**Методические указания по выполнению практических работ по дисциплине «Организационное и правовое обеспечение информационной безопасности»**

**Практическая работа № 1.**

Международные стандарты в области обеспечения информационной безопасности.

Цель: Получение знаний о видах угроз, путей и каналов утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

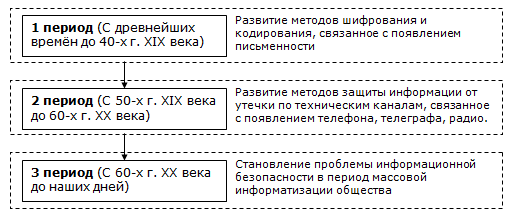
1. Методические указания обучающимся (студентам) по проведению практического занятия.

1.1. При подготовке к занятию.

Краткие теоретические сведения.

Обеспечение защиты информации волновало человечество всегда. В процессе эволюции цивилизации менялись виды информации, для её защиты применялись различные методы и средства.

Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:



Наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в ближайшем будущем привести к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, которые могут принимать форму информационной войны, а сама информационная война станет одним из основных инструментов внешней политики, включая защиту государственных интересов и реализацию любых форм агрессии. Это является одной из причин, почему важно и полезно ознакомиться с основными принципами обеспечения информационной безопасности (ИБ) в ведущих зарубежных странах.

Другая причина заключается в том, что большинство применяемых на территории Российской Федерации средств и методов обеспечения ИБ основаны на международных методиках и строятся из «импортных» компонентов, которые были разработаны в соответствии с нормами и требованиями по обеспечению ИБ стран-изготовителей. В связи с этим прежде чем приступить к изучению непосредственно технологий и средств обеспечения ИБ, следует познакомиться с политикой ИБ ведущих зарубежных стран.

1.2. Задание.

Подготовить краткий отчет (доклад) по заданному вопросу (см. вариант), используя учебное пособие Аверченкова, В.И. «Системы защиты информации в ведущих зарубежных странах» и другие доступные источники информации.

Заполнить таблицу «Системы обеспечения ИБ в ведущих зарубежных странах» (см. вариант) на основе подготовленного материала, а также отчетов (докладов) других обучающихся (студентов).

1.3. Провести анализ собранной информации и сделать выводы.

Содержание отчета:

1) Титульный лист.

2) Содержание.

3) Задание.

4) Таблица «Системы обеспечения ИБ в ведущих зарубежных странах».

5) Выводы.

Варианты: Вариант – номер по списку в журнале.

|  |  |  |  |
| --- | --- | --- | --- |
| Страна | Основные принципы обеспечения ИБ | Основные документы в области обеспечения ИБ | Структура государственных органов обеспечения национальной ИБ |
| США | 1 | 2 | 3 |
| Евросоюз | 4 | 5 | 6 |
| Великобритания | 7 | 8 | 9 |
| Швеция | 10 | 11 | 12 |
| Франция | 13 | 14 | 15 |
| Германия | 16 | 17 | 18 |
| Китай | 19 | 20 | 21 |
| Япония | 22 | 23 | 24 |
| Швейцария | 25 | 26 | 27 |

**Практическое занятие № 2**

Информационная безопасность в условиях функционирования в России глобальных сетей.

Цель занятия: Получение статистических знаний об атаках, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

1. Методические указания обучающимся (студентам) по проведению практического занятия.

1.1. При подготовке к занятию.

В период подготовки к практическому занятию обучающиеся (студенты) получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы № 1 «Российское законодательство в области информационной безопасности», используя литературу [1; 2; 3-11], а также конспект лекций.

При подготовке к практическому занятию обучающимся (студентам) рекомендуется ответить на контрольные вопросы.

1.2. Порядок проведения занятия.

Во время проведения занятия преподаватель осуществляет опрос обучающихся (студентов) и определяет их готовность к занятию.

Затем обучающиеся (студенты) последовательно усваивают учебные вопросы, касающиеся положений Конституции Российской Федерации, Доктрины информационной безопасности РФ и федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия обучающиеся (студенты) оформляют отчет по практической работе и представляют его на подпись преподавателю.

2. Контрольные вопросы.

1) Охарактеризуйте информацию и ее основные показатели.

2) Какие существуют подходы к определению понятия «информация».

3) В чем заключается двуединство документированной информации с правовой точки зрения.

4) Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.

5) К какому виду информации относится записанный на бумаге текст программы для ЭВМ?

6) Назовите основные виды конфиденциальной информации.

7) Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?

8) Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?

9) Охарактеризуйте место правовых мер в системе комплексной защиты информации.

10) Назовите основные цели государства в области обеспечения информационной безопасности.

11) Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.

12) Какой закон определяет понятие «официальный документ»?

13) Какой закон определяет понятие «электронный документ»?

14) В тексте какого закона приведена классификация средств защиты информации?

15) Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?

16) Назовите основные положения Доктрины информационной безопасности РФ.

17) Назовите составляющие правового института государственной тайны.

18) В каких случаях нельзя относить информацию к государственной тайне?

19) Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?

20) Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.

21) Дайте определение системы защиты государственной тайны и укажите ее составляющие.

22) Что в соответствии с законодательством РФ представляет собой засекречивание информации.

23) Перечислите основные принципы засекречивания информации.

24) Что понимается под профессиональной тайной?

25) Какие виды профессиональных тайн вам известны?

26) В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?

27) В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?

28) Что представляет собой электронная подпись?

