МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность и защита информации

Кафедра **Информатики и информационных технологий**

факультета **Информатики и информационных технллогий**

Образовательная программа

09.03.02 «Информационные системы и технологии»

Профиль подготовки

Информационные системы и технологии

Уровень высшего образования

Бакалавриат

Форма обучения

очная

Статус дисциплины: **вариативная (обязательная)**

Махачкала 2016

Рабочая программа дисциплины составлена в 2016 году в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии», профиль подготовки «Информационные системы и технологии» (уровень бакалавриат), утвержденного приказом Минобрнауки РФ от 12 марта 2015 г. № 219, вступил в силу 30 марта 2015 г.

Разработчик: кафедра информатики и информационных технологий,
Абдуллаев Габид Шаванович, кандидат экономических наук, доцент

Рабочая программа дисциплины одобрена:
на заседании кафедры Информатики и информационных технологий
от «02» 07 2016 г., протокол № 1

Зав. кафедрой _____ проф. Ахмедов С.А.
(подпись)

на заседании Методической комиссии факультета Информатики и информационных технологий

от «07» X 2016 г., протокол № 1.

Председатель _____ доц. Камилов К.Б.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «7» 10 2016 г.

Цели дисциплины

Целями изучения дисциплины «Информационная безопасность и защита информации» является:

формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ;

создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ;

развитие способностей по использованию существующей системы управления информационной безопасности.

Место дисциплины в структуре ООП

Учебная программа дисциплины «Информационная безопасность и защита информации» является дисциплиной вариативнов (обязательной) части профессионального цикла дисциплин ООП по направлению 09.03.02 «Информационные системы и технологии» (бакалавриат).

Изучение дисциплины базируется на знаниях, полученных студентами при изучении дисциплин «информационные процессы обмена данными», «надежность информационных систем», «администрирование в информационных системах». Изучение дисциплины позволяет овладеть как теоретической базой, так и конкретными практическими навыками по организации информационной безопасности.

Требования к результатам освоения дисциплины

В совокупности с дисциплинами базовой и вариативной части профессионального цикла ФГОС ВПО дисциплина «Информационная безопасность и защита информации» обеспечивает инструментарий формирования следующих общекультурных (ОК) и профессиональных (ПК) компетенций:

№ п/п	Код	Компетенция	Формы и методы обучения
1	ОК-6	Владение широкой общей подготовкой (базовыми знаниями) для решения	Лекции. Практические занятия. Работа с источниками и поиск информаций в Интернете. Решение проблемных задач связанных с
2	ПК-32	Способность поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества	

3	ПК-33	Готовность обеспечивать безопасность и целостность данных информационных систем и технологий	методологией управления информационной безопасностью. Обсуждение актуальных вопросов, связанных с перспективными направлениями развития науки и техники в области защиты информации. Выступления студентов с докладами и презентациями.

В результате освоения дисциплины «Управление информационной безопасностью» студент должен:

знать:

 основные понятия, термины, определения в бизнес-процессах, а также понятия анализа видов информации, в которых данные процессы проявляются: учредительная и лицензионная база организации, правовая сфера бизнеса, внутренняя нормативная база организации, внешняя и внутренняя отчетность, материальные и информационные активы;

 основные методики оценки уровня информационной безопасности организации и примеры их использования;

 основные методы противодействия «внутренним» угрозам информационной безопасности организации;

 архитектуру основных стандартов защиты информации;

уметь:

 использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы организационного проектирования, методы управления информационными активами организации;

Владеть навыками:

 использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации как систематической практической деятельности коллегиальных органов управления

организацией и руководителя службы, направленной на формирование и поддержание концептуальных и организационных основ деятельности организации и эффективное выполнение поставленных задач.

Объём дисциплины и виды учебной работы

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 4 зачётные единицы.

Вид промежуточной аттестации – экзамен.

Вид учебной работы	**Часы**	**Семестр**
		6
Общая трудоёмкость дисциплины	**144**	**144**
Аудиторные занятия	**54**	**54**
Лекции (Л)	32	32
Лабораторные занятия	16	16
КСР	6	6
Самостоятельная работа (СР)	**90**	**90**
В семестре	**63**	**63**
В сессию	**27**	**27**

Содержание дисциплины

Часть 1. Содержание дисциплины

Тема 1. Современные проблемы ИБ

Информационная безопасность и проблемы защиты информации. Ретроспективный анализ развития подходов к защите информации. Современная постановка задачи защиты информации. Сущность, необходимость, пути и условия перехода к интенсивным способам защиты информации

Тема 2. Основные понятия и определения в области информационной безопасности автоматизированных систем

Концепция информационной безопасности. Основные составляющие. Важность проблемы. Доступность, целостность и конфиденциальность информационных ресурсов. Основные положения теории информационной безопасности информационных систем.

Тема 3. Угрозы и уязвимости информации

Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной

(случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные

Тема 4. Политика безопасности

Основные понятия политики безопасности. Структура политики безопасности организации. Разработка политики безопасности организации.

Тема 5. Организационно-правовое обеспечение информационной безопасности

Российское и зарубежное законодательство в области информационной безопасности и проблемы, которые существуют в настоящее время в российском законодательстве. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно- справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Тема 6. Стандарты информационной безопасности

Обзор международных и национальных стандартов и спецификаций в области информационной безопасности - от "Оранжевой книги" до ISO 15408. Политики безопасности. Уровень гарантированности. Доверенная вычислительная база. Периметр безопасности. Классы безопасности. Международные стандарты информационного обмена.

Тема 7. Проблемы информационной безопасности сетей

ведение в сетевой информационный обмен, анализ угроз сетевой безопасности, обеспечение информационной безопасности сетей

Раздел2.Теоретические основы информационной безопасности

Тема 8. Криптографическая защита информации

Общесистемные аспекты криптологии, основные понятия криптологии, криптографические алгоритмы, шифры перестановки, шифры замены, симметричные блочные шифры, ассиметричные шифры.

Тема 9. Защита информации от НСД

Общесистемные аспекты, способы защиты идентификация и аутентификация, методы реализации контроля и разграничения доступа, способы контроля и управления доступом, механизмы контроля и разграничения доступа протоколирование и аудит, экранирование.

Тема 10. Технологии защиты от вирусов

Понятия о видах вирусов. Типология компьютерных вирусов. Программные и скриптовые вирусы. Файловые, бутовые и сетевые вирусы. Черви. Программы-шпионы. Признаки заражения компьютерной системы вирусом. Методы заражения компьютерных систем. Наиболее распространенные виды антивирусного программного обеспечения. Антивирус Касперского. Нортон-Антивирус. Рейтинги антивирусных систем

Тема 11. Технологии обнаружения атак и история их развития

Сбор исходной информации системами обнаружения атак, методы обнаружения информационных атак, противодействие выявленным информационным атакам, проблема выбора системы обнаружения информационных атак

Тема 12. Практические аспекты защиты веб-порталов от атак

Подсистема разграничения доступа, подсистема антивирусной защиты, подсистема контроля целостности, подсистема обнаружения вторжений, подсистема анализа защищенности, подсистема криптографической защиты, подсистема управления средствами защиты.

Тема 13. Методы построения защищенных баз данных

Актуальность защиты БД. Основные понятия и методы защиты: защита паролем, шифрование, разграничение прав доступа. Правовая охрана баз данных.

Тема 14. Технологии межсетевых экранов

Функции межсетевых экранов, особенности функционирования межсетевых экранов на различных уровнях модели ОБ, схемы сетевой защиты на базе межсетевых экранов

Темы дисциплины и виды учебных занятий
(учебно – тематический план)

Названияразделов и тем	Всего часов	Трудоёмкость в часах			
		Аудиторныезанятия,в томч исле			Самостоятельная работа
		общая	лекции	Лабор. работ	
Модуль1.Проблемы информационной безопасности.					
Тема 1.Современные проблемы ИБ	6	2	2		4
Тема 2.Основные понятия и определения в области информационной	6	4	2	2	4
Тема 3.Угрозы и уязвимости	6	4	2	2	4
Тема 4.Политика безопасности	6	2	2		4
Тема 5.Организационно-правовое обеспечение информационной	10	2	2		4

Тема 6.Стандарты информационной безопасности	10	4	2	2	4
Тема 7. Проблемы информационной безопасности сетей	10	2	2		4
Модуль 2.Технологии защиты данных					
Тема 8.Криптографическая защита информации	18	6	4	2	6
Тема 9.Защита информации от НСД	1	4	2	2	5
Тема 10. Технологии защиты от	1	4	2	2	4
Тема 11.Технологии обнаружения атак и	12	2	2		5
Тема 12.Практические аспекты защиты веб-	12	4	2	2	5
Тема 13. Методы построения защищенных	16	6	4	2	6
Тема 14. Технологии межсетевых	1	2	2		4
КСР		6			
Подготовка к экзамену	2				
ИТОГО	144	54	32	16	63

Лабораторныеработы(лабораторныйпрактикум)

Лабораторная работа №1. Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer.

Microsoft *Baseline Security analyzer* - *программа*, позволяющая проверить уровень безопасности установленной конфигурации операционной системы (ОС) *Windows 2000*, XP, *Server* 2003, Vista *Server* 2008. Также проверяется и ряд других приложений разработки Microsoft. Данное средство можно отнести к разряду систем *анализа защищенности*. Оно распространяется бесплатно и доступно для скачивания с *web-сервера* Microsoft (*адрес* страницы данной утилиты на момент подготовки описания был:http://technet.microsoft.com/ru-ru/security/cc184924(en-us).aspx).

В процессе работы *BSA* проверяет наличие обновлений безопасности операционной системы, офисного пакета Microsoft Office(для версий XP и более поздних), серверных приложений, таких как MS *SQL Server*, MS *Exchange Server*, *Internet Information Server* и т.д. Кроме того, проверяется ряд настроек, касающихся безопасности, например, действующая политика паролей.

Перейдем к знакомству с программным продуктом. Надо отметить, что при подготовке описания данной лабораторной работы использовалась версия *BSA* 2.1. К сожалению, продукт не локализован, поэтому использовалась англоязычная версия.

При запуске открывается окно, позволяющее выбрать *объект* проверки - один *компьютер* (выбирается *по* имени или ip-адресу), несколько (задаваемых диапазоном ip-адресов или доменным именем) или просмотреть ранее

сделанные отчеты сканирования системы. При выборе сканирования отдельного компьютера *по* умолчанию подставляется имя локальной станции, но можно указать имя или *ip-адрес* другого компьютера.

Можно задать перечень проверяемых параметров. На рис. 3.2 представлен выбор вариантов проверки:

- проверка на наличие уязвимостей Windows, вызванных некорректным администрированием;
- проверка на "слабые" пароли (пустые пароли, отсутствие ограничений на срок действия паролей и т.д.);
- проверка на наличие уязвимостей web-сервера IIS, вызванных некорректным администрированием;

аналогичная проверка в отношении СУБД MS SQL Server;

проверка на наличие обновлений безопасности.

