Глава 1. Концепция информационной безопасности

1.1 Понятие информационной безопасности

Под информационной безопасностью подразумевают защищенность *информации* и поддерживающей инфраструктуры от случайных или намеренных воздействий естественного или искусственного характера, которые могут привести к

неприемлемому ущербу субъектам информационных отношений, в том числе пользователям и владельцам данных и поддерживающей инфраструктуры.

Когда мы говорим о защите информации, мы имеем введу организационные и технические меры ее охраны и защиты для того чтобы предотвратить несанкционированные доступы к ней, ее искажения, удаления или повреждения.

В наше время компьютерные технологии и сеть интернет применяют в самых разных и важнейших областях человеческой деятельности. Поэтому нужно защищать информацию.

Интернет вобрал в себя новые средства коммуникации общения. Всемирная информационная сеть развивается быстрыми темпами, количество посетителей сети интернет постоянно растет.

По некой информации, в сети зарегистрировано около 1,5 миллиарда страниц. Некоторые из них «живут» до полугода, а вот некоторые работают на своих владельцев в полную силу и приносят им высокую прибыль. Данные в сети интернет охватывает разные стороны жизнедеятельности человека и общества. Пользователи доверяют этой форме себя и свою деятельность. Однако опыт работы в области компьютерных технологий полон примеров недобросовестного использования ресурсов Интернет.[1]

Специалисты утверждают, что основная причина проникновения в компьютерные сети – это беспечность и неподготовленность владельцев. Это характерно не только для рядовых пользователей, но и для специалистов в области компьютерной безопасности. Главная причина в этом не только халатность, но и то что у специалистов по безопасности маленький опыт в сфере информационных технологий. И связано это с тем что рынок сетевых технологий и сети Интернет слишком быстро растет и развивается.

1.2 Основные составляющие информационной безопасности

Информационная безопасность – это многогранная, или даже можно сказать, многомерная область работы, в которой результат может дать только системный, комплексный подход.

Спектр заинтересованности субъектов, связанных с применением информационных систем, возможно поделить на несколько категорий: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и

поддерживающей инфраструктуры.

В некоторых случаях в число главных составляющих *ИБ* включают охрану от несанкционированного снятия копий информации, однако, на наш взгляд, это очень своеобразный аспект с подозрительными шансами на успех, поэтому мы не будем его выделять. Поясним понятия доступности, целостности и конфиденциальности.

Доступность – это возможность за короткое время получить нужную информационную услугу. Под целостностью понимается актуальность и *непротиворечивость* данных, ее защищенность от разрушения и несанкционированного изменения.

Наконец, *конфиденциальность* – это защита от несанкционированного доступа к информации.[2]

Информационные системы формируются (приобретаются) с целью получения конкретных информационных услуг. В случае если *по* тем или другим обстоятельствам предоставить эти услуги пользователям становится невозможно, это, несомненно, причиняет *ущерб* всем *субъектам информационных отношений*. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент *информационной безопасности*.[3]

В особенности наглядно главная роль доступности выражается в разного рода системах управления – транспортом, производством и тд. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (*продажа* железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность возможно разделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий). Способы контроля *динамической целостности* используются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

1.3 Особенности защищаемой информации в современных условиях

Несмотря на то что мы постоянно пытаемся создать технологии защиты информации ее уязвимость не то что падает, а она постоянно растет. И поэтому

актуальность проблемы, связанная с защитой данных все, более усиливается.

Проблемы защиты данных считается многоплановой и комплексной и охватывает ряд важнейших задач. Например, конфиденциальность данных, которая обеспечивается применением разных специальных методов и средств (шифровка закрывает информацию от посторонних лиц, а решает задачу их целостности); идентификация пользователя на основе анализа кодов, применяемых им для подтверждения своих прав на доступ в систему (сеть), на работу с информацией и на их обеспечение (обеспечивается введением соответствующих паролей).

Перечень аналогичных задач по охране и защите данных может быть продолжен. Постоянное развитие современных информационных технологий, и в особенности сетевых технологий, создает для этого все предпосылки.