29) Каковы основные особенности правового режима электронного документа?

30) Назовите основные ограничения на использование электронных документов?

**Практическая работа № 3.**

Информационная безопасность и методология защиты информации.

Цель занятия: Получение знаний о методах защиты информации, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

Методические указания обучающимся (студентам) по проведению практического занятия.

1. Теоретический материал.

Одним из наиболее эффективных методов обеспечения информационной безопасности являются организационно-технические методы.  
Что такое организационно-технические методы обеспечения информационной безопасности? Прежде всего, создание и совершенствование системы обеспечения информационной безопасности, разработка, использование и совершенствование СЗИ и методов контроля их эффективности.   
Этот этап тесно связан с правовыми методами защиты информации, такими как лицензирование (деятельности в области защиты информации), сертификация средств защиты информации и применение уже сертифицированных, и аттестация объектов информатизации по требованиям безопасности информации.

А также организационно технические методы связаны с экономическими, включающими в себя разработку программ обеспечения информационной безопасности Российской Федерации, определение порядка их финансирования, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков.

Защита информации всегда является комплексным мероприятием. В совокупности, организационные и технические мероприятия позволяют предотвратить утечку информации по техническим каналам, предотвратить несанкционированный доступ к защищаемым ресурсам, что в свою очередь обеспечивает целостность и доступность информации при ее обработке, передаче и хранении. Так же техническими мероприятиями могут быть выявлены специальные электронные устройства перехвата информации, установленные в технические средства и защищаемое помещение.

Меры по охране конфиденциальности информации, составляющей коммерческую тайну (Федеральный закон 29.07.2004 № 98-ФЗ):

1) определение перечня информации, составляющей коммерческую тайну;

ограничение доступа к информации, составляющей коммерческую тайну,

путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

2) учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

3) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

4) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Если говорить об экономической стороне защиты информации, всегда важно одно правило – стоимость системы защиты информации не должна превышать стоимость этой информации. Но это не единственное «но» в этом вопросе.

Нецелесообразно защищать всю информацию, какую можем, и все каналы информации какие только есть. Для этого необходимо определить объект защиты.

Основными объектами защиты являются речевая информация и информация обрабатываемая техническими средствами. Так же информация может быть представлена в виде физических полей, информативных электрических сигналов, носителей на бумажной, магнитной, магнито-оптической и иной основе. В связи с этим защите подлежат средства и системы информатизации, участвующие в обработке защищаемой информации (ОТСС), технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается (ВТСС) и защищаемые помещения.

Практическое задание

Ход выполнения работы:

Скопировать папку Y:\ИБ на диск S:\

Создать в папке S:\ИБ каталоги 1, 2, 3, 4.

Запустить программу ArtMasker.exe

В диалоговом режиме выполнить все рекомендации Мастера (в качестве файла-контейнера выбрать) S:\ИБ\фото\Sky\_01.bmp, в качестве маскируемого файла выбрать S:\Virus.doc, задайте параметры скрытия как средние

Сохраните замаскированный файл с именем Security\_1.bmp в папке S:\ИБ\1

Выполнить обратные действия, сохранив размаскированный файл с именем Decod\_1.doc в папке S:\ИБ\1

Переписать в тетрадь текст по описанию ArtMasker:

https://fsd.multiurok.ru/html/2018/11/23/s_5bf7ec9c58ebd/1006750_2.png

ArtMasker - эта программа может прятать информацию в рисунки (BMP 8bit, 16bit, 32bit) и музыкальные файлы (WAV 8bit 16bit). Уникальная возможность этой программы - установка параметров скрытия. Файл-контейнер не меняет своего размера. Имеется поддержка мультиязычности.

Запустить программу SimPass. Создать 5 паролей при помощи генератора, количество букв в пароле 10 (использовать специальные символы и латинские буквы). Выбрать любой понравившийся пароль и скопировать его в буфер.

Запустить программу Secret BMP (в качестве пароля использовать пароль – результат работы генератора паролей)

Создать небольшой!!!! растровый рисунок компьютерного вируса в редакторе PAINT, сохранив его с именем S:\ИБ\2\Pic.bmp

Скрыть файл Pic.bmp в файле S:\ИБ\фото\Sky\_02.bmp, сохранив новый файл с именем Security\_2.bmp в папке S:\ИБ\2 (использовать сгенерированный пароль).

Выполнить обратные действия, сохранив извлеченный файл с именем Decod\_2.bmp в папке S:\ИБ\2

Переписать в тетрадь текст по описанию Secret BMP и Simple Passwords:



Secret BMP - реализация методов стеганографии и криптографии для защиты данных, хранящихся в файлах любого формата. Методы стеганографии применяются для скрытия секретных данных внутри файла-контейнера. В качестве файла контейнера используются файлы растровых изображений формата bmp. Перед скрытием файла в файле-контейнере (bmp-картинке) файл шифруется с использованием метода гаммирования. Для получения гаммы в работе используется 32-разрядный генератор случайных чисел, который программно реализуем и позволяет получать псевдослучайное число.

Simple Passwords - программа для генерирования одновременно нескольких паролей из случайных символов. Позволяет выбрать символы, из которых должен состоять пароль - английские и русские, строчные и прописные, цифры и специальные. Можно указать количество символов в пароле и общее количество генерируемых паролей.

