МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ОЦЕНОЧНЫЕ СРЕДСТВА)

Шифр	Наименование дисциплины (модуля)
Б1.В	**Программно-аппаратное обеспечение информационной безопасности**

Код направления подготовки	44.04.04
Направление подготовки	Профессиональное обучение (по отраслям)
Наименование (я) ОПОП (направленность / профиль)	Управление информационной безопасностью в профессиональном образовании
Уровень образования	магистр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Старший преподаватель	кандидат педагогических наук		Гафарова Елена Аркадьевна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	10	13.06.2019	
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	1	13.09.2020	

Раздел 1. Компетенции обучающегося, формируемые в результате освоения образовательной программы с указанием этапов их формирования

Таблица 1 - Перечень компетенций, с указанием образовательных результатов в процессе освоения дисциплины (в соответствии с РПД)

Формируемые компетенции			
Индикаторы ее достижения	**Планируемые образовательные результаты по дисциплине**		
	знать	**уметь**	**владеть**
ПК-18 способен участвовать в мониторинге эффективности применяемых инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности			
ПК.18.1 Знает современные способы мониторинга эффективности применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП	З.3 понятие и современное состояние средств информационной защиты; понятие семиуровневой системы обеспечения информационной безопасности		
ПК.18.2 Умеет проводить мониторинг эффективности применения инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности в области организации ВО, современного профессионального образования, ДПО и ДПП		У.3 умеет прводить оценку информационной защищенности	
ПК.18.3 Владеет способами управления мониторингом инженерно-техническими и программно-аппаратными средствами обеспечения информационной безопасности в организациях ВО, современного профессионального образования, ДПО и ДПП			В.3 владеет опытом управления ИБ посредством обучения сотрудников (студентов)
ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности			
ПК.16.1 Знает научные тенденции отечественных и зарубежных исследований перспективных технологий применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП	З.1 сущность информационной безопасности, правовые нормы, регламентирующие ее реализацию		

ПК.16.2 Умеет применять перспективные технологические разработки инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП		У.1 □ давать оценку защищенности информационной системе	
ПК.16.3 Владеет научными основами практики применения перспективных технологические разработки инженер-но-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, сов-ременного профессионального образования, ДПО и ДПП			В.1 опытом выстраивать комплексную систему защиты информации по принципу разумной достаточности

ПК-17 способен участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего состояния, в проведении технического обслуживания и текущего ремонта, выявлении технических каналов утечки информации и оценке возникающих опасностей, устранении отказов и восстановлении работоспособности

ПК.17.1 Знает содержание теории и практики эксплуатации, диагностики, технического обслуживания и ремонта инженерно-технических средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП	З.2 □ компоненты программно-аппаратных средств обеспечения информационной защиты		
ПК.17.2 Умеет квалифицированно проводить эксплуатацию, диагностику, техническое обслуживание и ремонт инженерно-технических средств обеспечения информационной безопасности в области организации ВО, современного профессионального образования, ДПО и ДПП		У.2 □ применять на практике программно-аппаратные средства ОИБ	
ПК.17.3 Владеет способами эксплуатации, диагностики, технического обслуживания и ремонта инженерно-технических средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП			В.2 владеет опытом применения информационной защиты

УК-3 способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

УК.3.1 Знает жизненный цикл команды, основы ее формирования и развития; основы обеспечения эффективности командной работы и руководства ею; функции, обязанности проект-менеджера, требования к нему	З.4 основы проектной технологии		
УК.3.2 Умеет разрабатывать стратегию командной работы; формировать команду, планировать командную работу, распределять поручения и делегировать полномочия, инструктировать членов команды, организовывать и управлять их конструктивным взаимодействием		У.4 умеет руководить командной работой	
УК.3.3 Владеет инструментами и методами мотивации участников командной работы; методиками изучения и коррекции психологического климата группы, предупреждения и решения возникающих в команде разногласий и конфликтов; методами оценки компетенций и опыта участников команды; методами установления коммуникативных связей, организации и проведения совещаний, ведения переговоров			В.4 владеет опытом управления командной работы

Компетенции связаны с дисциплинами и практиками через матрицу компетенций согласно таблице 2.