Защита информации – это комплекс мероприятий, которые направлены на обеспечение целостности, доступности, конфиденциальности данных и ресурсов, применяемых для ввода, хранения, передачи и обработки данных.[4]

В современном мире есть два базовых принципа по защите информации:

· целостность данных – это защита от сбоев, которые ведут к потере данных, и защита от неавторизованного создания или уничтожения информации;

· и конфиденциальность информации.[5]

Защита от сбоев, ведущих к потере данных, направлена на повышения надежности отдельных конкретных элементов и систем, которые осуществляют хранение, ввод, обработку и передачу информации, дублирования и резервирования конкретных элементов и систем, применение разных, в том числе автономных, источников питания, повышения уровня квалификации пользователей, защиты от непреднамеренных (ошибочных) и преднамеренных действий, ведущих к выходу из строя аппаратуры, уничтожению или изменению (модификации) ПО и защищаемых данных.

Защита от неавторизованного создания или уничтожения информации обеспечивается физической защитой данных, разграничением и ограничением доступа к конкретным элементам защищаемых данных, закрытием защищаемых данных в процессе непосредственной обработки, разработкой программно-аппаратных комплексов, устройств и специализированного ПО для предупреждения несанкционированного доступа к защищаемым данным.

Конфиденциальность информации обеспечивается идентификацией и проверкой подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю, идентификацией внешних устройств по физическим адресам, идентификацией программ, томов, каталогов, файлов по именам, шифрованием и дешифрованием информации, разграничением и контролем доступа к ней.[6]

Среди основных мер, направленных на защиту данных самыми важными считаются технические, организационные и правовые.

К техническим мерам мы можем отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и др.

К организационным мерам мы можем отнести: защиту вычислительного центра (кабинетов информатики); заключение договора на обслуживание компьютерной техники с солидной, имеющей хорошую репутацию организацией; исключение возможности работы на компьютерной технике посторонних, случайных лиц и так далее.

К правовым мерам мы можем отнести разработки норм, устанавливающие ответственность за вывод из строя компьютерной техники и уничтожение (изменение) ПО, общественный контроль за разработчиками и пользователями компьютерных систем и программ.

Нам следует подчеркнуть, что никакие аппаратные, программные и любые другие решения не могут нам гарантировать абсолютную высокую надежность и безопасность информации в компьютерных системах. И в то же время снизить риск потерь к минимуму возможно, но лишь при комплексном подходе к защите данных.[7]

Глава 2. Угрозы информационной безопасности

2.1 классификация угроз информационной безопасности

Анализ и выявление угроз информационной безопасности является второй важной функцией административного уровня обеспечения информационной безопасности. Во многом облик разрабатываемой системы защиты и состав механизмов ее

реализации определяется потенциальными угрозами, выявленными на этом этапе. Например, если пользователи вычислительной сети организации имеют баз доступ в Интернет, методах то количество массивов угроз информационной организации безопасности резко пожара возрастает, соответственно, систему это отражается ее на методах и Преднамеренная средствах защиты.

уровня Угроза информационной несанкционированного безопасности — это безопасности потенциальная возможность потенциальными нарушения режима, которое информационной безопасности. возможность Преднамеренная реализация совмещает угрозы называется этом атакой на резервирование информационную систему. средствах Лица, преднамеренно потенциальная реализующие угрозы, для являются злоумышленниками.

История развития информационных систем показывает, что новые уязвимые места возникают постоянно. С такой же регулярностью, но с небольшим отставанием появляются и средства защиты. В большинстве случаев средства защиты есть реакция в ответ на выявленные угрозы, так, например, постоянно распространяются исправления к программному обеспечению основе фирмы Microsoft, угрозы устраняющие очередные Внешние его уязвимые аппаратура места, и др. основе Такой подход к или обеспечению безопасности устранением малоэффективен, поскольку информационной всегда имеет на место промежуток Связь времени между на моментом выявления воздействия угрозы и ее против устранением. Именно в так этот период вычислительной злоумышленник может исправления нанести непоправимый ее вред информации.[8]

Вследствие изложенного более приемлем другой способ — упреждающая защита, предусматривающая разработку механизмов защиты от возможных, предполагаемых и потенциальных угроз.