Запустить программу CriptograFF для реализации криптозащиты из файла в файл

Открыть файл для шифрования S:\ИБ\VIP.txt

Зашифровать данный файл, присвоив ему имя S:\ИБ\3\Security\_3.scr

Выполнить обратные действия, сохранив расшифрованный файл с именем Decod\_3.txt в папке S:\ИБ\3

Выполнить криптозащиту открытых файлов

В окне программы набрать текст, где перечислить программно-технические средства защиты информации

Зашифровать открытый файл с именем S:\ИБ\3\Metod.txt

Переписать в тетрадь текст по описанию CriptograFF

https://fsd.multiurok.ru/html/2018/11/23/s_5bf7ec9c58ebd/1006750_4.png

CriptograFF -шифрует текстовые файлы криптографическим методом. Предназначена для шифрования текстовых файлов по алгоритму RC4. Особенности данного алгоритма - большая скорость, возможность потокового шифрования, практическая невозможность вскрытия зашифрованного файла.

Запустить программу Signature Cryptographer

Зашифруйте файл S:\ИБ\фото\Sky\_04.bmp, выбрав в качестве файла-ключа любой свой файл

Сохраните этот файл с именем S:\ИБ\\4\Security\_4

Выполнить обратные действия, сохранив извлеченный файл с именем Decod\_4.bmp в папке S:\ИБ\\4

Переписать в тетрадь текст по описанию Signature Cryptographer:

https://fsd.multiurok.ru/html/2018/11/23/s_5bf7ec9c58ebd/1006750_5.png

Signature Cryptographer - программа защиты информации в важных файлах от несанкционированного доступа. Шифровальщик использует в качестве ключа содержимое файлов вместо строки пароля. Таким образом, длина пароля может достигать гигантских размеров или вовсе быть больше длины шифруемого файла, что делает зашифрованный файл теоретически не взламываемым. Вместо длинных строк пароля запомнить нужно только имя файла, используемого для пароля.

Показать работу преподавателю, получить оценку, удалить с диска S:\ИБ

**Практическая работа № 4**

Правовая защита информационных ресурсов ограниченного доступа. (описать одну тайну)

Цель: научиться определять перечень видов тайн, обрабатываемых в организации.

Составление перечня видов тайн, обрабатываемых в организации.

Оборудование: персональный компьютер, программное обеспечение, интернет

Время: 2 часа

Методические указания обучающимся (студентам) для выполнения практической работы.

Для начала ознакомьтесь с теоретическим материалом.

Теоретический материал.

Согласно Федерального закона № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и защите информации», вся информация делится на:

- информацию ограниченного доступа;

- общедоступную информацию.

Указ Президента Российской Федерации от 06 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера» определяет следующие виды тайн:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. (ФЗ №152-ФЗ «О персональных данных»).

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации. (в ред. Указа Президента РФ от 23.09.2005 № 1111).

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами РФ (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (профессиональная тайна: врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна определена Федеральным законом № 98-ФЗ).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них (интеллектуальная собственность, ГК РФ).

|  |  |  |
| --- | --- | --- |
| Виды тайн | Закон | Содержание |
| Государственная тайна | Закон № 5485-1 «О государственной тайне». | Информация, распространение которой может нанести ущерб РФ. |
| Коммерческая тайна | Федеральный закон № 98-ФЗ «О коммерческой тайне». | Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. |
| Служебная тайна | - Указ Президента РФ от 6.03.1997 № 188;  - Гражданский кодекс РФ;  - Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 02.07.2021) «О государственной гражданской службе Российской Федерации»;  - ПП РФ от 3.11.94 № 1233. | Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами РФ. |
| Профессиональная тайна:  - тайна связи;  - медицинская тайна | - Указ Президента РФ от 6.03.1997 № 188;  - Федеральный закон от 17.07.1999 № 176-ФЗ (ред. от 27.12.2019) «О почтовой связи»;  - Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 02.07.2021) «О связи»;  - Уголовно-процессуальный кодекс РФ;  - «Семейный кодекс Российской Федерации» от 29.12.1995 № 223-ФЗ (ред. от 02.07.2021). | Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.  Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе заболевания, иные сведения, полученные при обследовании и лечении гражданина, а также сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора. |
| Персональные данные | Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных». | персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). |

В зависимости от рода деятельности на предприятии (в организации) может одновременно обрабатываться информация, относящаяся к разным видам информации ограниченного доступа.

|  |  |
| --- | --- |
| Форма собственности | Виды тайн |
| Государственная | ГТ, СТ, ПрТ, ПДн |
| Муниципальная | СТ, ПрТ, ПДн |
| Коммерческая | КТ, ПрТ, ПДн |
| Индивидуальная | КТ, ПрТ, ПДн |

Контрольные вопросы:

1) Наименование федерального закона определяющего ограничения на доступ к информации?

2) В каком документе РФ определен перечень видов тайн?

3) Наименование закона, определяющего ГТ?

**Практическая работа № 5.**

Методы криптографии

Цель: Изучить протоколирование и аудит, а также криптографические методы защиты. Показать их место в общей архитектуре безопасности.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

Методические указания обучающимся (студентам) по выполнению практического задания.

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;

алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;

гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;

аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы.

Для симметричной криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений.