Таблица 2 - Компетенции, формируемые в результате обучения

Код и наименование компетенции	
Составляющая учебного плана (дисциплины, практики, участвующие в формировании компетенции)	**Вес дисциплины в формировании компетенции (100 / количество дисциплин, практик)**
ПК-18 способен участвовать в мониторинге эффективности применяемых инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности	
Программно-аппаратное обеспечение информационной безопасности	**100,00**
ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности	
Программно-аппаратное обеспечение информационной безопасности	**33,33**
Организационно-правовое обеспечение информационной безопасности образовательной организации	33,33
Цифровизация и квалиметрическая оценка учебных достижений в образовательной организации	33,33

ПК-17 способен участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего состояния, в проведении технического обслуживания и текущего ремонта, выявлении технических каналов утечки информации и оценке возникающих опасностей, устранении отказов и восстановлении работоспособности	
Программно-аппаратное обеспечение информационной безопасности	**100,00**
УК-3 способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	
производственная практика (педагогическая)	14,29
Программно-аппаратное обеспечение информационной безопасности	**14,29**
Стандартизация и сертификация аппаратно-программного обеспечения	14,29
Управление закупками	14,29
Проектирование и мониторинг образовательных результатов	14,29
Психология профессионализма	14,29
учебная практика (научно-исследовательская работа)	14,29

Таблица 3 - Этапы формирования компетенций в процессе освоения ОПОП

Код компетенции	Этап базовой подготовки	Этап расширения и углубления подготовки	Этап профессионально-практической подготовки
ПК-18	**Программно-аппаратное обеспечение информационной безопасности**		
ПК-16	**Программно-аппаратное обеспечение информационной безопасности, Организационно-правовое обеспечение информационной безопасности образовательной организации, Цифровизация и квалиметрическая оценка учебных достижений в образовательной организации**		
ПК-17	**Программно-аппаратное обеспечение информационной безопасности**		

УК-3	**производственная практика (педагогическая), Программно-аппаратное обеспечение информационной безопасности, Стандартизация и сертификация аппаратно-программного обеспечения, Управление закупками, Проектирование и мониторинг образовательных результатов, Психология профессионализма, учебная практика (научно-исследовательская работа)**		производственная практика (педагогическая), учебная практика (научно-исследовательская работа)

Раздел 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 4 - Показатели оценивания компетенций на различных этапах их формирования в процессе освоения учебной дисциплины (в соответствии с РПД)

№	Раздел	
	Формируемые компетенции	
	Показатели сформированности (в терминах «знать», «уметь», «владеть»)	**Виды оценочных средств**
1	Основные средства и методы программно-аппаратной защиты информации	
	ПК-16	
	Знать сущность информационной безопасности, правовые нормы, регламентирующие ее реализацию	Тест
	Уметь давать оценку защищенности информационной системе	Опрос
2	Идентификация, аутентификация. Управление доступом.	
	ПК-16 ПК-17	
	Знать компоненты программно-аппаратных средств обеспечения информационной защиты	Тест
	Уметь применять на практике программно-аппаратные средства ОИБ	Отчет по лабораторной работе
	Владеть опытом выстраивать комплексную систему защиты информации по принципу разумной достаточности	Отчет по лабораторной работе
3	. Протоколирование и аудит. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств	
	ПК-17 ПК-18	
	Знать понятие и современное состояние средств информационной защиты; понятие семиуровневой системы обеспечения информационной безопасности	Тест
	Владеть владеет опытом применения информационной защиты	Кейс-задачи
4	Шифрование. Криптография.	
	ПК-18	
	Уметь умеет прводить оценку информационной защищенности	Кейс-задачи
	Владеть владеет опытом управления ИБ посредством обучения сотрудников (студентов)	Задача
5	Экранирование. Классификация межсетевых экранов.	
	УК-3	
	Знать основы проектной технологии	Реферат
	Уметь умеет руководить командной работой	Ситуационные задачи
6	Компьютерные вирусы как особый класс разрушающих программных воздействий и защита от них.	
	УК-3	
	Владеть владеет опытом управления командной работы	Эссе