Перед началом работы *программа* обращается на *сервер* Microsoft для получения перечня обновлений для ОС и известных уязвимостей. Если на момент проведения проверки *компьютер* не подключен к *Интернет*, база уязвимостей не будет обновлена,*программа* об этом сообщит и дальнейшие проверки выполняться не будут. В подобных случаях нужно отключать проверку обновлении безопасности.

Для успешной проверки локальной системы необходимо, чтобы *программа* выполнялась от имени учетной записи с правами локального администратора. Иначе проверка не может быть проведена и о чем будет выдано сообщение: "You do *not* have sufficient *permissions* to *perform this command*. Make sure that you are *running as* the *local administrator* or have opened the *commandprompt* using the 'Run *as administrator*' *option*".

По результатам сканирования формируется отчет, в начале которого дается общая оценка уровня безопасности конфигурации проверяемого компьютера.

Далее приводится перечень обнаруженных уязвимостей, разбитый на группы: результаты проверки установки обновлений, результаты проверки *Windows* и т.д. Надо отметить, что выпускаемые Microsoft обновления бывают различных типов:

Security updates - собственно обновления безопасности, как правило, посвященные исправлению одной уязвимости программного продукта;

Update rollups - набор исправлений безопасности, который позволяет одновременно исправить несколько уязвимостей. Это упрощает обслуживание процесса обновления программного обеспечения (*ПО*);

Service packs - набор исправлений, как связанных, так и несвязанных с *безопасностью. Установка Service* pack, как правило, исправляет все уязвимости, обнаруженные с момента выхода предыдущего *Service* pack, таким образом устанавливать промежуточные обновления уже не надо.

В описании рассматриваемого результата проверки (рис.3.4) можно выбрать ссылку **Result details** и получить более подробное описание найденных проблем данной группы. При наличии подключения к *Интернет*, перейдя *по* приводимой в

отчете ссылке, можно получить информацию об отсутствующем обновлении безопасности и скачать его из сети.

Нужно отметить, что установка обновлений для систем с высокими требованиями в области непрерывности работы, требует предварительной тщательной проверки совместимости обновлений с использующимися приложениями. Подобная проверка обычно производится на тестовых системах с близкой конфигурацией *ПО*. В то же время, для небольших организаций и пользователей домашних компьютеров такая проверка зачастую неосуществима. Поэтому надо быть готовым к тому, чтобы восстановить систему после неудачного обновления. Для современных ОС семейства *Windows* это можно сделать, например, используя специальные режимы загрузки ОС - безопасный режим или режим загрузки последней удачной конфигурации.

Также надо отметить еще одну особенность. На данный момент **baseline security analyzer** не существует в локализованной русскоязычной версии. И содержащиеся там ссылки на пакеты обновлений могут указывать на иные языковые версии, что может создать проблемы при обновлении локализованных продуктов.

Аналогичным образом проводится работа *по* анализу других групп уязвимостей.
Описывается *уязвимость*, указывается ее уровень критичности, даются рекомендации *по* исправлению.Указывается, неограниченные *по* сроку действия. что 3 учетные записи имеют пароли,
Кроме версии программы с графическим интерфейсом, существует также *утилита* с интерфейсом командной строки. Называется она mbsacli.exe и находится в том же каталоге, куда устанавливался *Baseline security analyzer*, например, **"C:\Program Files\Microsoft Baseline Security Analyzer 2"**. У утилиты есть достаточно много ключей, получить информацию о которых можно запустив ее с ключом **"/?"**.

Запуск без ключей приведет к сканированию локального компьютера с выводом результатов на *консоль*. Чтобы сохранить результаты сканирования, можно перенаправить *вывод* в какой-либо *файл*. Например: mbsacli > mylog.txt. Хотелось бы еще раз обратить внимание на то, что при настройках *по* умолчанию сначала *утилита* обращается на *сайт* Майкрософт за информацией об обновлениях. Если соединение с *Интернет* отсутствует, то утилиту надо запускать или с ключом /nd (указание "не надо скачивать файлы с сайта Майкрософт") или с ключом /n Updates (указание "не надо проводить проверку обновлений").

Запуск с ключом /xmlout приводит к запуску утилиты в режиме проверки обновлений (т.е. проверка на уязвимости, явившиеся результатом неудачного администрирования, проводиться не будет), при этом, отчет формируется в формате xml. Например:

mbsacli /xmlout > c:\myxmlog.xml

Задания

1. Выполните проверку Вашего компьютера с помощью

MicrosoftBaselinesecurityanalyzer.

В отчете о выполнении лабораторной укажите:

- как оценен уровень уязвимости Вашего компьютера;
- какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;
- опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.

Проведите анализ результатов - какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.

2. Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.
3. Теперь выполните проверку нескольких компьютеров с помощью утилиты mbsacli. Для этого, предварительно создайте текстовый файл с перечнем имен компьютеров или ip- адресов и запускайте mbsacli с ключом /listfile, после которого указывается имя файла с перечнем компьютеров. В результате Вы получите сообщение примерно следующего содержания:
4. Computer Name, IP Address, Assessment, Report Name 5. ----------

HOME\MYNBOOK, 127.0.0.1, Severe Risk, HOME - MYNBOOK (06.12.2008 13-51)

Для того, чтобы увидеть подробные результаты проверки, надо повторно запустить mbsacli с ключом /ld, после которого указывается имя отчета. *Вывод* можно перенаправить в *текстовый файл* для дальнейшей обработки. Например:

```
mbsacli /ld "HOME - MYNBOOK (06.12.2008 13-51)" > c:\test\report1.txt
```

После выполнения задания проанализируйте результаты, кратко опишите их в отчете по лабораторной работе.

Лабораторная работа №2. Реализация политики безопасности в защищенных версиях операционной системы Windows

Цель работы: освоения средств администратора и аудитора защищенных версий операционной системы Windows, предназначенных для

- определения параметров политики безопасности;
- определения параметров политики аудита;
- просмотра и очистки журнала аудита.

Подготовка к выполнению работы: по материалам лекций по дисциплине «Защита информационных процессов в компьютерных системах» и изученным ранее дисциплинам («Введение в специальность», «Теория информационной безопасности и методология защиты информации» и другим) вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

аудит;

событие безопасности;
журнал (*файл*) *аудита*;
политика аудита;
интерактивный вход;
сетевой доступ;
домен компьютерной сети;
цифровая подпись.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) какие события безопасности должны фиксироваться в журнале аудита?
2) какие параметры определяют политику аудита?
3) целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
4) целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
5) как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
6) нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

Порядок выполнения работы:

1. После собеседования с преподавателем и получения допуска к работе войти в систему под указанным именем (с правами администратора).
2. Освоить средства определения политики безопасности:

- открыть окно определения параметров политики безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности);
- установить заголовок «ПРЕДУПРЕЖДЕНИЕ» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»;
- установить текст «На этом компьютере могут работать только зарегистрированные пользователи!» в качестве значения параметра «Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»;
- установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»;
- установить значение «Включен» для параметра «Интерактивный вход в систему: не отображать последнего имени пользователя»;
- установить значение «7 дней» для параметра «Интерактивный вход в систему:

напоминать пользователям об истечении срока действия пароля заранее»;

- включить в отчет о лабораторной работе сведения о порядке назначения параметров политики безопасности, относящихся к интерактивному входу, и ответ на вопрос о
смысле этих параметров;
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к интерактивному входу;
- с помощью раздела Справки Windows «Параметры безопасности» включить в отчет о лабораторной работе пояснения отдельных параметров локальной политики безопасности компьютерной системы и их возможных значений (в соответствии с номером варианта и приложением 1). Обязательно ответить на вопрос, чем может угрожать неправильное определение данного параметра.

1. Освоить средства определение политики аудита:

- открыть окно определения параметров политики аудита (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Политика аудита);
- с помощью параметров политики аудита установить регистрацию в журнале аудита успешных и неудачных попыток
  - входа в систему, изменения
  - политики,
  - использования привилегий,
  - событий входа в систему,
  - управления учетными записями;
- открыть окно определения параметров безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности) и включить в отчет о лабораторной работе ответ на вопрос,
какие еще параметры политики аудита могут быть определены;
- открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность), выполнить команду «Свойства» контекстного меню (или команду Действие | Свойства) и включить в отчет о лабораторной работе ответы на вопросы
  - какие еще параметры политики аудита могут быть
  - изменены, где расположен журнал аудита событий
  - безопасности;
- включить в отчет о лабораторной работе сведения о порядке назначения параметров политики аудита и ответ на вопрос о смысле этих параметров;
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики аудита.

2. Освоить средства просмотра журнала аудита событий безопасности:

- открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность);
- включить в отчет о лабораторной работе копии экранных форм с краткой и полной информацией о просматриваемом событии безопасности;
- с помощью буфера обмена Windows и соответствующей кнопки в окне свойств события включить в отчет о лабораторной работе полную информацию о

нескольких событиях безопасности.

3. Освоить средства определения политики ограниченного использования программ:

- открыть окно определения уровней безопасности политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Уровни безопасности);
- включить в отчет о лабораторной работе пояснения к возможным уровням безопасности при запуске программ и копии соответствующих экранных форм;
- открыть окно определения дополнительных правил политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Дополнительные правила);
- включить в отчет о лабораторной работе ответы на вопросы, какие дополнительные правила для работы с программами могут быть определены (с помощью команд контекстного меню или меню «Действие») и в чем их смысл, а также копии соответствующих экранных форм.

4. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

- в чем уязвимость с точки зрения безопасности информации принимаемая по умолчанию реакция системы на превышение размера журнала аудита?
- какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?
- из каких этапов состоит построение политики безопасности для компьютерной системы? к чему может привести ошибочное определение политики безопасности (приведите примеры)?
- почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

7. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета (*Московский государственный социальный университет*), факультета (*информатики и информационных технологий*), кафедры (*информационной безопасности*), учебной дисциплины и лабораторной работы, номером варианта, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

Порядок защиты лабораторной работы:

1. К защите лабораторной работы допускаются студенты, выполнившие ее в компьютерном классе, предъявившие результаты своей работы преподавателю и подготовившие отчет о выполнении лабораторной работы, содержание которого соответствует п. 7 порядка выполнения работы;
2. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы

преподавателя.

3. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.
4. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в
другой день.