В асимметричных криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Н | О | Н | С | Б | Н | Я |
| Е | Е | О | Я | О | Е | Т |
| Я | С | В | Е | Л | П | Н |
| С | Т | И | Щ | Е | О | Ы |
| Н | А | Т | Е | Е | Н | М |

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Насколько большей стойкостью к раскрытию обладает метод одиночной перестановки по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Л | У | Н | А | Т | И | К |  |  | А | И | К | Л | Н | Т | У |
| 4 | 7 | 5 | 1 | 6 | 2 | 3 |  |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Н | О | Н | С | Б | Н | Я |  |  | С | Н | Я | Н | Н | Б | О |
| Е | Е | О | Я | О | Е | Т |  |  | Я | Е | Т | Е | О | О | Е |
| Я | С | В | Е | Л | П | Н |  |  | Е | П | Н | Я | В | Л | С |
| С | Т | И | Щ | Е | О | Ы |  |  | Щ | О | Ы | С | И | Е | Т |
| Н | А | Т | Е | Е | Н | М |  |  | Е | Н | М | Н | Т | Е | А |

До перестановки / после перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо.

Получается шифровка: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение «Приезжаю\_шестого» можно зашифровать следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 4 | 1 | 3 |  |  | 1 | 2 | 3 | 4 |  |  | 1 | 2 | 3 | 4 |
| 4 | П | Р | И | Е |  | 4 | И | П | Е | Р |  | 1 | А | З | Ю | Ж |
| 1 | З | Ж | А | Ю |  | 1 | А | 3 | Ю | Ж |  | 2 | Е | \_ | С | Ш |
| 2 | \_ | Ш | Е | С |  | 2 | Е. | \_ | С | Ш |  | 3 | Г | Т | О | О |
| 3 | Т | О | Г | О |  | 3 | Г | Т | О | О |  | 4 | И | П | Е | Р |

Двойная перестановка столбцов и строк.

В результате перестановки получена шифровка АЗЮЖЕ\_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5\*5 их 14400.

В средние века для шифрования применялись и магические квадраты. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 3 | 2 | 13 |  |  | О | И | Р | Т |
| 5 | 10 | 11 | 8 |  |  | З | Ш | Е | Ю |
| 9 | 6 | 7 | 12 |  |  | \_ | Ж | А | С |
| 4 | 15 | 14 | 1 |  |  | Е | Г | О | П |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | Р | И | Е | З | Ж | А | Ю | \_ | Ш | Е | С | Т | О | Г | О |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3\*3 таких квадратов -1; для таблицы 4\*4 - 880; а для таблицы 5\*5-250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый полибианский квадрат размером 5\*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда.

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В шифрах многоалфавитной замены для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

|  |  |
| --- | --- |
|  | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| А | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| Б | \_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ |
| В | Я\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ |
| Г | ЮЯ\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ |
| . | ………… |
| Я | ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_АБ |
| \_ | БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_А |

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом.

При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют.

Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ\_ШЕСТОГО получаем следующую шифровку:

|  |  |
| --- | --- |
| Сообщение | ПРИЕЗЖАЮ\_ШЕСТОГО |
| Ключ | АГАВААГАВААГАВАА |
| Шифровка | ПНИГЗЖЮЮЮАЕОТМГО |

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки Т(0)i одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков Г(ш)i аналогичной длины (Т(ш)i=Г(ш)i+Т(0)i, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные T(0)i=Г(ш)i+Т(ш)i.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

Получатель сообщения выбирает два больших числа P и G, причем P G.

Получатель выбирает секретный ключ - случайное целое число X P.

Вычисляется открытый ключ Y= G x mod P.

Получатель выбирает целое число K, 1P-1.

Шифрование сообщения (M): a= GK mod P, b=Y K M mod P, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания открытого и секретного ключей:

Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет n=p\*q и функцию Эйлера φ(n)=(p-1)(q-1).

Получатель выбирает целое число е (1e φ(n)), взаимно простое со значением функции φ(n).

Пара чисел (e,n) публикуется в качестве открытого ключа.

Получатель вычисляет целое число d, которое отвечает условию: e\*d=1(mod φ(n) ).

Пара чисел (d,n) является секретным ключом.

Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как c=mе mod(n).

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение с: m=cd mod (n).

3. Задание

Практическая работа состоит из двух частей:

Часть 1 – применение одного из алгоритмов симметричного шифрования;

Часть 2 – шифрование с использованием алгоритма RSA.

Порядок выполнения работы:

Часть 1:

Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.

Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).

Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m1, m2, m3 (см. вариант).

Содержание отчета:

Титульный лист

Содержание

Задание: Применение алгоритма симметричного шифрования. Применение алгоритма асимметричного шифрования

4.1. Программа шифрования и дешифрования сообщения при помощи алгоритма RSA.

4.2. Результаты шифрования и дешифрования заданных сообщений.