Таблица 5 - Описание уровней и критериев оценивания компетенций, описание шкал оценивания

Код	**Содержание компетенции**			
Уровни освоения компетенции	**Содержательное описание уровня**	**Основные признаки выделения уровня (критерии оценки сформированности)**	**Пятибалльная шкала (академическая оценка)**	**% освоения (рейтинговая оценка)**
ПК-18	ПК-18 способен участвовать в мониторинге эффективности применяемых инженерно-технических и программно-аппаратных средств обеспечения информационной...			
ПК-16	ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности			

ПК-17	ПК-17 способен участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состоян...
УК-3	УК-3 способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Раздел 3. Типовые контрольные задания и (или) иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (модулю)

1. Оценочные средства для текущего контроля

Раздел: Основные средства и методы программно-аппаратной защиты информации

Задания для оценки знаний

1. Тест:

1. Выберите все правильные варианты ответов
Активным видом атак является
 отказ в обслуживании - DoS-атака (Denial of Service)
 модификация потока данных - атака "man in the middle"
 фальсификация (нарушение аутентичности) - попытка одного субъекта выдать себя за другого
 прослушивание (сниффинг)
 анализ трафика
2. Выберите все правильные варианты ответов
Алгоритм симметричного шифрования может быть применим в
 шифровании большого потока данных
 создании определенного количества случайных битов
 хэшировании данных
 секретной передаче ключа
3. Выберите все правильные варианты ответов
Односторонняя функция с секретом - это
 односторонняя функция, которую легко вычислить в одном направлении и трудно вычислить в обратном направлении до тех пор, пока недоступна некоторая дополнительная информация
 при наличии дополнительной информации инверсию можно вычислить за полиномиальное время
 при наличии дополнительной информации инверсию можно вычислить за экспоненциальное время
4 Выберите все правильные варианты ответов
Укажите основные угрозы информационной безопасности в вычислительных сетях
 несанкционированный доступ к информации
 искажение информации или подлог (имитация)
 отказ от авторства
 отказ от шифрования
 взлом сейфа с ценными бумагами
5. Выберите все правильные варианты ответов
В необходимый минимум средств защиты от вирусов входит:
 архивирование
 профилактика
 входной контроль

Задания для оценки умений

1. Опрос:

Что такое программный вирус и какова его природа?
2.
В чем состоят вредные проявления компьютерных вирусов?
3.
Какие основные виды компьютерных вирусов вам известны?
4.
Какие существуют виды программ для обнаружения и защиты от вирусов?
5.
В чем состоят достоинства программ-ревизоров и программ-фильтров?
6.
Назовите основные меры по защите от компьютерных вирусов.
7.
Опишите технологию периодической проверки жесткого диска на наличие вирусов.

Задания для оценки владений

Раздел: Идентификация, аутентификация. Управление доступом.

Задания для оценки знаний

1. Тест:

.. Выберите правильный вариант ответа
Если n человек хотят обмениваться между собой конфиденциально (на основе симметричного криптоалгоритма) сообщениями, то необходимо
- n(n-1) ключей
- n(n-1)/2 ключей
- (n-1)! Ключей

7.Выберите все правильные варианты ответов
"Безопасное" хранение паролей можно обеспечить на основе
- упрятывания пароля в тело программы
- шифрования пароля
- хранения хэша пароля
- хранения "подсоленого" хэша пароля
- соль "подсоленого" хэша пароля является тайной
- соль "подсоленого" хэша пароля может храниться открыто