Приложение 1

Номер вариан	**Поясняемые параметры политики безопасности**
1	Учетные записи: состояние учетной записи «Администратор» Устройства: разрешено форматировать и извлекать съемные носители Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию Клиент сети Microsoft: использовать цифровую подпись (всегда) Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля
2	Учетные записи: состояние учетной записи «Гость» Устройства: разрешать отстыковку без входа в систему Контроллер домена: запретить изменение пароля учетных записей компьютера Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера) Сетевая безопасность: принудительный вывод из сеанса по истечении
3	Учетные записи: ограничить использование пустых паролей только для консольного входа Устройства: запретить пользователям установку драйверов принтера Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB- серверам Сетевая безопасность: уровень проверки подлинности LAN Manager
4	Учетные записи: переименование учетной записи администратора Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям Член домена: шифрование данных безопасного канала, когда это возможно Сервер сети Microsoft: длительность простоя перед отключением сеанса Сетевая безопасность: минимальная сеансовая безопасность для
5	Учетные записи: переименование учетной записи гостя Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям Член домена: цифровая подпись данных безопасного канала, когда это возможно Сервер сети Microsoft: использовать цифровую подпись (всегда)

6	Завершение работы: разрешить завершение работы системы без выполнения входа в систему Устройства: поведение при установке неподписанного драйвера Член домена: максимальный срок действия пароля учетных записей компьютера Сервер сети Microsoft: использовать цифровую подпись (с согласия

Номер варианта	Поясняемые параметры политики безопасности
7	Завершение работы: очистка страничного файла виртуальной памяти Член домена: требует стойкого ключа сеанса (Windows 2000 или выше) Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования
8	Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов Член домена: отключить изменение пароля учетных записей компьютера Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями
9	Системные объекты: учитывать регистр для подсистем, отличных от Windows Сетевой доступ: не разрешать средству сохранения имен пользователей и
	Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам Сервер сети Microsoft: отключать клиентов по истечении
10	Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок) Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям Сетевой доступ: разрешать анонимный доступ к именованным каналам Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)

Лабораторная работа №3. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP Цель работы: освоение системных программ Windows XP, программ из комплекта

WindowsNT Resource Kit и других программных средств, предназначенных для

- просмотра и управления разрешениями на доступ к конфиденциальным объектам компьютерной системы;

просмотра и анализа записей аудита;
анализа соответствия реализуемой в компьютерной системе политики безопасности требованиям стандартов безопасности;

- дополнительной защиты базы учетных записей пользователей компьютерной системы и используемых ими рабочих станций.

Подготовка к выполнению работы: по материалам лекций по дисциплине «Защита информационных процессов в компьютерных системах» и изученным ранее дисциплинам («Введение в специальность», «Теория информационной безопасности и методология защиты информации» и другим) вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

- *матрица доступа*;
- *дискреционный список контроля доступа*;
- *домен безопасности*;
- *журнал (файл) аудита*;
- *запись журнала аудита*;
- *стандарт безопасности*.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

7) что такое Trusted Computer System Evaluation Criteria (TCSEC)?
8) какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?
9) какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?
10) кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?
11) как должны использоваться записи журнала аудита событий безопасности?
12) какие права доступа к файлу аудита имеет по умолчанию администратор системы?
13) что такое консольное приложение Windows? Порядоквыполненияработы:

5. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами администратора).
6. Освоить использование системной программы по управлению списками контроля доступа (CACLS):

- начать сеанс работы в режиме командной строки Windows XP (Пуск | Программы | Стандартные | Командная строка);
- в строке приглашения ввести название программы, ознакомиться с ее назначением и параметрами и сохранить данную информацию в отчете о лабораторной работе (через буфер обмена с помощью команд подменю «Изменить» системного меню окна командной строки);
- перейти (с помощью команды cd \Учебные материалы) в папку «Учебные материалы» и с помощью программы cacls получить и сохранить в файле в своей индивидуальной папке разрешения на доступ к папке «КЗИ2000», введя следующую команду

cacls КЗИ2000 >*имя файла*

(для переключения раскладок клавиатуры в режиме командной строки использовать комбинации клавиш Alt+правый Shift и Alt+левый Shift);

- просмотреть созданный файл с помощью Internet Explorer и включить его содержимое в отчет о лабораторной работе, снабдив необходимыми комментариями (с учетом сведений, приведенных в приложении);
- повторить два предыдущих пункта для своей индивидуальной папки;
- перейти в свою индивидуальную папку (с помощью команды командной строки cd) и с помощью одного вызова программы cacls запретить доступ группе «Пользователи» ко всем файлам и вложенным папкам своей индивидуальной папки;
- проверить результаты выполнения предыдущего пункта с помощью команды «Свойства» контекстного меню своей индивидуальной папки и включить в отчет о лабораторной работе текст вызова программы cacls и ответ на вопрос, почему доступ Вам к файлам своей папки теперь недоступен;
- разрешить доступ по чтению группе «Пользователи» к файлам и вложенным папкам своей индивидуальной папки с помощью одного вызова программы cacls, проверить результаты и включить в отчет о лабораторной работе текст вызова программы cacls;
- завершить (с помощью команды exit) сеанс работы в режиме командной строки и включить в отчет о лабораторной работе ответ на вопрос, в чем преимущество использования программы cacls перед назначением разрешений на доступ к объектам при помощи Проводника Windows.

7. Ознакомиться с возможностями программ управления и анализа разрешений на доступ к объектам компьютерных систем на основе WindowsXP:

- начать работу с программой просмотра разрешений на доступ к объектам и параметров политики безопасности DumpACL, размещенной в папке TEMP \ DumpACL на диске с;
- ознакомиться с порядком настройки параметров отчета о результатах анализа разрешений (команда меню Report | PermissionsReportOptions) и включить эти сведения в отчет о лабораторной работе;
- с помощью команды меню Report | DumpPermissionsforFileSystem получить и включить в отчет сведения о результатах анализа разрешений на доступ к папке «КЗИ2000» и своей индивидуальной папке, а также ответ на вопрос, в чем разница между данными результатами и сведениями, полученными при помощи команды cacls;
- с помощью других команд меню Report получить и включить в отчет результаты анализа разрешений на доступ к реестру Windows (только раздел HKEY_CURRENT_USER) и принтеру;
- ознакомиться и включить в отчет о лабораторной работе сведения о порядке получения и содержании информации о зарегистрированных пользователях и

группах (команды Dump… меню Report);

- включить в отчет о лабораторной работе сведения о назначении и результатах применения команд DumpPolicies и DumpRights меню Report;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой DumpACL, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к объектам FileAdmin из группы AdministratorAssistant меню Пуск | Программы;
- получить с помощью данной программы разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке и включить их в отчет;
- с помощью программы FileAdmin оставить полный доступ к своей индивидуальной папке, вложенным в нее папкам и файлам только самому себе (своей индивидуальной учетной записи) и пользователю User (учесть при этом действие переключателей “PropagateThroughEntireTree?”), а всем остальным пользователям и группам – доступ только для чтения;
- с помощью программы FileAdmin (кнопка Clone) распространить виды доступа к своей индивидуальной папке, установленные для группы «Пользователи», на группу «Опытные пользователи»;
- изучить назначение кнопки Options программы FileAdmin (определение настроек и просмотр журнала изменений прав доступа к объектам);
- включить в отчет о лабораторной работе копии экранных форм, используемых программой FileAdmin, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к реестру WindowsRegAdmin из группы AdministratorAssistant меню Пуск | Программы;
- с помощью программы RegAdmin получить и включить в отчет о лабораторной работе сведения о разрешениях на доступ к разделам реестра HKEY_LOCAL_MACHINE и HKEY_CURRENT_USER, а также ответ на вопрос, как изменить права доступа к разделам реестра Windows с помощью программы RegAdmin;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой RegAdmin, и завершить работу с этой программой;
- начать работу с программой управления и анализа разрешений на доступ к объектам SecurityExplorer из группы AdministrativeTools (Common) меню Пуск | Программы;
- с помощью программы SecurityExplorer (команда меню Tools | Showpermissions) просмотреть и включить в отчет о лабораторной работе разрешения на доступ к папке «КЗИ2000» и к своей индивидуальной папке, а также ответ на вопрос, какая дополнительная информация о дискреционных списках контроля доступа выводится программой SecurityExplorer;
- изучить и включить в отчет сведения о назначении кнопок диалогового окна DirectoryPermissions программы SecurityExplorer (Modify, GrantPermissions и т.д.), а также ответ на вопрос, возможно ли «клонирование» прав доступа к объекту в программе SecurityExplorer;
- с помощью команды меню Tools | SearchforPermissions программы SecurityExplorer получить, сохранить в файле в своей индивидуальной папке и

включить в отчет о лабораторной работе сведения о папках диска с, к которым имеет доступ (в том числе полный) группы «Пользователи» и «Все»;

- изучить и отразить в отчете о лабораторной работе средства вызова функций программы SecurityExplorer с помощью контекстного меню Проводника Windows;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой SecurityExplorer, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к объектам SecurityManager из группы AdminTools меню Пуск | Программы;
- получить с помощью программы SecurityManager и включить в отчет о лабораторной работе разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке (для
сохранения отчета программы можно воспользоваться командой ее меню File | Save Report);
- выделить в левой части окна программы SecurityManager имя своей индивидуальной папки и на ее примере изучить и включить в отчет о лабораторной работе команды контекстного меню и связанные с ними функции этой программы по управлению разрешениями на доступ к объектам (особо обратить внимание на команду ReplaceOwner и включить в отчет о лабораторной работе ответ на вопрос, в чем потенциальная опасность применения этой возможности);
- включить в отчет о лабораторной работе копии экранных форм, используемых программой SecurityManager, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к объектам компьютерной системы предприятия Virtuosity (с помощью меню Пуск | Программы);
- с помощью программы Virtuosity получить и отразить в отчете разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке;
- с помощью Справки программы Virtuosity изучить и включить в отчет о лабораторной работе сведения о назначении команд меню Actions | Save into Database и Actions | Apply
from Database;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой Virtuosity, и завершить работу с этой программой.

8. Ознакомиться с возможностями программ анализа выбранной для компьютерной системы политики безопасности и ее соответствия требованиям стандартов в области
информационной безопасности:

- начать работу с программой проверки соответствия настроек WindowsXP требованиям класса C2 TCSEC (программа c2config из комплекта WindowsNTResourceKit) с помощью команды «Выполнить» меню «Пуск»;
- ознакомиться с результатами анализа политики безопасности, полученными с помощью программы c2config, сохранить их в отчете о лабораторной работе и снабдить необходимыми комментариями, раскрывающими сущность того или иного анализируемого параметра (наиболее подробно для тех параметров, значения которых не соответствуют требованиям класса безопасности C2);
- включить в отчет сведения о смысле изображений рядом с анализируемым

параметром политики безопасности в окне программы c2config (при необходимости можно воспользоваться разделом ListBoxDisplay Справки данной программы;

- включить в отчет о лабораторной работе копии экранных форм, используемых программой c2config, и завершить работу с этой программой;
- начать работу с демонстрационной версией программы анализа безопасности компьютерных систем и сетей KaneSecurityAnalyst из группы KaneSecurityAnalystforNT меню Пуск | Программы;
- с помощью кнопок главного окна программы KaneSecurityAnalyst изучить и включить в отчет ее основные функции (анализ политики учетных записей, выбираемых пользователями паролей, политики аудита, прав доступа к файлам и папкам, прав доступа к реестру, соответствия требованиям класса С2, рисков при использовании данной политики безопасности и др.);
- включить в отчет о лабораторной работе копии экранных форм, используемых программой KaneSecurityAnalyst, и завершить работу с этой программой.