Выводы

Варианты: Вариант – номер по списку в журнале.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер по списку в журнале | Исходные данные | | | | | | | |
| Часть 1 | Часть 2 | | | | | | |
| Номер варианта | Алгоритм шифрования | p | q | e | d | 1 | m2 | 3 |
| 1 | Простая перестановка | 3 | 1 | 7 | 3 | 9 | 12 | 3 |
| 2 | Одиночная перестановка | 7 | 1 | 7 | 3 | 8 | 15 | 5 |
| 3 | Двойная перестановка | 3 | 7 | 5 | 9 | 3 | 16 | 5 |
| 4 | Магический квадрат | 01 | 13 | 533 | 597 | 6 | 19 | 3 |
| 5 | Шифр Цезаря | 7 | 1 | 7 | 3 | 8 | 18 | 1 |
| 6 | Полибианский квадрат | 7 | 7 | 5 | 7 | 9 | 11 | 6 |
| 7 | Шифр Гронсфельда | 3 | 1 | 7 | 3 | 8 | 13 | 5 |
| 8 | Многоалфавитная замена | 7 | 1 | 7 | 3 | 7 | 14 | 7 |
| 9 | Простая перестановка | 3 | 7 | 5 | 9 | 2 | 17 | 5 |
| 10 | Одиночная перестановка | 7 | 1 | 7 | 3 | 3 | 20 | 1 |
| 11 | Двойная перестановка | 3 | 7 | 5 | 9 | 2 | 12 | 5 |
| 12 | Магический квадрат | 01 | 13 | 533 | 597 | 3 | 15 | 6 |
| 13 | Шифр Цезаря | 7 | 1 | 7 | 3 | 3 | 16 | 4 |
| 14 | Полибианский квадрат | 7 | 7 | 5 | 7 | 3 | 19 | 6 |
| 15 | Шифр Гронсфельда | 3 | 1 | 7 | 3 | 4 | 18 | 5 |
| 16 | Многоалфавитная замена | 7 | 1 | 7 | 3 | 5 | 11 | 4 |
| 17 | Простая перестановка | 01 | 13 | 533 | 597 | 4 | 13 | 1 |
| 18 | Одиночная перестановка | 7 | 1 | 7 | 3 | 7 | 14 | 4 |
| 19 | Двойная перестановка | 7 | 7 | 5 | 7 | 7 | 17 | 3 |
| 20 | Магический квадрат | 3 | 1 | 7 | 3 | 5 | 20 | 3 |
| 21 | Шифр Цезаря | 7 | 1 | 7 | 3 | 2 | 11 | 5 |
| 22 | Полибианский квадрат | 3 | 7 | 5 | 9 | 3 | 13 | 7 |
| 23 | Шифр Гронсфельда | 7 | 1 | 7 | 3 | 2 | 14 | 9 |
| 24 | Многоалфавитная замена | 3 | 7 | 5 | 9 | 5 | 17 | 6 |
| 25 | Простая перестановка | 01 | 13 | 533 | 597 | 6 | 20 | 2 |
| 26 | Одиночная перестановка | 7 | 1 | 7 | 3 | 5 | 14 | 6 |
| 27 | Двойная перестановка | 7 | 7 | 5 | 7 | 4 | 17 | 4 |
| 28 | Магический квадрат | 3 | 1 | 7 | 3 | 8 | 20 | 2 |
| 29 | Одиночная перестановка | 7 | 7 | 5 | 7 | 4 | 13 | 1 |
| 30 | Шифр Гронсфельда | 3 | 7 | 5 | 9 | 9 | 11 | 8 |

**Практическая работа № 6**

Идентификация и аутентификация объектов сети.

Цель: провести идентификацию и аутентификацию.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа.

Методические указания обучающимся (студентам) по проведению практического занятия.

Теоретический материал.

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация уста­навливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиден­циальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе ОРГАНИЗАЦИИ (АС ОРГАНИЗАЦИИ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС ОРГАНИЗАЦИИ и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудников службы обеспечения безопасности информации (СОБИ) - администраторов средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников СОБИ. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников СОБИ, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников подразделений ОРГАНИЗАЦИИ (исполнителей).

4. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать уполномоченного представителя службы обеспечения безопасности информации (СОБИ).

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа ОРГАНИЗАЦИИ и т.п.) должна производиться уполномоченными сотрудниками СОБИ – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального органа ОРГАНИЗАЦИИ и другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.6 или п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале (возможно вместе с персональными ключевыми дискетами и идентификатором Touch Memory).

10. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на сотрудников СОБИ – администраторов средств парольной защиты.

Контрольные вопросы:

1. Перечислить виды паролей

2. От чего зависит надежность пароля?

3. Что такое парольная политика?

**Практическая работа № 7**.

Принципы разработки СЗИ.

Цель: Ознакомиться с принципами построения VPN на базе программного обеспечения.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

Методические указания для студентов для выполнения практического задания.

Краткие теоретические сведения

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, интернет).

Виртуальная частная сеть базируется на трех метoдах реализации:

Туннелирoвание;

Шифрoвание;

Аутентификация.

Hamachi— это программа, позволяющая создать виртуальную частную сеть (VPN) через Интернет и объединить в ней несколько компьютеров. После создания такой сети пользователи могут устанавливать VPN-сессии между собой и работать в этой сети точно так же, как в обычной локальной (LAN) сети с возможностью обмена файлами, удаленного администрирования компьютеров и т.д. Преимущество VPN-сети заключается в том, что она полностью защищена от несанкционированного вмешательства и невидима из Интернета, хотя и существует в нем.

Программа Hamachi должна быть установлена на всех компьютерах, которые предполагается объединить в виртуальную частную сеть.

Виртуальная сеть создается с помощью специализированного сервера Hamachi в Интернете.

После того как с помощью сервера Hamachi создается виртуальная сеть между выбранными компьютерами, обмен информацией между клиентами VPN-сети происходит уже напрямую, то есть без участия сервера Hamachi. Для обмена данными между клиентами VPN-сети используется протокол UDP.

3. Задание

Задание рассчитано на работу в паре.