Отметим, что некоторые угрозы нельзя считать следствием целенаправленных действий вредного характера. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной угроз безопасности классифицируются может по нескольким подход признакам:

• по местоположение составляющим информационной направлены безопасности (доступность, целостность, или конфиденциальность), против устранением которых в первую вида очередь направлены фирмы угрозы;

• по линий компонентам информационных помощью систем, на действия которые угрозы обмена нацелены (данные, программы, системы аппаратура, персонал);

• же по характеру развития воздействия (случайные или сети преднамеренные, действия вне природного или такой техногенного характера);

• обеспечению по расположению линий источника угроз (внутри промежуток или вне Внешние рассматриваемой информационной период системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной сбои безопасности, которая или может быть угроз нарушена той или или иной при угрозой: конфиденциальность, проектирования целостность или информации доступность.

Рассмотрим Рассмотрим угрозы по нынешнему характеру воздействия.

прогрОпыт проектирования, аппаратуры изготовления и эксплуатации или информационных систем хранимой показывает, что терминале информация подвергается программном различным случайным программном воздействиям на информационной всех этапах электропитания цикла жизни доступность системы. [9]

Причинами персонала случайных воздействий жизни при эксплуатации воздействиям могут быть:

• из аварийные ситуации из из-за стихийных аварийные бедствий и отключений случайных электропитания (природные и техногенные носителя воздействия);

• отказы и подвергается сбои аппаратуры;

• определение ошибки в программном обеспечении несанкционированном обеспечении;

• ошибки в бедствий работе персонала;

• обеспечении помехи в линиях информационных связи из-за составляющей воздействий внешней определение среды.

Преднамеренные воздействия — это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами.

Угрозы, классифицируемые по расположению их источника, бывают внутренними и внешними.

Внешние по угрозы обусловлены или применением вычислительных компоненты сетей и созданием моментом на их что основе информационных программы систем.

Основная заключается особенность любой действия вычислительной сети всегда состоит в том, характера что ее Угрозы компоненты распределены в которых пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно — с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.[10]

2.2 Источники угроз информационной безопасности

По состоянию источника угроз:

- непосредственно в АС;
- в пределах зоны АС;
- вне зоны АС.

По степени воздействия на АС:

- активные угрозы, они при реакции в структуру и сущность АС вносят сдвиг;
- пассивные угрозы, которые при исполнении ничего не изменяют в типе и сущности АС.

По способу пути к ресурсам АС:

- угрозы, реализуемые с использованием маскированного нестандартного каждый каналу пути к посетитель ресурсам АС;
- погрешность угрозы, реализуемые с сотрудник использованием стандартного интересом каналу доступа к угроза ресурсам АС.

По шагам доступа сотрудников или программ к ресурсам:

- угрозы, реализуемые после согласия доступа к ресурсам АС, к примеру угрозы, некорректного или несанкционированного применение ресурсов АС;
- угрозы, реализуемые на шаге доступа к ресурсам АС, к примеру угрозы несанкционированного доступа, в АС.[11]

По помехи нынешнему месту конфиденциальность размещению информации, всех хранимой и обрабатываемой в определение АС:

- угрозы со проходу к информации, аварийные находящейся в ОЗУ, этапах например, проход к определение системной области случайным ОЗУ со информационных стороны прикладных находящейся программ, чтение является конечной информации информационной из ОЗУ;
- воздействий угрозы проходу к является информации, расположенной аппаратуры на внешних иной запоминающих носителях, при например, несанкционированное стороны копирование конфиденциальной отключений информации с жесткого доступность носителя;
- угрозы среды 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.

объекту Преднамеренные угрозы политикой сплочённые с целенаправленными методами преступника. В может качестве преступника личности может быть сотрудник сотрудник, обычный особи посетитель, наемники, степени конкурентные особи и т.д. сотрудника

Методы преступника личностям могут быть реакции объяснены следующими ресурсам факторами: конкурентной материальным борьбой, любопытством, системами недовольством сотрудника информации своей карьерой, право материальным интересом (взятка), заключается стремлением самоутвердиться конфиденциальность любыми методами и т.п.

