Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:
https://stuservis.ru/kursovaya-rabota/366049

Тип работы: Курсовая работа

Предмет: Педагогика

ВВЕДЕНИЕ

Актуальность темы исследования. Использование компьютеризиро-ванных средств в управлении различными структурами требует мощных си-стем обработки и передачи данных. Решение этой проблемы привело к созда-нию единой инфраструктуры. Его использование позволяло людям, имеющим компьютер и модем, получать доступ к информации из крупнейших библио-тек и баз данных мира, быстро выполнять сложные вычисления и быстро об-мениваться информацией с другими респондентами в сети, независимо от рас-стояния и страны проживания.
Данные вопросы стали возможны к разрешению в том числе благодаря активному внедрению в образовательных учреждениях предмета «Информа-тика», благодаря чему еще со школы формируются кадры, которые впослед-ствии работают в организациях программистами и защищают информацию данных организаций от неправомерного вмешательства.
Однако в настоящее время различные системы обмена информацией вы-звали ряд проблем, одной из которых является риск обработки и передачи данных. Особенно «беззащитными» были данные, передаваемые в глобальных телекоммуникационных сетях. В настоящее время над безопасностью инфор-мации работает большое количество специалистов практически во всех эко-номически развитых странах мира.
Можно сказать, что информационная безопасность превратилась в быстро развивающуюся дисциплину. Однако, несмотря на усилия многочис-ленных организаций, занимающихся защитой информации, обеспечение ин-формационной безопасности по-прежнему остается чрезвычайно острой про-блемой. Определенные трудности связаны с изменениями в технологиях об-работки и передачи.
С одной стороны, использование информационных технологий дает ряд очевидных преимуществ: повышение эффективности процессов управле-ния, обработки и передачи данных.
С другой стороны, использование информационных технологий имеет ряд очевидных преимуществ: повышение эффективности процессов управле-ния, обработки и передачи данных. Сегодня невозможно представить себе крупную организацию без использования новейших информационных техно-логий, от автоматизации отдельных рабочих мест до создания распределен-ных информационных систем для предприятий. С другой стороны, развитие сетей, их сложность, взаимная интеграция и открытость приводят к появле-нию качественно новых угроз и увеличению числа злоумышленников, кото-рые могут повлиять на систему.
В настоящее время для обеспечения защиты информации необходимо разработать не только механизмы частной защиты, но и системный подход, включающий комплекс взаимосвязанных мер (использование специальных технических и программных средств, организационные меры, правовые акты, морально-этические контрмеры).
Сложный характер защиты проистекает из сложных действий злоумыш-ленников, которые всеми силами пытаются получить важную для них инфор-мацию. Сегодня можно утверждать, что рождается новая

современная техно-логия — технология защиты информации.
Эти обстоятельства определяют актуальность выбранной темы исследо-вания.
Изученность темы. В ходе своего исследования было установлено, что в настоящее время существует множество интересных и аналитических работ различных авторов, включая ученых, преподавателей, посвященных этой те-ме, что позволило мне подробно проанализировать их, выделить наиболее важные аспекты по этому вопросу и систематизировать полученные данные.
Проблема исследования - выявить методы защиты информации.
Объектом исследования является процесс изучения и применения ме-тодов защиты информации.
Предметом исследования являются основы и принципы применения методов защиты информации.
Цель исследования. Целью данной исследовательской работы является выявление благоприятных условий для применения методов защиты инфор-мации.
Задачи работы. Для достижения цели курсовой работы необходимо решить несколько задач:
- рассмотреть сущность проблемы и задачи защиты информации;
- изучить угрозы информации, а также способы их воздействия на объ-екты защиты информации;
- детально проанализировать традиционные меры и методы защиты ин-формации;
- изучить криптографические методы и средства защиты информации;
- рассмотреть нетрадиционные методы защиты информации;
- проанализировать кодирование как метод защиты информации.
Методология исследования. При написании этой курсовой работы бы-ли использованы следующие методы исследования: анализ литературы, изу-чение документов, наблюдение, описание, сравнение, обобщение, статистиче-ский анализ данных, моделирование.
Источниковая база. В качестве источников были использованы науч-ные статьи, статистика и интернет-ресурсы.
Структура работы. Курсовая работа состоит из введения, двух глав, заключения и списка использованных источников.