8. Выберите все правильные варианты ответов
Пространство имен System.Security.Cryptography содержит набор классов, обеспечивающий работу
- алгоритмов цифровой подписи данных
- алгоритмов вычисления контрольных избыточных кодов данных
- алгоритмов кодирования base64
- симметричных криптографических алгоритмов
- ассиметричных криптографических алгоритмов
- алгоритмов получения хэша данных

9.Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода.
- Макровирус
- Троянский конь
- Червь
- Файловый вирус

10. Выберите правильный вариант ответа
Прослушивание данных (sniffing) в локальных сетях Ethernet, построенных на основе коммутаторов, сопряжено с трудностями, поскольку коммутаторы передают трафик непосредственно получателю. Тем не менее, если в сети используется TCP/IP, то существует легко реализуемая на практике атака, позволяющая злоумышленнику встроиться между отправителем и получателем и прослушивать трафик. Это делается путем отправки обеим сторонам специальных пакетов. Уязвимость какого протокола эксплуатируется в этой атаке?
- TCP
- UDP
- IP
- ICMP
- ARP
- RIP

Задания для оценки умений

1. Отчет по лабораторной работе:

Лабораторная работа: Установка паролей в документы MSWord и MS Excel.
Цель: научиться ставить пароли на документы в MSWord и MS Excel.
Теоретические сведения
В документах MS Office предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным и их изменением.

Просмотр документов MS Word, книг MS Excel и баз данных MS Access может быть ограничен с помощью парольной защиты (пароль для открытия файла). При установке пароля на открытие документа содержимое файла шифруется (алгоритм шифрования AES).
Для документов MS Word и MS Excel также имеется возможность установки парольной защиты на сохранение внесенных изменений (пароль разрешения записи). Если пользователю не известен пароль разрешения записи, он может открыть документ в режиме «только для чтения». В этом случае возможно внесение изменений в текст документа, однако нельзя сохранить измененный файл документа под старым именем. Для сохранения изменений требуется ввести новое имя файла.
Пароль на открытие, пароль разрешения записи устанав-лива-ются на файл, то есть относятся к документу/книге в целом.
Кроме паролей на файл в целом, имеются возможности защиты отдельных элементов документов MS Office:
Парольная защита от просмотра элементов книги Excel (строк, столбцов, листов). Невозможно защитить от просмотра часть документа MS Word, отдельные ячейки книги MS Excel;
Парольная защита от изменения частей (разделов) документа Word, содержимого отдельных ячеек и их диапазонов в Excel, структуры листа (вставка, удаление и форматирование строк и столбцов),структуры книги (добавление и удаление листов, отображение, скрытые листов), изменение размеров, положения или видимости окна, настроенного для отображения книги Excel.
Разграничение доступа (возможность изменения) к диапазонам ячеек Excel для локальных и сетевых пользователей ОС Windows;
Разграничение доступа аутентифи-ци-ро-ванн-ных пользователей к фрагментам текста MS Word, задан ограничений на несанкционированное распространение документа (пересылка по электронной почте, изменение, копирование) требует установки дополнительного программного обеспечения (сервера аутентификации, WRM – клиента управления правами Windows).
Следует учитывать, что функциональные возможности парольной защиты на отдельные элементы MS Excel (скрытие данных и защита листов и книг) и MS Word (защита разделов) не предназначены для защиты данных или важных сведений в документах MS Office.
Они используются для более понятного представления сведений, скрывая сведения или формулы, которые могут сбить с толку некоторых пользователей. Эти средства служат также для предотвращения случайного изменения данных пользователями. Скрытые или защищенные паролем данные внутри документов MS Office не шифруются. При определенных усилиях и наличии времени пользователи смогут просмотреть и изменить все сведения внутри документа MS Office, если они имеют доступ к самому документу (пароль на открытие документа не установлен или известен).
Чтобы предотвратить изменение данных и обеспечить безопасность важных сведений, следует ограничить доступ к файлам (пароль на открытие файла), содержащим подобные сведения, сохранив их в расположениях, доступных только пользователям, прошедшим аутентификацию (разграничение доступа к файлам и папкам средствами ОС).
В документах MS Office имеется возможность заверять цифровой подписью как документ в целом, так и внедренный в документ код макросов на языке VBA. Наличие действительной цифровой подписи гарантирует целостность (неизменность) содержимого, а также аутентичность и неотрекаемость (подлинность авторства и невозможность отказа от авторства).
Полноценная проверка подлинности цифровых подписей возможна в том случае, если они выданы сетевым сервером аутентификации (в домене локальной сети), либо доверенным центром сертификации в Интернете. Если же используется локальный сертификат, создаваемый самим пользователем с помощью утилиты selfcert.exe (Digital Certificate for VBA Projects, Цифровой сертификат для проектов VBA), то проверить на другом компьютере подлинность подписи, созданной с его помощью, будет невозможно. Кроме того, другие пользователи локального компьютера также не будут доверять такой подписи.
Один из самых простых, но в то же время надежных способов защиты своих документов – это установить пароль на документ Microsoft Word. Человек, не знающий пароля, попросту не сможет этот документ открыть. Есть несколько способов установить пароль. Один из них – это использование стандартных средств Microsoft Office. Причем можно установить пароль как и на открытие документа MS Word, так и на изменение содержимого документа.
Для того чтобы установить пароль для своего документа Microsoft Word, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 6).