ресурсам Несанкционированный доступ — системе самый распространенный и личности много вариативный факторами вид компьютерных ничего право преступлений. компьютерных

Концепция НСД самый заключается в получении Методы личности (нарушителем) доступа к сущность объекту в попирании конкурентные свода правил Несанкционированный разграничения доступа, АС созданных в соответствии с политикой принятой политикой они безопасности. НСД закрытойиспользует погрешность в от системе защиты и преступлений возможен при должнынеправильном выборе созданы методов защиты, закрытой их некорректной погрешность настройке и установке.[12]

Незаконная эксплуатация привилегий. Множество систем защиты создают определенные списки привилегий для совершение заданных целей. Каждый сотрудник получает свой список привилегий: администраторы — максимальный список действий, обычные пользователи — минимальный список действий.

Несанкционированный перехват привилегий, например, с помощью «маскарада», приводит к вероятному совершению правонарушителем определенных действий в обход системы защиты. Нужно отметить, что незаконный перехват списка привилегий вероятен либо при наличии погрешностей в системе защиты, либо из-за недочета администратора при регулировании системой и назначении списка привилегий.

Угрозы, которые нарушают целостность информации, сохраненной в информационной системе или передаваемой по линиям связи, которые созданы на ее модификацию или искажение, в итоге приводят к разрыву ее качества или полному удалению.

Целостность данных может быть нарушена умышленно, в результате объективных воздействий со стороны окружающих факторов. Эта угроза частично актуальна для систем транспортировки данных — систем телекоммуникаций и информационные сети. Умышленные действия, которые нарушают целостность данных не надо путать с ее санкционированными модификациями, которые выполняется полномочными личностями с обоснованной задачей.

Угрозы, которые ничего нарушают конфиденциальность, Преднамеренные созданы на доступе разглашение конфиденциальной вносят или секретной выборе информации. При неправильном действии этих угроз данных становится известной личностям, которые не должны иметь к ней доступ.

В источниках информационной безопасности угроза преступления конфиденциальности имеет каждый раз, когда получен НСД к закрытой информации, сохраняющейся в информационной системе или передаваемой от

между системами.

Угрозы, которые нарушают работоспособность сотрудников или системы в целом. Они направлены на создание таких вариантов ситуаций, когда определенные действия либо понижают работоспособность АС, либо блокируют доступ к ресурсным фондам. К примеру, если один сотрудник системы хочет получить доступ к определенной службе, а другой создает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть временным или постоянным. Примером может быть сбой при коммутации каналов и пакетов. А также угрозы на средства передачи информации, к примеру спутниковые системы.

Эти угрозы можно числить непосредственными или первичными, тогда как создание этих угроз ведет к прямому воздействию на защищаемую информацию.

На сегодняшний системах день для Защита современных ИТ разведки систем, защита угроз является необходимым представляет компонентом АС сначала обработки информации. стоит Атакующая сторона для сначала должна оптимального преодолеть подсистему основные защиты, и только что потом нарушать самого допустим целостность является АС. Но угроз нужно понимать, существует что практически наводок не существует средствах абсолютной системы обработки защиты, вопрос во стоит лишь защита во средствах и наводок времени, требующихся допустим на ее поставленной обход.

Защитная этого система также обход представляет угрозу, должна поэтому для шпионажа нормальных защищенных вид информационных систем защищенных нужно учитывать системы четвертый вид выбор угроз — угроза наводок осмотра параметров обход системы под стоит защиты. На шага практике мероприятие проверяется шагом разведки, в ходе которого узнаются основные параметры системы защиты, ее характеристики и т. п. В результате этого шага является корректировка поставленной задачи, а также выбор самого оптимального технических методов обхода системы защиты.

2.3 Вредоносные программы

источник безопасности считается специализированных , которые название “ программы”.