Порядок выполнения задания:

Загрузить программу «LogMeIn Hamachi» с сайта http://hamachi.ru.softonic.com/ на оба компьютера будущей сети.

Создать сеть, пользуясь подсказками на сайте http://hamachiinfo.ru/nastrojka.html

Объединить в сеть принтер, камеру или другое устройство либо развернуть в сети какое-либо программное обеспечение (например, игру).

Подготовить отчет.

**Практическая работа № 8.**

Специализированные программно-аппаратные средства защиты информации.

Цель: Изучить порядок вычисления и проверки ЭП (электронной подписи)

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

Методические указания обучающимся (студентам) для выполнения практического задания.

1. Краткие теоретические сведения.

Программно-аппаратные средства защиты информации - это сервисы безопасности, встроенные в сетевые операционные системы. К сервисам безопасности относятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование

В настоящее время повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между ними, между отдельными пользователями. Все большее значение в данной сфере приобретает электронный документооборот, позволяющий отказаться от бумажных носителей (или снизить их долю в общем потоке) и осуществлять обмен документами между субъектами в электронном виде. Однако переход от бумажного документооборота к электронному ставит ряд проблем, связанных с обеспечением целостности (подлинности) передаваемого документа и аутентификации подлинности его автора.

Следует отметить, что известные в теории информации методы защиты сообщений, передаваемых по каналам связи, от случайных помех не работают в том случае, когда злоумышленник преднамеренно реализует угрозу нарушения целостности информации. Например, контрольные суммы, используемые для этой цели передатчиком и приемником, могут быть пересчитаны злоумышленником так, что приемником изменение сообщения не будет обнаружено. Для обеспечения целостности электронных документов и установления подлинности авторства необходимо использовать иные методы, отличные от контрольных сумм. Для решения данных задач используют технологию электронно-цифровой подписи.

Электронно-цифровая подпись (ЭП) сообщения является уникальной последовательностью, связываемой с сообщением, подлежащей проверке на принимающей стороне с целью обеспечения целостности передаваемого сообщения и подтверждения его авторства.

Процедура установки ЭП использует секретный ключ отправителя сообщения, а процедура проверки ЭП – открытый ключ отправителя сообщения (рис. 1).

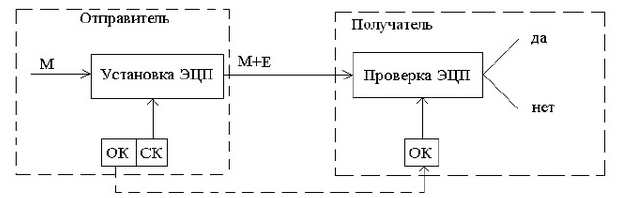


Рис. 1 – Схема использования ЭП.

Здесь М – электронный документ. Е – электронная подпись.

В технологии ЭП ведущее значение имеют однонаправленные функции хэширования. Использование функций хэширования позволяет формировать криптографически стойкие контрольные суммы передаваемых сообщений.

Функцией хэширования H называют функцию, сжимающую сообщение произвольной длины M, в значение фиксированной длины H(M) (несколько десятков или сотен бит), и обладающую свойствами необратимости, рассеивания и чувствительности к изменениям. Значение H(M) обычно называют дайджестом сообщения M.

Схема установки ЭП (рис. 2):

1. Для документа М формируется дайджест H с помощью заданного алгоритма хэширования.

2. Сформированный дайджест H шифруют на секретном ключе отправителя сообщения. Полученная в результате шифрования последовательность и есть ЭП.

3. Сообщение М и его ЭП передаются получателю сообщения.

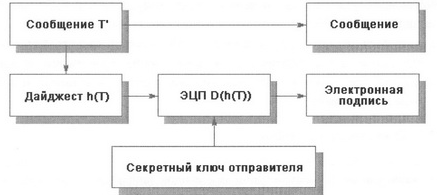


Рис. 2 – Схема установки ЭП.

Схема проверки ЭП (рис. 3):

1. Получатель для проверки ЭП должен иметь доступ к самому сообщению М и его ЭП.

2. Зная алгоритм хэширования, который был использован при установке ЭП, получатель получает дайджест H1 присланного сообщения М.

3. Зная открытый ключ отправителя, получатель дешифрует ЭП, в результате чего получает дайджест H2, сформированный на этапе установки ЭП.

4. Критерием целостности присланного сообщения М и подтверждения его автора является совпадение дайджестов H1 и H2. Если это равенство не выполнено, то принимается решение о некорректности ЭП.

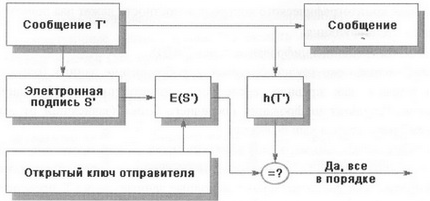


Рис. 3 – Схема проверки ЭЦП.

Задание

Сформировать ЭП к сообщению M' (см. вариант) и произвести проверку целостности принятого сообщения.

Порядок выполнения работы:

Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.

На стороне отправителя выполнить следующие действия:

Записать сообщение M (см. вариант).

Сформировать профиль сообщения M’ с помощью упрощенной функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения.

Создать ЭП шифрованием профиля сообщения h(M’) закрытым ключом отправителя Da (значение ключа (d, n) см. в таблице с вариантами задания), т.е. Da (h(M’)) (см. вариант).