9. Изучить средства эффективного анализа журнала аудита событий безопасности:

- начать работу с системной программой Просмотр событий (Панель управления | Администрирование) и открыть журнал аудита событий безопасности;
- с помощью команды «Фильтр» меню «Вид» изучить и отразить в отчете о лабораторной работе средства отбора необходимых для анализа записей (критерии отбора, переход от
просмотра отобранных записей к просмотру всего журнала и наоборот, изменение порядка сортировки записей, поиск нужных записей, изменение вида отображения
записей);
- с помощью команд меню «Действие» изучить и отразить в отчете средства сохранения и восстановления журнала аудита (сохранить журнал аудита событий безопасности в виде текстового файла в своей индивидуальной папке);
- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и завершить работу с системной программой Просмотр событий;
- запустить в режиме командной строки программу dumpel из комплекта WindowsNTResourceKit с параметром -?, включить в отчет сведения о параметрах этой программы работы с журналами аудита;
- с помощью программы dumpel сохранить в текстовом файле в своей индивидуальной папке выбранные записи системного журнала аудита, введя следующую строку

dumpel –l system –f *имя файла* –e 6005 –e 6006 –e 6009 –m EventLog

Включить в отчет фрагмент созданного таким образом файла и ответ на вопрос, какая дополнительная по сравнению с системной программой Просмотр событий возможность существует у программы dumpel;

- завершить работу в режиме командной строки.

6. Ознакомиться с возможностями системной программы дополнительной защиты

базы
учетных записей с помощью ее шифрования:

- начать работу с программой syskey с помощью команды «Выполнить» меню «Пуск»; нажать кнопку «Обновить», ознакомиться и отразить в отчете варианты генерации системного ключа шифрования базы учетных записей, нажать кнопку «Отмена» (дважды);
- включить в отчет о лабораторной работе ответ на вопрос, какие достоинства и недостатки есть у каждого из предлагаемых программой syskey вариантов генерации
криптографического ключа.

7. Ознакомиться с возможностями дополнительного хранителя экрана из комплекта
WindowsNTResourceKit, осуществляющего принудительный выход из системы по истечении заданного периода времени:
- скопировать файл winexit.scr из папки C:\Disrtrib\ResourceKit 2\COMMON\COMMON в папку C:\WINDOWS\system32 (если это еще не сделано);
- с помощью команды «Свойства» контекстного меню Рабочего стола (закладка «Заставка») установить и настроить (кнопка «Параметры») хранитель экрана LogoffScreenSaver;
- закрыть окно свойств экрана и проверить работу установленного хранителя экрана; включить в отчет о лабораторной работе сведения о параметрах и порядке использования дополнительного хранителя экрана, а также копии экранных форм, использованных при выполнении данного пункта.

8. Включить в отчет о лабораторной работе ответы на контрольные вопросы:
- почему компьютерные системы на основе WindowsXP не могут быть сертифицированы по классу безопасности TCSEC выше, чем C2?
- какой класс защищенности автоматизированных систем в соответствии с требованиями руководящих документов Гостехкомиссии РФ соответствует, на Ваш взгляд, классу C2 TCSEC?
- почему многие из рассмотренных в настоящей лабораторной работе программ работают в режиме командной строки?
- какая из рассмотренных в данной лабораторной работе программ управления разрешениями на доступ к объектам кажется Вам наиболее удобной и почему?
- составьте строку вызова системной программы cacls для того, чтобы обеспечить доступ по чтению ко всем файлам и папкам папки c:\students для всех членов группы
«Преподаватели»;
- в чем преимущества, на Ваш взгляд, дополнительного хранителя экрана winexit.scr перед стандартными хранителями экрана?
- какие угрозы безопасности и каналы утечки конфиденциальной информации может устранить программа syskey?
- какая из рассмотренных в данной лабораторной работе программ управления разрешениями на доступ к объектам имеет небезопасную функцию и как могут быть
нейтрализованы последствия ее несанкционированного применения?

9. Подготовить отчет о выполнение лабораторной работы, который должен включать в

себя:

- титульный лист с названиями университета (*Московский государственный социальный университет*), факультета (*информатики и информационных технологий*), кафедры (*информационной безопасности*), учебной дисциплины и лабораторной работы, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

Порядокзащитылабораторнойработы:

5. К защите лабораторной работы допускаются студенты, выполнившие ее в компьютерном классе, предъявившие результаты своей работы преподавателю и подготовившие отчет о выполнении лабораторной работы, содержание которого соответствует п. 9 порядка выполнения работы;
6. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
7. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.
8. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.

Приложение

Стандартные типы доступа к объектам в операционной системе WindowsXP

- SINCHRONIZE – использовать объект для синхронизации;
- WRITE_OWNER – изменить владельца объекта;
- WRITE_DAC – изменить дискреционный список контроля доступа к объекту;
- READ_CONTROL – прочитать данные из дискреционного списка контроля доступа; DELETE – удалить объект.

Специальные права доступа к объектам

- READ_DATA – прочитать данные из объекта;
- WRITE_DATA – записать данные в объект;
- APPEND_DATA – добавить данные в объект;
- READ_ATTRIBUTES – прочитать атрибуты объекта;
- WRITE_ATTRIBUTES – записать атрибуты объекта;
- READ_EA – прочитать расширенные атрибуты объекта;
- WRITE_EA – записать расширенные атрибуты объекта;
- EXECUTE – выполнить программный файл.

Родовые права доступа к объектам

- GENERIC_READ - READ_CONTROL, READ_DATA, READ_ATTRIBUTES, READ_EA, SINCHRONIZE;
- GENERIC_WRITE - READ_CONTROL, WRITE_DATA, WRITE_ATTRIBUTES, WRITE_EA, APPEND_DATA, SINCHRONIZE;
- GENERIC_EXECUTE - READ_CONTROL, READ_ATTRIBUTES, EXECUTE, SINCHRONIZE.

Лабораторная работа №4.Разработка и программная реализация криптографических алгоритмов

Содержание задания

1. В программу, разработанную при выполнении лабораторной работы №1, добавить средства шифрования (расшифрования) или хеширования паролей, хранящихся в файле зарегистрированных пользователей. Способ шифрования (хеширования) задается преподавателем.
2. При использовании шифрования введенный пользователем пароль должен сравниваться с расшифрованным значением из файла.
3. При использовании хеширования хеш-значение введенного пользователем пароля
   должно сравниваться со значением из файла.

Способ шифрования (хеширования) пароля

1. Шифрование перестановкой (произвольный ключ определяет порядок следования символов пароля в шифре).
2. Хеширование (в файл записывается результат шифрования перестановкой строки
   «12345678», ключ шифрования – пароль пользователя).
3. Хеширование (аналогично варианту 2, но в файл записывается результат шифрования имени пользователя).
4. Шифрование заменой (использовать одноалфавитную подстановку по произвольному ключу).
5. Хеширование (шифрование по варианту 4 строки «12345678» с ключом, равным сумме по модулю 256 байтов пароля).
6. Хеширование (аналогично варианту 5, но шифруется имя пользователя).
7. Шифрование заменой (использовать многоалфавитную подстановку по произвольному
   ключу).
8. Шифрование гаммированием (длина блока – 1 байт, блоки гаммы формируются по
   правилу Gi+1=A*Gi+C {mod 256}, где A=5, C=3, G0 – любое).
9. Хеширование (в файл записывается результат шифрования гаммированием строки
   «12345678», блоки гаммы формируются аналогично варианту 8, но A – код 1-го символа пароля, C – код 2-го символа пароля, G0 – код 3-го символа пароля).
10. Хеширование (аналогично варианту 9, но шифруется имя пользователя).

11. Шифрование гаммированием (аналогично варианту 8, но блоки гаммы получаются при помощи стандартной функции random(256), прототип которой определен в файле stdlib.h).
12. Хеширование (в файл записывается результат шифрования аналогично варианту 11
строки «12345678», но начальное значение датчика псевдослучайных чисел выбирается равным сумме по модулю 256 байтов пароля и устанавливается с помощью функции srand(начальное значение), прототип которой определен в файле stdlib.h).
13. Хеширование (аналогично варианту 12, но шифруется имя пользователя).
14. Шифрование гаммированием (аналогично варианту 8, но A, C и G0 выбираются равными соответственно 1-му, 2-му и 3-му случайным числам, полученным с помощью функции random(256)).
15. Комбинированное шифрование (сначала по варианту 1, затем по варианту 8).
16. Комбинированное шифрование (сначала по варианту 4, затем по варианту 8).
17. Комбинированное шифрование (сначала по варианту 7, затем по варианту 8).
18. Комбинированное шифрование (сначала по варианту 1, затем по варианту 11).
19. Комбинированное шифрование (сначала по варианту 4, затем по варианту 11).
20. Комбинированное шифрование (сначала по варианту 7, затем по варианту 11).
21. Комбинированное шифрование (сначала по варианту 1, затем по варианту 14).
22. Комбинированное шифрование (сначала по варианту 4, затем по варианту 14).
23. Комбинированное шифрование (сначала по варианту 7, затем по варианту 14).
24. Комбинированное шифрование (сначала по варианту 1, затем по варианту 4).
25. Комбинированное шифрование (сначала по варианту 1, затем по варианту 7).
26. Комбинированное шифрование (сначала по варианту 8, затем по варианту 11).
27. Хеширование (в файл записывается сумма по модулю 256 произведений вида pi*i, где pi
– код i-го символа пароля).
28. Хеширование (в файл записывается результат шифрования строки «12345678» сначала
по варианту 2, затем по варианту 9).
29. Хеширование (в файл записывается результат шифрования имени пользователя сначала
по варианту 3, затем по варианту 10).
30. Хеширование (в файл записывается результат шифрования строки «12345678» сначала
по варианту 5, затем по варианту 9).

Рекомендуемые для разработки программы средства языка Си++

1. (char) – операция приведения произвольного целого числа к типу char (получение символа по его коду)
2. ^ – операция поразрядного сложения по модулю 2 (используется при шифровании гаммированием)
3. % – операция вычисления остатка от целочисленного деления (используется для приведения целого числа по модулю)

Лабораторная работа №5. Использование функций криптографического интерфейса Windows для защиты информации

Содержание задания

1. В программу, разработанную при выполнении лабораторных работ №1 и №2, добавить средства защиты от несанкционированного доступа к файлу с учетными данными зарегистрированных пользователей:
   - файл с учетными записями должен быть зашифрован при помощи функций CryptoAPI с использованием сеансового ключа, генерируемого на основе вводимой администратором парольной фразы;
   - при запуске программы файл с учетными записями должен расшифровываться во временный файл, который после завершения работы программы должен быть

     снова зашифрован для отражения возможных изменений в учетных записях пользователей («старое» содержимое файла учетных записей при этом стирается).
2. Варианты использования алгоритмов шифрования и хеширования при вызове функций CryptoAPI выбираются в соответствии с выданным преподавателем
   заданием.