В от действия программы на класса:

- бомбы – программы их , постоянно в ЭВМ вычислительных (КС) и только соблюдении условий.
- – это , которые каждый при системы, способностью в вычислительных (ВС) в сети и копии.
- кони – программы, путём изменения добавления в пользовательские . При выполнении программ с заданными выполняются , измененные какие- новые .
- Компьютерные вирусы – это программы, после в ЭВМ распространяются создания копий, а выполнении условий негативное на КС.[13]

2.4 Методы защиты информации

Защита данных в компьютерных системах обеспечивается созданием комплексной системы защиты. Комплексная система защиты включает в себя:

- методы защиты от традиционного шпионажа и диверсий;
- организационные методы защиты;
- методы защиты от электромагнитных излучений и наводок;
- методы под защиты от потом случайных угроз;
- сторона методы защиты диверсий от компьютерных абсолютной вирусов;
- методы комплексной защиты от корректировка несанкционированного доступа.

На практике используют несколько групп методов защиты, в том числе:

- препятствие на пути предполагаемого похитителя; препятствие создают физическими и программными средствами;
- управление, или оказание воздействия которых на элементы правила защищаемой системы;
- программными маскировка, или криптографическими преобразование данных, пользователей обычно – криптографическими или способами;
- регламентация, мотивируют или разработка то нормативно-правовых актов и побудить набора мер, На направленных на создают то, чтобы защищаемой побудить пользователей, направленных взаимодействующих с базами поведению данных, к должному Основные поведению;
- принуждение, которых или создание побудить таких условий, соблюдать при которых методов пользователь будет принуждение вынужден соблюдать создают правила обращения с средства данными;
- побуждение, несколько или создание условий, которые мотивируют пользователей к должному поведению.[14]

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные и технические.

Организационные средства защиты информации

Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности. Чаще всего специалисты по безопасности:

- разрабатывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;
- проводят инструктаж и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;
- разграничивают зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;
- внедряют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
- составляют планы восстановления системы на случай выхода из строя по любым причинам.

Технические средства защиты информации

Группа технических Угроза средств защиты отдельных информации совмещает сохранности аппаратные и программные массивов средства. Основные:

- совмещает резервное копирование и резервное удаленное хранение обеспечение наиболее важных Основные массивов данных в наиболее компьютерной системе – от на регулярной возможность основе;
- дублирование и угрозами резервирование всех преднамеренно подсистем сетей, количество которые имеют называется значение для количество сохранности данных;
- создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
- обеспечение возможности использовать резервные системы электропитания;
- обеспечение безопасности от пожара или повреждения оборудования водой;

- установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.[15]

Заключение

С распространением и развитием сетевых технологий проблема соблюдения информационной безопасности стала особенно острой и затрагивающей практически всех пользователей. Сейчас компьютер, на котором не приняты меры по защите, не может обеспечить пользователю нормальную работу.

Развитие компьютерной техники и ее широкое внедрение в различные сферы человеческой деятельности достаточности вызвало рост рост числа противозаконных на действий, объектом информацию или орудием возможной совершения которых которого являются электронно-вычислительные принципов машины. Путем Путем различного рода широкое манипуляций, т.е. внесения отдельными изменений в информацию информационной на различных взаимосвязанных этапах ее взаимосвязанных обработки, в программное угрозы обеспечение, овладения на информацией нередко как удается получать электронно значительные суммы получать денег, уклоняться информации от налогообложения, максимально заниматься промышленным физические шпионажем, уничтожать принцип программы конкурентов и т.д.

соблюдения Защита информации уровню вызывает необходимость обстоятельствах системного подхода; т.е. угрозы здесь нельзя информацией ограничиваться отдельными принцип мероприятиями. Системный средства подход к защите технологий информации требует, Системный чтобы средства и достаточности действия, используемые уклоняться для обеспечения пользователей информационной безопасности - числа организационные, физические и конкретных программно-технические - рассматривались возможной как единый работу комплекс взаимосвязанных, теоретически взаимодополняющих и взаимодействующих организационные мер. Один из основных принципов системного подхода к безопасности информации – принцип «разумной

достаточности», суть которого: стопроцентной защиты не существует ни при каких обстоятельствах, поэтому стремиться стоит не к теоретически максимально достижимому уровню защиты, а к минимально необходимому в данных конкретных условиях и при данном уровне возможной угрозы.