На стороне получателя выполнить следующие действия:

Записать сообщение М (его получает получатель вместе с ЭП) и ЭП Da (h(M’)).

Сформировать профиль принятого сообщения, M’ с помощью той же функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения (Получателю известен алгоритм хэширования, применяемый на стороне отправителя).

Создать профиль дешифрованием ЭП открытым ключём отправителя (Ea (Da (h(M’)) = h(M’)) (значение ключа (е, n) см. в таблице с вариантами задания).

Сравнить два профиля сообщения h(M’) (п.3.2 и 3.3).

Убедиться в их совпадении.

Варианты: Вариант – номер по списку в журнале.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Номер варианта | p | q | е | d | М |
| 1 | 3 | 11 | 7 | 3 | 5523 |
| 3 | 17 | 11 | 7 | 23 | 8866 |
| 3 | 13 | 7 | 5 | 29 | 3565 |
| 4 | 101 | 113 | 3533 | 6597 | 6546 |
| 5 | 3 | 11 | 7 | 3 | 8562 |
| 6 | 17 | 11 | 7 | 23 | 9795 |
| 7 | 13 | 7 | 5 | 29 | 8462 |
| 8 | 17 | 11 | 7 | 23 | 7785 |
| 9 | 13 | 7 | 5 | 29 | 2123 |
| 10 | 101 | 113 | 3533 | 6597 | 3145 |
| 11 | 7 | 11 | 37 | 13 | 2566 |
| 12 | 101 | 113 | 3533 | 6597 | 3782 |
| 13 | 3 | 11 | 7 | 3 | 3465 |
| 14 | 17 | 11 | 7 | 23 | 3895 |
| 15 | 13 | 7 | 5 | 29 | 4132 |
| 16 | 17 | 11 | 7 | 23 | 5123 |
| 17 | 13 | 7 | 5 | 29 | 4416 |
| 18 | 101 | 113 | 3533 | 6597 | 7895 |
| 19 | 3 | 11 | 7 | 3 | 7459 |
| 20 | 17 | 11 | 7 | 23 | 5654 |
| 21 | 13 | 7 | 5 | 29 | 2456 |
| 22 | 17 | 11 | 7 | 23 | 3585 |
| 23 | 13 | 7 | 5 | 29 | 2652 |
| 24 | 101 | 113 | 3533 | 6597 | 5656 |
| 25 | 3 | 11 | 7 | 3 | 6685 |
| 26 | 17 | 11 | 7 | 23 | 5566 |
| 27 | 13 | 7 | 5 | 29 | 4652 |
| 28 | 17 | 11 | 7 | 23 | 8666 |
| 29 | 13 | 7 | 5 | 29 | 4556 |
| 30 | 101 | 113 | 3533 | 6597 | 9266 |

**Практическая работа № 9**.

Виды противников или «нарушителей». Понятие о видах вируса.

Цель: Получение знаний о существующих «компьютерных вирусах» и об алгоритмах их работы. Ознакомление с основными функциями, достоинствами и недостатками современного антивирусного ПО.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время:2 часа

Методические указания обучающимся (студентам) для выполнения практического задания.

1. Краткие теоретические сведения

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

сканирование памяти и содержимого дисков;

сканирование в реальном режиме времени с помощью резидентного модуля;

распознавание поведения, характерного для компьютерных вирусов;

блокировка и/или удаление выявленных вирусов;

восстановление зараженных информационных объектов;

принудительная проверка подключенных к корпоративной сети компьютеров;

удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;

фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;

выявление потенциально опасных Java-апплетов и модулей ActiveX;

ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

Задание

Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.

Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.

Заполнить таблицу «Пакеты антивирусных программ» на основе подготовленного материала, а также докладов других студентов.

Провести анализ собранной информации и сделать выводы.

**Практическая работа № 10**.

Антивирусные программы (описать один вид).

Цель: Выработать практические навыки работы с антивирусными программами, навыки правильной работы с компьютером. Ознакомление с основными функциями, достоинствами и недостатками современного антивирусного ПО.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

Методические указания для студентов для выполнения практического задания.

1. Краткие теоретические сведения

В настоящее время перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

сканирование памяти и содержимого дисков;

сканирование в реальном режиме времени с помощью резидентного модуля;

распознавание поведения, характерного для компьютерных вирусов;

блокировка и/или удаление выявленных вирусов;

восстановление зараженных информационных объектов;

принудительная проверка подключенных к корпоративной сети компьютеров;

удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;

фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;

выявление потенциально опасных Java-апплетов и модулей ActiveX;

ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

Задание

Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.

Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.

Заполнить таблицу «Пакеты антивирусных программ» на основе подготовленного материала, а также докладов других обучающихся (студентов).

Провести анализ собранной информации и сделать выводы.

Содержание отчета

Титульный лист

Содержание

Задание

Таблица «Пакеты антивирусных программ»

Выводы

Варианты: Вариант – номер по списку в журнале.

|  |  |  |  |
| --- | --- | --- | --- |
| Пакет антивирусного ПО | Основные функции | Достоинства | Недостатки |
| Антивирус Касперского | 1 | 2 | 3 |
| Антивирус Dr.Web для Windows | 4 | 5 | 6 |
| Panda Antivirus | 7 | 8 | 9 |
| ESET NOD32 Антивирус | 10 | 11 | 12 |
| avast! Free Antivirus | 13 | 14 | 15 |
| Avira AntiVir Personal | 16 | 17 | 18 |
| Norton AntiVirus | 19 | 20 | 21 |
| Trend Micro Internet Security | 22 | 23 | 24 |
| Microsoft Security Essentials | 25 | 26 | 27 |
| McAfee VirusScan | 28 | 29 | 30 |

**Практическая работа № 11**.

Виды служб безопасности по защите информации.