Используемые алгоритмы шифрования и хеширования

№	Тип симметричного	Используемый режим шифрования	Добавление к ключу случайно	Используемый алгоритм хеширования
1	Блочный	Электронная кодовая книга	Д	MD
2	Потоковый	-	Д	MD
3	Блочный	Сцепление блоков шифра	Д	MD
4	Потоковый	-	Д	MD
5	Блочный	Обратная связь по	Д	MD
6	Потоковый	-	Д	SH
7	Блочный	Электронная кодовая книга	Д	MD
8	Потоковый	-	Не	MD
9	Блочный	Сцепление блоков шифра	Д	MD
10	Потоковый	-	Не	MD
11	Блочный	Обратная связь по	Д	MD
12	Потоковый	-	Не	SH
13	Блочный	Электронная кодовая книга	Д	MD
14	Блочный	Сцепление блоков шифра	Д	MD
15	Блочный	Обратная связь по	Д	MD
16	Блочный	Электронная кодовая книга	Д	SH
17	Блочный	Сцепление блоков шифра	Д	SH
18	Блочный	Обратная связь по	Д	SH
19	Блочный	Электронная кодовая книга	Не	MD
20	Блочный	Сцепление блоков шифра	Не	MD

№	Тип симметричного	Используемый режим шифрования	Добавление к ключу случайно	Используемый алгоритм хеширован
21	Блочный	Обратная связь по	Не	MD
22	Блочный	Электронная кодовая книга	Не	MD
23	Блочный	Сцепление блоков шифра	Не	MD
24	Блочный	Обратная связь по	Не	MD
25	Блочный	Электронная кодовая книга	Не	MD
26	Блочный	Сцепление блоков шифра	Не	MD
27	Блочный	Обратная связь по	Не	MD
28	Блочный	Электронная кодовая книга	Не	SH
29	Блочный	Сцепление блоков шифра	Не	SH
30	Блочный	Обратная связь по	Не	SH

Рекомендуемые для разработки программы средства языка Си++

1. ***Файл учетных записей зарегистрированных пользователей для операций шифрования (расшифрования).***

Объект класса fstream, открытый в двоичном режиме (определен в файле fstream.h).

2. Работа с файлом учетных записей (методы класса fstream):

/* открытие существующего файла под именем FileName для чтения в двоичном режиме */

void open(const char *FileName, ios::in|ios::binary);

// создание нового файла с именем FileName

void open(const char *FileName, ios::out|ios::binary);

// чтение данных из файла в буфер buf длины n, кратной длине блока шифра

istream& read(char *buf, int n);

/* получение количества байт, фактически прочитанных во время последней операции чтения из файла */

intgcount();

// запись в файл данных из буфера buf длины n, кратной длине блока шифра

ostream& write(const char *buf, int n);

// закрытие файла voidclose();

// проверка достижения конца файла

booleof();

// удаление файла с именем filename

int remove(const char *filename);

3. Шифрование (расшифрование) файла учетных записей (константы, типы данных и прототипы функций определены в заголовочном файле wincrypt.h):

HCRYPTPROV, HCRYPTKEY, HCRYPTHASH – типы данных для дескрипторов криптопровайдера (CSP), криптографического ключа, хеш-объекта

ALG_ID – тип данных для кодов криптографических алгоритмов

/* инициализация криптопровайдера:

в *phProv записывается его

дескриптор, pszContainer=NULL,

pszProvider=NULL,

dwProvType=PROV_RSA_FULL,
dwFlags=0 или (если при первом запуске программы CryptAcquireContext возвращает FALSE) регистрация нового пользователя в криптопровайдере dwFlags= CRYPT_NEW_KEYSET */

BOOL CryptAcquireContext(HCRYPTPROV *phProv, LPCSTR
pszContainer, LPCSTR pszProvider, DWORD dwProvType,
DWORD dwFlags);
/* создание пустого хеш-объекта (hProv – дескриптор инициализированного криптопровайдера, Algid – код алгоритма хеширования, hKey=0, dwFlags=0, в *phHash записывается дескриптор хеш-объекта) */

BOOL CryptCreateHash(HCRYPTPROV hProv, ALG_ID Algid, HCRYPTKEY hKey,
DWORD dwFlags, HCRYPTHASH *phHash);
/* хешированиепарольнойфразы pbData длины dwDataLen (hHash – дескрипторхеш-объекта, dwFlags=0) */
BOOL CryptHashData(HCRYPTHASH hHash, CONST BYTE *pbData,
DWORD dwDataLen, DWORD dwFlags);
// разрушениехеш-объектасдескрипторомhHash
BOOL CryptDestroyHash(HCRYPTHASH hHash);
/* создание ключа шифрования из хеш-объекта с парольной фразой hBaseData (hProv – дескриптор криптопровайдера, Algid – код алгоритма шифрования, dwFlags=CRYPT_EXPORTABLE с возможным объединением через | с признаком добавления к ключу случайного значения CRYPT_CREATE_SALT, в *phKey записывается дескриптор ключа)

```
BOOL CryptDeriveKey(HCRYPTPROV hProv, ALG_ID Algid,
        HCRYPTHASH hBaseData, DWORD dwFlags, HCRYPTKEY
        *phKey);
// разрушение ключа шифрования с дескриптором hKey
BOOL CryptDestroyKey(HCRYPTKEY hKey);
// освобождение криптопровайдера с дескриптором hProv (dwFlags=0)
BOOL CryptReleaseContext(HCRYPTPROV hProv, DWORD dwFlags);
/* шифрование на ключе с дескриптором hKey порции данных из буфера pbData
длины
```

dwBufLen (dwDataLen – длина порции данных, после выполнения функции в эту переменную записывается фактическая длина зашифрованных данных; hHash=0, dwFlags=0, Final – признак последней порции данных) */

```
BOOL CryptEncrypt(HCRYPTKEY hKey, HCRYPTHASH hHash, BOOL
        Final, DWORD dwFlags, BYTE *pbData, DWORD *pdwDataLen,
        DWORDdwBufLen);
```

/* расшифрование на ключе с дескриптором hKey порции данных из буфера pbData (dwDataLen – длина порции данных, после выполнения функции в эту переменную записывается фактическая длина расшифрованных данных; hHash=0, dwFlags=0, Final – признак последней порции данных) */

```
BOOL CryptDecrypt(HCRYPTKEY hKey, HCRYPTHASH hHash, BOOL Final,
        DWORD dwFlags, BYTE *pbData, DWORD *pdwDataLen);
/* установка режима шифрования для ключа hKey (dwParam= KP_MODE, pbData
указывает
```

на переменную типа unsignedlong, в которой записан код устанавливаемого режима, dwFlags=0) */

```
BOOL CryptSetKeyParam(HCRYPTKEY hKey, DWORD dwParam, BYTE *pbData,
        DWORDdwFlags);
```

Лабораторная работа №6. Защита программного обеспечения от несанкционированного использования и копирования

Содержание задания

1. Для программы, разработанной при выполнении лабораторных работ №1, №2 и №3, написать программу-инсталлятор, которая
   - запрашивает у пользователя папку для установки защищаемой программы, записывает туда файл с исполнимым кодом программы,
   - собирает информацию о компьютере, на котором устанавливается программа, хеширует эту информацию,
   - подписывает ее личным ключом пользователя программы и записывает подпись в реестр Windows в раздел HKEY_CURRENT_USER \ Software \ *Фамилия_студента* как значение параметра Signature.
2. В саму защищаемую программу включить фрагмент, в котором
   - собирается информация о компьютере, на котором запускается программа, вычисляется хеш-значение этой информации,

считывается подпись из указанного выше раздела реестра, которая проверяется с помощью открытого ключа пользователя.

3. При неудачной проверке работа защищаемой программы должна завершаться с выдачей соответствующего сообщения.
4. Собираемая о компьютере информация включает в себя:
   - имя пользователя, имя компьютера,
   - путь к папке с ОС Windows,
   - путь к папке с системными файлами ОС Windows,

   а также данные, выбираемые в соответствии с выданным заданием.

Собираемая информация о компьютере

№	Тип и под-тип кла- виатуры	Количе-ство кно- пок мыши	Ши-рина экрана	Высота экрана	Набор диско- вых уст-ройст	Объем памяти	Данные о диске, на котором установлена
1	Не	Д	Нет	Д	Нет	Д	Объем
2	Не	Д	Д	Нет	Нет	Д	Объем
3	Д	Не	Нет	Д	Нет	Д	Объем
4	Д	Не	Д	Нет	Нет	Д	Объем
5	Не	Д	Нет	Д	Д	Нет	Объем
6	Не	Д	Д	Нет	Д	Нет	Объем
7	Д	Не	Нет	Д	Д	Нет	Объем
8	Д	Не	Д	Нет	Д	Нет	Объем
9	Не	Д	Нет	Д	Нет	Д	Метка тома
№	Тип и под-тип кла- виатуры	Количе-ство кно- пок мыши	Ши-рина экрана	Высота экрана	Набор диско- вых уст-ройст	Объем памяти	Данные о диске, на котором установлена
10	Не	Д	Д	Нет	Нет	Д	Метка тома
11	Д	Не	Нет	Д	Нет	Д	Метка тома
12	Д	Не	Д	Нет	Нет	Д	Метка тома
13	Не	Д	Нет	Д	Д	Нет	Метка тома
14	Не	Д	Д	Нет	Д	Нет	Метка тома
15	Д	Не	Нет	Д	Д	Нет	Метка тома
16	Д	Не	Д	Нет	Д	Нет	Метка тома
17	Не	Д	Нет	Д	Нет	Д	Серийный №
18	Не	Д	Д	Нет	Нет	Д	Серийный №
19	Д	Не	Нет	Д	Нет	Д	Серийный №
20	Д	Не	Д	Нет	Нет	Д	Серийный №
21	Не	Д	Нет	Д	Д	Нет	Серийный №
22	Не	Д	Д	Нет	Д	Нет	Серийный №
23	Д	Не	Нет	Д	Д	Нет	Серийный №

24	Д	Не	Д	Нет	Д	Нет	Серийный №
25	Не т	Д а	Нет	Д а	Нет	Д а	Файловая система
26	Не т	Д а	Д а	Нет	Нет	Д а	Файловая система
27	Д а	Не т	Нет	Д а	Нет	Д а	Файловая система
28	Д а	Не т	Д а	Нет	Нет	Д а	Файловая система
29	Не т	Д а	Нет	Д а	Д а	Нет	Файловая система
30	Не т	Д а	Д а	Нет	Д а	Нет	Файловая система