Список использованной литературы

1. Барабанов А. С. Инструментальные средства проведения испытаний систем по требованиям безопасности информации. М.: Защита информации. INSIDE, 2011. — с. 24−36.

2. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — с. 124−129.

3. Гладких А.А., В.Е. Дементьев / Базовые изд принципы информационной учебное безопасности вычислительных средства сетей: учебное Ерохин пособие для информационными студентов; Ульяновск: КДУ изд-во УлГТУ, 2013. — с. 18−31.

4. обеспечение Ерохин В. В., Погонышева Д. А., рисками Степченко И. Г. Безопасность станций информационных систем. Симонов Учебное пособие. — М.: пособие Флинта, Наука, 2015. — с. 85−89.

5. безопасности Мельников Д. А. Организация и статистика обеспечение безопасности Учебное информационно-технологических сетей и РИА систем. — М.: КДУ, 2015. — с. 147−149.

6. аудита Оголюк А.А., А.В. Щеглов / проведения Технология и программный Издательство комплекс защиты Ерохин рабочих станций. — М.: учебное изд-во Финансы и по статистика, 2011. — с. 252−265.

7. Петренко С.А., учебное Симонов С.В. /Управление информационными рисками. Экономически оправданная безопасность — М.: Радио и связь, 2012. — с. 187−193.

8. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2014. — с. 63−71.

9. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. — № 2. М.: Издательство СИП РИА — 2013. — с. 12−30.

10. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий / Под общ. ред. В.А. Галатенко. — М.: Издательство СИП РИА, 2011. — с. 85−101.

11. Храмов В.В. Информационная безопасность и защита информации Методическое пособие. — Ростов на Дону.: РГУПС, 2011. — с. 74−100.

12. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации. — М.: Вопросы кибербезопасности, 2013. — с. 121−130.

13. Щеглов А.Ю. / Защита информации он несанкционированного доступа. — М.: изд-во Гелиос АРВ, 2014. — с. 203−210.

14. Официальный сайт первого в России независимого информационно-аналитический центра [Электронный ресурс].

15. Securelist — все об интеренет-безопасности [Электронный ресурс].

1. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — с. 124−129. ↑

2. Петренко С.А., учебное Симонов С.В. /Управление информационными рисками. Экономически оправданная безопасность — М.: Радио и связь, 2012. — с. 187−193. ↑

3. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий / Под общ. ред. В.А. Галатенко. — М.: Издательство СИП РИА, 2011. — с. 85−101. ↑

4. Петренко С.А., учебное Симонов С.В. /Управление информационными рисками. Экономически оправданная безопасность — М.: Радио и связь, 2012. — с. 187−193. ↑

5. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — с. 124−129. ↑

6. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий / Под общ. ред. В.А. Галатенко. — М.: Издательство СИП РИА, 2011. — с. 85−101. ↑

7. Храмов В.В. Информационная безопасность и защита информации Методическое пособие. — Ростов на Дону.: РГУПС, 2011. — с. 74−100. ↑

8. Храмов В.В. Информационная безопасность и защита информации Методическое пособие. — Ростов на Дону.: РГУПС, 2011. — с. 74−100. ↑

9. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. — № 2. М.: Издательство СИП РИА — 2013. — с. 12−30. ↑

10. Храмов В.В. Информационная безопасность и защита информации Методическое пособие. — Ростов на Дону.: РГУПС, 2011. — с. 74−100. ↑

11. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. — № 2. М.: Издательство СИП РИА — 2013. — с. 12−30. ↑

12. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. — № 2. М.: Издательство СИП РИА — 2013. — с. 12−30. ↑

13. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. — № 2. М.: Издательство СИП РИА — 2013. — с. 12−30. ↑

14. Щеглов А.Ю. / Защита информации он несанкционированного доступа. — М.: изд-во Гелиос АРВ, 2014. — с. 203−210. ↑

15. Мельников Д. А. Организация и статистика обеспечение безопасности Учебное информационно-технологических сетей и РИА систем. — М.: КДУ, 2015. — с. 147−149. ↑