ГЛАВА 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

1.1 Сущность проблемы и задачи защиты информации

Широкое использование компьютерных технологий в автоматизирован-ных системах обработки и управления данными обострило проблему защиты информации, циркулирующей в компьютерных системах, от несанкциониро-ванного доступа. Защита информации в компьютерных системах имеет ряд специфических особенностей, поскольку информация не привязана жестко к носителю, может быть легко и быстро скопирована и передана по каналам связи.
Существует очень большое количество информационных угроз, кото-рые могут быть реализованы как внешними, так и внутренними злоумышлен-никами. В области информационной безопасности и компьютерной безопас-ности в целом наиболее актуальными являются три группы проблем:
1. нарушение конфиденциальности информации;
2. нарушение целостности информации;
3. сбои в информационных и компьютерных системах.
Защита информации становится важной проблемой общественной без-опасности, когда речь идет о государственной, дипломатической, военной, промышленной, медицинской, финансовой и другой конфиденциальной, сек-ретной информации. Огромные объемы такой информации хранятся в элек-тронных архивах, обрабатываются в информационных системах и передаются по телекоммуникационным сетям [12]. Наиболее важными характеристиками этой информации являются кон-фиденциальность и целостность, которые должны поддерживаться законом, а также организационными, техническими и программными средствами. Кон-фиденциальность информации (от латинского confidentia - доверие) означает введение определенных ограничений для круга лиц, имеющих доступ к этой информации.
Степень конфиденциальности выражается определенным установлен-ным свойством (особая важность, секретность, секретность для официального использования, не для печати и т.д.), которое субъективно определяется вла-дельцем информации в зависимости от содержания не подлежащей разглаше-нию информации, которая, предназначенная для ограниченного круга лиц, яв-ляется тайной. Конечно, установленный уровень конфиденциальности ин-формации должен поддерживаться при обработке в

информационных систе-мах и при передаче по телекоммуникационным сетям. Еще одним важным свойством информации является ее целостность.
Информация является полной, если она правильно (адекватно) отражает предметную область в любой момент времени. Целостность информации в информационных системах обеспечивается своевременным вводом достовер-ной (корректной) информации, подтверждением достоверности информации, защитой от искажения и уничтожения (удаления). Несанкционированный до-ступ к информации лицами, которым доступ запрещен, преднамеренные или непреднамеренные ошибки операторов, пользователей или программ, непра-вильные изменения информации из-за сбоев оборудования приводят к нару-шению этих важных характеристик и делают эту информацию непригодной для использования и даже опасной. Его использование может привести к ма-териальному и/или моральному ущербу, поэтому создание системы инфор-мационной безопасности становится насущной задачей [7].

1. Гражданский кодекс Российской Федерации. Часть вторая: Феде-ральный закон от 26.01.1996 № 14-ФЗ // СПС Консультант Плюс.
2. Федеральный закон Российской Федерации «Об информации, ин-формационных технологиях и о защите информации от 27 июля 2006 г. № 149-ФЗ» // СПС Консультант Плюс.
3. Федеральный закон Российской Федерации «Об электронной цифровой подписи» от 10 января 2002 года № 1-ФЗ. // СПС Консультант Плюс.
4. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А. Биячуев. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
5. Вихорев, С. Как определить источники угроз / С. Вихорев, Р.Кобцев //Открытые системы. – 2002. - №07-08.- С.43.
6. Волчков А. Современная криптография. // Открытые системы.- 2002. №07-08. С.48.
7. Гмурман, А.И. Информационная безопасность/ А.И. Гмурман - М.: «БИТ-М», 2004.-387с.
8. Дъяченко, С.И. Правовые аспекты работы в ЛВС/ С.И. Дъяченко–СПб.: «АСТ», 2002.- 234с.
9. Зима, В. Безопасность глобальных сетевых технологий / В.Зима, А. Молдовян, Н. Молдовян – СПб.: BHV, 2000. – 320 с.
10. Информатика: Базовый курс / С.В. Симонович [и др]. – СПб.: Пи-тер, 2002. – 640с.:ил.
11. Конахович, Г. Защита информации в телекоммуникационных си-стемах/ Г.Конахович.-М.:МК-Пресс,2005.- 356с.
12. Коржов, В. Стратегия и тактика защиты / В.Коржов //Computerworld Россия.- 2004.-№14.-С.26.
13. Мельников, В. Защита информации в компьютерных системах / В.Мельников - М.: Финансы и статистика, Электронинформ, 1997. – 400с.
14. Молдовян, А.А. Криптография / А.А.Молдовян, Н.А. Молдовян, Советов Б.Я. – СПб.: Издательство “Лань”, 2001. – 224с.,ил.
15. Осмоловский, С. А. Стохастические методы защиты информации/ С. А. Осмоловский – М., Радио и связь, 2002. – 187с.
16. Острейковский, В.А. Информатика: Учеб. пособие для студ. сред. проф. учеб. Заведений/ В.А. Острейковский– М.: Высш. шк., 2001. – 319с.:ил.
17. Семенов, Г. Цифровая подпись. Эллиптические кривые / Г.Семенов // Открытые системы.- 2002. - №07-08. – С.67-68.
18. Титоренко, Г.А. Информационные технологии управления/ Г.А. Титоренко - М.: Юнити, 2002.-376с.
19. Устинов, Г.Н. Уязвимость и информационная безопасность теле-коммуникационных технологий/ Г.Н. Устинов– М.: Радио и связь, 2003.-342с.
20. Шахраманьян, М.А. Новые информационные технологии в зада-чах обеспечения национальной безопасности России/ Шахраманьян, М.А. – М.: ФЦ ВНИИ ГОЧС, 2003.- 222с.
21. Экономическая информатика / под ред. П.В. Конюховского и Д.Н. Колесова. – СПб.: Питер, 2000. – 560с.:ил.
22. Ярочкин, В.И. Информационная безопасность. Учебник для ву-зов/ В.И. Ярочкин– М.: Академический Проект, Мир, 2004. – 544 с.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:
https://stuservis.ru/kursovaya-rabota/366049