Рекомендуемые для разработки программы средства языка Си++ и системы C++ Builder

1. Сбор информации о компьютере:

// получение в буфере lpBuffer длины nSize имени пользователя текущего сеанса

BOOL GetUserName(LPTSTR lpBuffer, LPDWORD nSize);

/* получение имени компьютера в буфере lpBuffer длины nSize>= MAX_COMPUTERNAME_LENGTH+1 */

BOOL GetComputerName(LPTSTR lpBuffer, LPDWORD nSize);

/* получение в буфере lpBuffer длины uSize>= MAX_PATH пути к каталогу с ОС

Windows */ UINT GetWindowsDirectory(LPTSTR lpBuffer,UINT uSize);

/* получение в буфере lpBuffer длины uSize>= MAX_PATH пути к системному каталогу Windows */

UINT GetSystemDirectory(LPTSTR lpBuffer, UINT uSize);

// получение типа (nTypeFlag=0) или подтипа (nTypeFlag=1) клавиатуры

intGetKeyboardType(intnTypeFlag);

/* получение количества кнопок мыши (nIndex=SM_CMOUSEBUTTONS), ширины (nIndex=SM_CXSCREEN) или высоты (nIndex=SM_CYSCREEN) экрана */

intGetSystemMetrics(intnIndex);

/* получение в буфере lpBuffer длины nBufferLength строки с корневыми каталогами всех дисков, разделенных 0-символами; результат – длина полученной строки без

заключительного 0-символа */

DWORD GetLogicalDriveStrings(DWORD nBufferLength, LPTSTR lpBuffer);

/* получение в буфере *lpBuffer структуры типа MEMORYSTATUS с характеристиками памяти компьютера (поле dwTotalPhys содержит целое число, равное общему объему физической памяти в байтах) */

VOIDGlobalMemoryStatus(LPMEMORYSTATUSlpBuffer);

/* получение информации об объеме текущего диска (lpRootPathName=NULL): количестве секторов в кластере (lpSectorsPerCluster), размере сектора (lpBytesPerSector), общем количестве кластеров (lpTotalNumberOfClusters), lpNumberOfFreeClusters=NULL */

BOOL GetDiskFreeSpace(LPCTSTR lpRootPathName,

LPDWORD lpSectorsPerCluster, LPDWORD lpBytesPerSector,

LPDWORD lpNumberOfFreeClusters,

LPDWORD lpTotalNumberOfClusters);

/* получение информации о текущем диске (lpRootPathName=NULL): метке тома (в буфере lpVolumeNameBuffer длины nVolumeNameSize), серийном номере (в переменной *lpVolumeSerialNumber), файловой системе (в буфере lpFileSystemNameBuffer длины nFileSystemNameSize), lpMaximumComponentLength=NULL, lpFileSystemFlags=NULL */

BOOL GetVolumeInformation(LPCTSTR lpRootPathName,

LPTSTR lpVolumeNameBuffer, DWORD nVolumeNameSize,

LPDWORD lpVolumeSerialNumber,

LPDWORD lpMaximumComponentLength, LPDWORD lpFileSystemFlags,

LPTSTR lpFileSystemNameBuffer, DWORD nFileSystemNameSize);

2. **Получение и проверка электронной цифровой подписи (ЭЦП) (константы, типы данных и прототипы функций пределены в файле wincrypt.h):**

HCRYPTPROV, HCRYPTKEY, HCRYPTHASH – типы данных для дескрипторов

криптопровайдера (CSP), криптографического ключа, хеш-объекта ALG_ID – тип данных для кодов криптографических алгоритмов

/* инициализация криптопровайдера:

в *phProv записывается его

дескриптор, pszContainer=NULL,

pszProvider=NULL,

dwProvType=PROV_RSA_FULL,

dwFlags=0 или (если при первом запуске программы CryptAcquireContext возвращает FALSE) регистрация нового пользователя в криптопровайдере dwFlags= CRYPT_NEW_KEYSET */

```
BOOL CryptAcquireContext(HCRYPTPROV *phProv, LPCSTR pszContainer,
    LPCSTR pszProvider, DWORD dwProvType, DWORD dwFlags);
```

/* создание в криптопровайдере с дескриптором hProv пары ключей ЭЦП (Algid=AT_SIGNATURE, dwFlags=0) и запись дескриптора открытого ключа в

*phKey */

```
BOOL CryptGenKey(HCRYPTPROV hProv, ALG_ID Algid,
    DWORD dwFlags, HCRYPTKEY *phKey);
```

/* получение у криптопровайдера с дескриптором hProv дескриптора открытого ключа ЭЦП (dwKeySpec=AT_SIGNATURE) в переменной *phUserKey (если функция возвращает FALSE, то пару ключей ЭЦП нужно создать с помощью функции CryptGenKey) */

```
BOOL CryptGetUserKey(HCRYPTPROV hProv, DWORD dwKeySpec,
    HCRYPTKEY *phUserKey);
```

/* созданиепустогохеш-объекта (hProv – дескрипториницализированногокриптопровайдера, Algid – кодалгоритмахеширования, hKey=0, dwFlags=0, в *phHashзаписываетсядескрипторхеш-объекта) */

```
BOOL CryptCreateHash(HCRYPTPROV hProv, ALG_ID Algid,
    HCRYPTKEY hKey, DWORD dwFlags, HCRYPTHASH
    *phHash);
```

/* добавление в хеш-объект данных из буфера *pbData длины dwDataLen (hHash – дескриптор хеш-объекта, dwFlags=0) */

```
BOOL CryptHashData(HCRYPTHASH hHash, CONST BYTE *pbData,
```

DWORD dwDataLen, DWORD dwFlags);

/* получениедляхеш-объектасдескриптромhHashЭЦПвбуферерbSignatureдлины *pdwSigLen (послевыполнениявфункциивэтупеременнуюзаписываетсяфактическаядлинаЭЦП); dwKeySpec=AT_SIGNATURE, sDescription=NULL, dwFlags=0 */

BOOL CryptSignHash(HCRYPTHASH hHash, DWORD dwKeySpec,

LPCTSTR sDescription, DWORD dwFlags, BYTE *pbSignature,

DWORD *pdwSigLen);

/* проверка ЭЦП из буфера *pbSignature длины dwSigLen для хеш-объекта с дескриптором hHash с помощью открытого ключа hPubKey (sDescription=NULL, dwFlags=0) */

BOOL CryptVerifySignature(HCRYPTHASH hHash, BYTE

*pbSignature, DWORD dwSigLen, HCRYPTKEY hPubKey,

LPCTSTR sDescription, DWORDdwFlags);

// разрушение хеш-объекта с дескриптором hHash
BOOLCryptDestroyHash(HCRYPTHASHhHash);

// разрушение ключа шифрования с дескриптором hKey
BOOL CryptDestroyKey(HCRYPTKEY hKey);
// освобождение криптопровайдера с дескриптором hProv
(dwFlags=0) BOOL CryptReleaseContext(HCRYPTPROV hProv,
DWORD dwFlags);

3. Работа с реестром Windows:

Класс TRegistry (определен в файле vcl\registry.hpp):

- конструктор без параметров;
- свойства:

HKEYRootKey (корневой раздел реестра, по умолчанию HKEY_CURRENT_USER);

HKEYCurrentKey (текущий раздел реестра, только для чтения);

AnsiStringCurrentPath (путь к текущему разделу реестра, только для

чтения).

- методы:

```
/* открытие или (если CanCreate=true) при необходимости создание текущего
раздела реестра Key */

bool OpenKey(const AnsiString Key, bool CanCreate);

/* запись (перезапись) в текущий раздел реестра значения параметра Name из буфера Buffer длины BufSize */

void WriteBinaryData(const AnsiString Name, void *Buffer, int BufSize);

// запись и закрытие текущего раздела реестра

voidCloseKey();

// проверка существования в реестре раздела Key

bool KeyExists(const AnsiString Key);

/* чтение из текущего раздела реестра значения параметра Name в буфер Buffer длины BufSize */

int ReadBinaryData(const AnsiString Name, void *Buffer, int BufSize);
```

Лабораторная работа №7.Основы работы с персональным сетевым экраном фирмы «Инфотекс»

Содержание задания

Ознакомиться с инструкцией по установке программного средства ViPNet[Персональный сетевой экран], находящейся в файле *Быстрый старт.doc*. Выполнить установку демонстрационной версии программы, приняв все выбираемые по умолчанию параметры установки. Согласиться с предложением программы установки произвести перезагрузку операционной системы, предварительно запомнив пароль для входа в программу (находится в файле password.txt). В процессе перезагрузки системы

- ввести пароль для входа в персональный сетевой экран;
- согласиться с предложенным каталогом для сохранения ключевой информации пользователя программы;
- нажать кнопку «Принять» в окне приветствия (программа автоматически стартует, в правой части панели задач появляется значок  , для отображения главного окна программы следует выбрать команду «Восстановить» контекстного меню этого значка или команду Пуск | Программы | ViPNet | [Персональный сетевой экран] | ViPNet Персональный сетевой экран).

Изучить (с помощью раздела 6.3 руководства пользователя программы в файле Doc \ Personal_Firewall.doc или с помощью Справки программы) основные режимы функционирования программы (кнопка «Режимы» в левой части ее главного окна):

блокировка всего IP-трафика (абсолютная защита);

пропуск только разрешенного сетевыми фильтрами IP-трафика;

бумеранг (разрешение инициативных соединений):

i. жесткий (устанавливается по умолчанию);
ii. мягкий;

пропуск всего IP-трафика с ведением журнала;

полное отключение драйвера.

Изучить (с помощью раздела 6 руководства пользователя программы или с помощью ее Справки) функции блокировки (кнопка в строке состояния главного окна программы): компьютера и IP-трафика;

только компьютера; только IP-трафика.