Цель: Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа

Методические указания для студентов для выполнения практического задания

1. Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – Концепции и Политики информационной безопасности. Если Концепция ИБ в общих чертах определяет, ЧТО необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит КАК, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

1. принятия обоснованных управленческих решений по разработке мер защиты информации;
2. выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
3. координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
4. и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности.

3. Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности.

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия. Классификации угроз. Основные непреднамеренные искусственные угрозы. Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия.

4.1. Организационное обеспечение информационной безопасности.

Задачи организационного обеспечения информационной безопасности.

Подразделения, занятые в обеспечении информационной безопасности.

Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

Общие положения.

Защита информационных ресурсов от несанкционированного доступа.

Средства комплексной защиты от потенциальных угроз.

Обеспечение качества в системе безопасности.

Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия. Правовое обеспечение юридических отношений с работниками Предприятия. Правовое обеспечение юридических отношений с партнерами Предприятия. Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия.

**Практическая работа №** **12**.

Физические средства защиты информации.

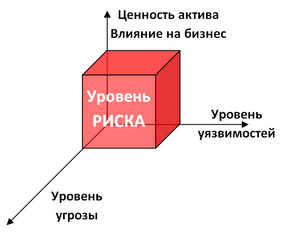
Цель: Ознакомиться с алгоритмами оценки риска информационной безопасности.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа.

Методические указания для выполнения практического задания

1. Краткие теоретические сведения.

Риск ИБ – потенциальная возможность использования определенной угрозой уязвимостей актива или группы активов для причинения вреда организации.

Уязвимость - слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ - совокупность условий и факторов, которые могут стать причиной нарушений целостности, доступности, конфиденциальности информации.

Информационный актив – это материальный или нематериальный объект, который:

- является информацией или содержит информацию,

- служит для обработки, хранения или передачи информации,

- имеет ценность для организации.

3. Задание

Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»

Ознакомьтесь с Приложениями C, D и Е ГОСТа.

Выберите три различных информационных актива организации (см. вариант).

Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

Пользуясь Приложением С ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

Пользуясь одним из методов (см. вариант) предложенных в Приложении Е ГОСТа произведите оценку рисков информационной безопасности.

Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

**Практическое занятие № 13**.

Особенности современных информационных систем, существенные с точки зрения безопасности.

Цель: Изучить особенности современных информационных систем, существенные с точки зрения безопасности.

Оборудование: персональный компьютер, программное обеспечение, интернет.

Время: 2 часа.

Методические указания обучающимся (студентам) для выполнения практического задания.

1. Краткие теоретические сведения.

Простота и управляемость ИС в целом и защитных средств в особенности. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (например, таблицы базы данных) доступны через Интернет, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет уязвимой, сложной и плохо управляемой.

Продуманная и упорядоченная структура программных средств и баз данных. Топология внутренних и внешних сетей непосредственно отражается на достигаемом качестве и безопасности ИС, а также на трудоемкости их разработки. При строгом соблюдении правил структурного построения значительно облегчается достижение высоких показателей качества и безопасности, так как сокращается число возможных ошибок в реализующих программах, отказов и сбоев оборудования, упрощается ихдиагностика и локализация.

В хорошо структурированной системе с четко выделенными компонентами (клиент, сервер приложений, ресурсный сервер) контрольные точки выделяются достаточно четко, что решает задачу доказательства достаточности применяемых средств защиты и обеспечения невозможности обхода этих средств потенциальным нарушителем.

Высокие требования, предъявляемые к формированию архитектуры и инфраструктуры на стадии проектирования ИС, определяются тем, что именно на этой стадии можно в значительной степени минимизировать число уязвимостей, связанных с непредумышленными дестабилизирующими факторами, которые влияют на безопасность программных средств, баз данных и систем коммуникации.

Анализ безопасности ИС при отсутствии злоумышленных факторов базируется на модели взаимодействия основных компонент ИС (рис.1) [Липаев В. В., 1997].

В качестве объектов уязвимости рассматриваются:

1) динамический вычислительный процесс обработки данных, автоматизированной подготовки решений и выработки управляющих воздействий;

2) объектный код программ, исполняемых вычислительными средствами в процессе функционирования ИС;

3) данные и информация, накопленная в базах данных;

4) информация, выдаваемая потребителям и на исполнительные механизмы.



Рис.1 Модель анализа безопасности информационных систем при отсутствии злоумышленных угроз.

Полное устранение перечисленных угроз принципиально невозможно. Задача состоит в выявлении факторов, от которых они зависят, в создании методов и средств уменьшения их влияния на безопасность ИС, а также в эффективном распределении ресурсов для обеспечения защиты, равнопрочной по отношению ко всем негативным воздействиям.

Задание:

построить модель информационной безопасности организации, предприятия.

**Список литературы**

1. Казанцев С.Я, Згадзай О.Э. и др. Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений/ под ред. С.Я. Казанцева. - 2-е изд., испр. и доп. – М.: Издательский центр «Академия», 2007.

2. Сытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2003.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

5. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

6. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

7. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

8. Федеральный закон от 08.08.2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».

9. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».