Изучить (с помощью разделов 6.1 и 7.5.1 руководства пользователя или с помощью Справки программы) функции для работы с сетевыми фильтрами (кнопка «Сетевые фильтры» в левой части главного окна программы):

- регистрация IP-адреса (команда Правила доступа | Добавить IP-адрес контекстного меню объекта «Сетевые фильтры» в правой части главного окна программы):
  i. в окне «Правило доступа» (строка «Имя компьютера») ввести доменное (например, www.yandex.ru) или сетевое имя хоста (при наличии доступа к сети Интернет или локальной сети), либо localhost (при автономной работе);
  ii. ввести (в строке «Псевдоним») произвольное наименование для регистрируемого IP-адреса;
  iii. нажать кнопку «Добавить» (в списке «IP-адрес» должен появиться регистрируемый адрес);
  iv. включить режим «разрешения» или «блокировки» работы с регистрируемым IP-адресом (с помощью соответствующего переключателя);
  v. нажать кнопку «Принять»;
- создание добавленного фильтра для зарегистрированного IP-адреса или всех незарегистрированных IP-адресов (команда Правила доступа | Добавить фильтр протоколов контекстного меню соответствующего объекта в правой части главного окна):
  i. выбрать протокол (ICMP, TCP или UDP) в соответствующем списке окна «Фильтр протоколов»);
  ii. настроить параметры добавленного фильтра для протокола ICMP (направление, тип и код передаваемого сообщения);
  iii. настроить параметры добавленного фильтра для протокола TCP (какой из участвующих в соединении компьютеров является сервером, номера «своего» и «чужого» портов);
  iv. настроить параметры добавленного фильтра для протокола UDP (направление передаваемого сообщения, номера «своего» и

«чужого» портов);

v. после настройки параметров добавленного фильтра нажать кнопку «Принять»;

- изучить (с помощью раздела 7.4 руководства пользователя программы или с помощью ее Справки) порядок применения основных и добавленных фильтров в зависимости от режима работы сетевого экрана.

Изучить (с помощью раздела 6.2 руководства пользователя или с помощью Справки программы) функции программы по отображению и использованию IP-адресов незащищенных узлов, трафик с которых (или на которые) блокируется сетевым экраном (кнопка «Блокированные IP-пакеты» в левой части главного окна программы).

Изучить (с помощью раздела 6.4 руководства пользователя программы или с помощью ее Справки) функцию просмотра статистики работы сетевого экрана (количества пропущенных и заблокированных пакетов и широковещательных сообщений) – кнопка «Статистика» в левой части главного окна программы.

Изучить (с помощью раздела 6.5 руководства пользователя или с помощью Справки программы) функцию настройки входящей в состав сетевого экрана системы обнаружения атак (кнопка «Обнаружение атак» в левой части главного окна программы):

- во входящем потоке; в
- исходящем потоке.

Изучить (с помощью раздела 6.6 руководства пользователя программы или с помощью ее Справки) функции программы по работе с журналом IP-пакетов (кнопка «Журнал IP- пакетов» в левой части главного окна программы):

- сформировать условия для поиска информации в журнале регистрации IP- пакетов:
  i. начало и конец интервала регистрации;
  ii. IP-адреса пакетов;
  iii. типы пакетов – входящие и (или) исходящие;
  iv. номера местного («своего») и внешнего («чужого») портов;
  v. тип протокола;
  vi. количество обращений (диапазон или конкретное значение);
  vii. количество отображаемых записей журнала (0 – отображаются все удовлетворяющие заданному условию записи);
  viii. тип зарегистрированного события (по умолчанию все);
- нажать кнопку «Найти» и ознакомиться со структурой журнала регистрации IP-пакетов;
- закрыть окно просмотра журнала;
- открыть окно настройки журнала регистрации IP-пакетов (кнопка «Настройка журнала» в левой части главного окна программы) и ознакомиться с параметрами настройки:
  i. интервал регистрации IP-пакетов;
  ii. размеры архива журналов и текущего журнала;
  iii. тип регистрации IP-пакетов;
  iv. режимы регистрации широковещательных пакетов и TCP-

соединений.

Изучить основные функции программы «Контроль приложений»:

- в окне «Режимы» сетевого экрана включить выключатель «Разрешить мониторинг активности приложений» (должна разблокироваться кнопка  в строке состояния главного окна программы);
- открыть окно настройки программы «Контроль приложений», нажав на соответствующую кнопку в строке состояния сетевого экрана;
- ознакомиться с назначением программы «Контроль приложений» с помощью ее Справки;
- добавить приложение в один из списков программы («белый» или «черный»):
  i. выполнить команду «Добавить» контекстного меню объекта «Зарегистрированные приложения» в правой части главного окна программы);
  ii. выбрать приложение для регистрации (например, calc.exe из каталога ОС Windows);
  iii. выбрать тип списка;
- повторить предыдущий пункт для добавления приложения в другой список программы;
- просмотреть свойства приложений, помещенных в один из списков программы (команда «Свойства» контекстного меню соответствующего объекта в правой части окна программы);
- с помощью Справки программы «Контроль приложений» ознакомиться с возможностями ее настройки (кнопка «Настройка» в левой части окна программы):
  i. режимы работы программы (приостановить слежение, показывать полные пути к файлам, разрешить соединения системного уровня);
  ii. способ авторизации программ;
  iii. политика – действия программы при регистрации приложения (по умолчанию тип списка определяется пользователем) и при неуспешной авторизации (по умолчанию реакция определяется пользователем);
- с помощью Справки программы «Контроль приложений» ознакомиться с ее функциями по просмотру и настройке журнала:
  i. открыть окно просмотра журнала (кнопка «Журнал» в левой части окна программы) и нажать кнопку «Обновить»;
  ii. изучить структуру записей журнала;
  iii. открыть окно настройки отображения событий в журнале (кнопка «Фильтр» в левой части окна программы);
  iv. изучить состав и назначение параметров отображения

событий в журнале;

v. открыть окно настройки журнала (кнопка «Настройка журнала») в левой части окна программы;
vi. изучить состав и назначение параметров настройки журнала;

- завершить работу программы «Контроль приложений».

Пользуясь информацией из файла *Быстрый старт.doc*выполнить удаление программного средства ViPNet[Персональный сетевой экран], согласившись со всеми вариантами удаления. По запросу программы удаления произвести перезагрузку ОС.

Включить в электронный вариант отчета о лабораторной работе копии экранных форм
(основных и дополнительных) изученных в данной работе программных средств ViPNet[Персональный сетевой экран] и «Контроль приложений».

Включить в электронный и печатный варианты отчета о лабораторной работе ответы на контрольные вопросы в соответствии с выданным преподавателем списком.

Контрольные вопросы

1. Для чего предназначена программа ViPNet[Персональный сетевой экран] и в чем заключаются ее основные функции?
2. Как происходит запуск программы ViPNet[Персональный сетевой экран]?
3. Какой режим работы программы ViPNet[Персональный сетевой экран] обеспечивает абсолютную защиту компьютера и почему?
4. В каких случаях целесообразноиспользоватьрежим пропуска только разрешенного сетевыми фильтрами IP-трафика?
5. В чем заключается режим жесткого бумеранга?
6. Чем отличается режим мягкого бумеранга?
7. Какой из режимов программы ViPNet[Персональный сетевой экран] позволяет только вести журнал IP-пакетов?
8. Какой из режимов программы ViPNet[Персональный сетевой экран] приводит и к отсутствию фильтрации IP-пакетов, и к отсутствию их регистрации в журнале?
9. Для чего в программе ViPNet[Персональный сетевой экран] может использоваться функция блокировки?
10. Какие варианты блокировки предусмотрены в программе ViPNet[Персональный сетевой экран]?
11. Как создать основной фильтр для конкретного IP-адреса?
12. Какая информация должна быть задана при создании сетевого фильтра для
конкретного IP-адреса?
13. Как создать добавленный фильтр для конкретного IP-адреса?
14. Как создать добавленный фильтр для всех незарегистрированных IP-адресов?
15. Какая информация должна быть задана при создании добавленного фильтра для
протокола ICMP?
16. Какая информация должна быть задана при создании добавленного фильтра для
протокола TCP?
17. Какая информация должна быть задана при создании добавленного фильтра

для
протокола UDP?
18. Как применяются сетевые фильтра при работе программы ViPNet[Персональный
сетевой экран] в режимах 1, 4 или 5?
19. Как применяются сетевые фильтры, если установлен режим 2?
20. Как применяются сетевые фильтры, если установлен режим 3?
21. Для чего в программе ViPNet[Персональный сетевой экран] используется окно
«Блокированные IP-пакеты»?
22. Как просмотреть статистику работы программы ViPNet[Персональный сетевой
экран]?
23. Какая информация отображается в окне статистики программы ViPNet[Персональный сетевой экран]?
24. Для чего предназначена входящая в состав программы ViPNet[Персональный
сетевой экран] система обнаружения атак?
25. Как настроить систему обнаружения атак в программе ViPNet[Персональный
сетевой экран]?

26. Какие параметры используются при настройке системы обнаружения атак в программе ViPNet[Персональный сетевой экран]?
27. Для чего предназначен журнал программы ViPNet[Персональный сетевой экран]?
28. Как сформировать условия для поиска информации в журнале программы
ViPNet[Персональный сетевой экран]?
29. Какие параметры используются для настройки отображения информации в
журнале программы ViPNet[Персональный сетевой экран]?
30. Как выполнить настройку журнала программы ViPNet[Персональный сетевой
экран]?
31. Какие параметры используются для настройки журнала программы ViPNet[Персональный сетевой экран]?
32. Для чего предназначена программа «Контроль приложений» и в чем заключаются
ее основные функции?
33. Как активизировать программу «Контроль приложений»?
34. Как добавить приложение к «белому» списку программы «Контроль приложений»?
35. Как добавить приложение к «черному» списку программы «Контроль приложений»?
36. В чем разница между сохраняемыми свойствами приложений, включенных в
«белый» и «черный» списки программы «Контроль приложений»?
37. Как выполнить настройку программы «Контроль приложений»?
38. Какие режимы работы программы «Контроль приложений» могут

быть
определены?

39. Какие способы авторизации приложений могут быть определены в программе
«Контроль приложений»?
40. Что означает термин «политика» в программе «Контроль приложений»?
41. Какой может быть реакция программы «Контроль приложений» при регистрации приложения?
42. Какой может быть реакция программы «Контроль приложений» при неудачной авторизации?
43. Как просмотреть журнал программы «Контроль приложений»?
44. Какая информация отображается в журнале программы «Контроль приложений»?
45. Как настроить отображениесобытий в журнале программы «Контроль приложений»?
46. Какие параметры используются при настройке отображения событий в журнале программы «Контроль приложений»?
47. Как настроить журнал программы «Контроль приложений»?
48. Какие параметры используются для настройки журнала программы «Контроль приложений»?

Списки контрольных вопросов для письменного ответа

№	Номера	№	Номера	№	Номера
1	1, 2, 9, 18, 32, 35	11	4, 13, 23, 29, 41,	21	1, 8, 16, 28, 38,
2	3, 10, 11, 19, 34,	12	16, 24, 28, 33, 38,	22	2, 17, 25, 27, 32,
3	4, 12, 20, 21, 37,	13	8, 15, 23, 27, 36,	23	3, 11, 13, 18, 36,
4	5, 13, 22, 27, 38,	14	7, 14, 20, 22, 34,	24	4, 14, 24, 30, 34,
5	6, 14, 23, 28, 39,	15	2, 12, 21, 31, 32,	25	5, 15, 20, 25, 35,
6	7, 15, 24, 29, 40,	16	3, 15, 20, 25, 39,	26	6, 16, 26, 31, 36,
7	8, 16, 25, 30, 41,	17	4, 9, 26, 27, 32, 47	27	7, 11,17, 27, 37,
8	17, 26, 31, 33, 42,	18	5, 10, 19, 22, 37,	28	8, 9, 18, 22, 38,
9	2, 10, 21, 27, 39,	19	6, 16, 26, 30, 40,	29	1, 10, 19, 33, 41,
10	3, 12, 22, 28, 40,	20	10, 11, 20, 32, 33,	30	2, 11, 17, 30, 37,

Лабораторная работа №8.Основы использования средств защиты от несанкционированного доступа в операционной системе Linux

Содержание задания

1. Выбрать при загрузке операционной системы вариант 1 (ASP Linux).
2. После загрузки операционной системы начать сеанс работы под именем userc указанным
преподавателем паролем.
3. Изучить способы регистрации пользователей и групп в системе:
а) запустить программу «Менеджер пользователей RedHat» (Главное меню | Система | Управление пользователями);
б) использовать команду «Не показывать системных пользователей и групп» меню
«Свойства» для управления списком пользователей;
в) освоить применение команд меню «Действие» - «Новый пользователь»,

«Добавить группу», «Свойства», «Удалить»;

г) создать учетную запись для себя, включив ее в группу «Users»;

д) запустить программу «Менеджер файлов», найти и просмотреть в каталоге /etc файлыpasswd, group, shadow и gshadow.

4. Включить в отчет о лабораторной работе ответы на следующие вопросы:

а) какая информация указывается при создании нового пользователя;

б) какая информация указывается при создании новой группы;

в) какой формат имеют записи файла passwd;

г) какой формат имеют записи файла group;

д) какой формат имеют записи файла shadow и для чего используется этот файл;

е) какой формат имеют записи файла gshadow и для чего используется этот файл.

5. Изучить средства управления настройками аутентификации:

а) запустить программу «Конфигурация распознавания» (Главное меню | Система | Настройка аутентификации);

б) открыть закладку «Аутентификация»;

в) ознакомиться с параметрами настройки аутентификации.

6. Включить в отчет о лабораторной работе ответы на следующие вопросы:

а) как включается и выключается режим использования скрытых паролей; б) что происходит при включении режима использования скрытых паролей; в) для чего предназначен режим использования скрытых паролей.

7. Освоить средства изменения пароля текущего пользователя (Главное меню | Утилиты |
Пароли) для созданной при выполнении п. 3.г учетной записи.

8. Освоить средства блокировки терминала при временном отсутствии пользователя:

а) немедленная блокировка (Контекстное меню Рабочего стола | Заблокировать экран);

б) использования хранителя экрана (Контекстное меню Рабочего стола | Настроить Рабочий стол |Хранитель экрана).

9. Включить в отчет о лабораторной работе ответ на следующий вопрос: в чем разница между изученнымисредствами блокировки терминала и какой из них является, на Ваш взгляд, более предпочтительным и почему.

10. Освоить средства разграничения доступа к файлам:

а) с помощью программы «Менеджер файлов» и команды «Свойства"»контекстного меню файла (закладка «Права») получить и включить в отчет о лабораторной работе права доступа пользователей к файламpasswd, group, shadow и gshadow (каталог /etc),

каталогу /etc, файлу /usr/bin/passwd, своемудомашнему каталогу (в каталоге /home), каталогу /tmp;

б) с помощью системной консоли (Главное меню | Система | Консоль (Терминал)) выполнить командыumask (получение значения переменной среды umask в восьмеричном виде) и umask -S (полученизначения переменной среды umask в символическом виде).

11. Включить в отчет о лабораторной работе ответы на следующие вопросы:

а) почему для файлов и каталогов, перечисленных в п. 10.а, установлены

именно такие правадоступа (дать пояснение по каждому файлу и каталогу);

б) почему для файла /usr/bin/passwd установлен дополнительный бит прав доступа SUID;

в) в чем смысл использования и потенциальная опасность дополнительных битов доступа SUIDи SGID;

г) какая политика разграничения доступа к файлам используется в операционной системе Linuxи чем она отличается от политики разграничения доступа к объектам в защищенных версияхоперационной системы Windows;

д) для чего используется переменная среды umask и что означает ее значение, определенное привыполнении п. 10.б;

е) кто может изменять права доступа к файлам.

12. Освоить средства определения параметров политики аудита и просмотра журнала аудита:

    а) открыть файл /etc/syslog.conf;

    б) включить в отчет о лабораторной работе сведения о правах доступа к файлу /etc/syslog.confи формате записи этого конфигурационного файла;

    в) открыть файл /var/log/secure и ознакомиться с его содержимым;

    г) открыть файл /var/log/messages и ознакомиться с его содержанием;

    д) включить в отчет о лабораторной работе сведения о правах доступа к файлам, указанным в п.п.12.в и 12.г.

13. Включить в отчет о лабораторной работе ответы на следующие вопросы:

    а) в чем назначение файла /etc/syslog.conf и какая информация в нем содержится;

    б) почему к файлам /etc/syslog.conf, /var/log/secure и /var/log/messages определены именнотакие права доступа;

    в) как может быть задана реакция на то или иное событие и в чем может заключаться эта реакция(помимо записи в журнал аудита).

14. Сохранить отчет о выполнении лабораторной работы в виде текстового файла (созданного, например,с помощью редактора KWrite - Главное меню | Редакторы) в своем домашнем каталоге (в подкаталоге сидентифицирующем Вас именем). Определить для этого файла права доступа, позволяющие всем другимпользователям знакомиться с его содержанием.

15. После проверки отчета преподавателем удалить файл с отчетом, предварительно сохранив его на дискете в формате HTML,и завершить сеанс работы (Главное меню | Завершить сеанс), после чего остановить систему (с помощью меню «Система» при входе в систему).

Самостоятельная работа

При изучении дисциплины «Управление информационной безопасностью» обязательными являются следующие виды самостоятельной работы:
- разбор теоретического материала по учебным пособиям и конспектам лекций;
- самостоятельное изучение указанных теоретических вопросов; подготовка к проведению ситуационных моделей в интерактивной форме;

№ темы дисциплины	Форма самостоятельной работы	Трудоемкость в часах
1–8	Работа с учебной литературой. Разбор вопросов по теме занятия. Работа с источниками и поиск информаций в Интернете.	32
1-8	Выполнение контрольной работы.	16
4, 6	Подготовка к интерактивному занятию	13
	Подготовка к экзамену	27
Итого:		**90**

Система оценивания

Уровень требований и критерии оценок

Текущий контроль усвоения знаний по дисциплине «Управление информационной безопасностью» осуществляется в течение семестра в ходе учебного процесса и консультирования студентов, по результатам выполнения аудиторных самостоятельных проверочных работ, контрольной работы и активного участия в проведении занятия в интерактивной форме.

- Основными формами текущего контроля знаний являются: решение проблемных задач по управлению информационной безопасностью;
- участие в обсуждении актуальных вопросов, связанных с введением новых требований по обеспечению информационной безопасности предприятий различных форм собственности, в проведении занятия в интерактивной форме;
- собеседование по теоретическим вопросам;
- выполнение аудиторных самостоятельных работ, контрольной работы, обсуждение и анализ их результатов. Промежуточная аттестация (экзамен) проводится в письменной форме в виде ответов на вопросы билета. Оценка знаний студентов осуществляется в баллах с учетом: оценки за работу в семестре (за: по управлению информационной безопасностью, успешное выполнение контрольной и самостоятельных проверочных работы, активное участие в обсуждениях на практических занятиях и др.); оценки итоговых знаний в ходе экзамена.

Оценка знаний студентов осуществляется по 100-балльной шкале в соответствии с критериями Финансового университета и реализуются следующим образом:

Требования к результатам освоения дисциплины	**Оценка или зачет**	**Баллы** (рейтиговая оценка)
Глубокое усвоение программного материала, связанного со знанием понятийного аппарата, определением в бизнес-процессах, методик оценки уровня информационной безопасности организации и примеров их использования, методов противодействия «внутренним» угрозам информационной безопасности организации, архитектуры основных стандартов защиты информации; умением использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы организационного проектирования, методы управления информационными активами организации; владением навыками использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации, а также логически стройное его изложение, умение применить теоретические знания для решения задач, свободное решение задач и обоснование принятого решения, выполнение текущей работы в семестре.	*отлично*	*86-100*

Твердые знания программного материала, связанного понятийным аппаратом, бизнес-процессов, методик оценки уровня информационной безопасности организации и примеров их использования, методов противодействия «внутренним» угрозам информационной безопасности организации, архитектуры основных стандартов защиты информации; умением использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы организационного проектирования, методы управления информационными активами организации; владением навыками использования методов изучения структуры современной	*хорошо*	*66-85*
Знание только основного материала, понятийного аппарата, определением в бизнес-процессах, методик оценки уровня информационной безопасности организации и примеров их использования; умением использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня	*удовлетв.*	*51-65*
методы анализа рисков информационной безопасности, методы организационного проектирования; владением навыками использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации, а также допустимы неточности в ответе на вопрос, недостаточно правильные формулировки, нарушение логической последовательности в		
Незнание значительной части программного материала, неумение сформулировать правильные ответы на вопросы экзаменационного билета,	неудовлетв.	0-50

Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература
а) основная:

1. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.Международный стандарт. ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы./ http://www.27000.org/
2. Аудит информационной безопасности. Под ред. А.П.Курило. – М: БДЦ-Пресс, 2014.
3. Галатенко В.А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий, 2006 г. – 264 с.
4. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005)./ http://www.27000.org/
5. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью./ http://www.27000.org/Международный стандарт. ISO/IEC 27003:2005 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью./ http://www.27000.org/
6. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью./ http://www.27000.org/
7. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности./ http://www.27000.org/
8. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью./ http://www.27000.org/
9. Международный стандарт. ISO/IEC 27007:2005 Информационные технологии. Методы обеспечения безопасности. Руководство для аудитора систем управления информационной безопасностью./ http://www.27000.org/
10. Минаев В.А., Фисун А.П. Правовое обеспечение информационной безопасности, Москва, 2014.
11. Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2012.
12. Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: ДМК пресс, 2013.
13. Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Стандарты и качество, 2014.
14. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: Академия, 2008 г. – 192 стр.
15. Тихонов В., Райх В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. – М.: Гелиос АРВ, 2012.

б) дополнительная:

1. Золотарев Управление информационной безопасностью. Ч. 1. Анализ информационных рисков - Красноярск: Сибирский государственный

аэрокосмический университет имени академика М. Ф. Решетнева, 2010.

Материально-техническое обеспечение дисциплины

В качестве материально-технического обеспечения дисциплины «Управление информационной безопасностью» используются мультимедийные средства, компьютерные симуляторы, графические презентационные материалы.