Рисунок 6 – Меню Сервис MS Word
После выполнения всех действий появится окно Microsoft Word – Параметры. В этом окне Microsoft Word - Параметры нужно перейти на закладку Безопасность (см. рисунок 7); далее в строке «пароль для открытия файла» ввести пароль. После ввода пароля нажмите кнопку ОК.
Рисунок 7 – Меню Безопасность MS Word
Для безопасности документа Microsoft Excel можно установить свой пароль на открытие документа. После того как вы установили пароль на открытие документа Microsoft Excel, Excel будет требовать пароль на открытие вашего документа.
Для того чтобы установить пароль для своего документа Microsoft Excel, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 8).

Рисунок 8 – Меню Сервис MS Excel

В этом окне Microsoft Excel – Параметры нужно перейти на закладку Безопасность(см. рисунок 9) далее в строке «пароль для открытия» ввести пароль. После ввода пароля нажмите кнопку ОК.

Рисунок 9 – Меню Безопасность MS Excel

После нажатия кнопки ОК появится окошко Microsoft Excel – «Подтверждения пароля», здесь вам нужно будет еще раз ввести пароль, который вы вводили, и нажать кнопку ОК (см. рисунок10).

Рисунок 10 – Меню Подтверждение пароля MS Excel

При установке пароля стоит помнить об очень важных моментах. Пароль можно «сломать». Для этого есть немало программ. Особенно легко «взламывать» короткие пароли. Поэтому желательно чтобы пароль был сложный. Лучше всего, чтобы пароль состоял как из латиницы, так и из кириллицы. Для надежности можно добавить еще несколько цифр. Желательно использовать пароль минимум из семи символов. Чем сложнее пароль, тем меньше шансов, что он будет «взломан». Но также не нужно слишком усердствовать, так как можно этот пароль забыть и самому. А еще лучше пароль записать и хранить в надежном месте, на случай если вы его забудете. Также для дополнительной защиты можно заархивировать документ и установить пароль к архиву. Тогда вероятность того, что кому-либо удастся сломать защиту, становится крайне низкой.

Чтобы установить пароль для защиты базы данных MS Access:

- закройте базу данных. Если база данных совместно используется в сети, убедитесь, что остальные пользователи ее закрыли;
- сделайте резервную копию базы данных и сохраните ее в надежном месте;
- в меню MS Access выберите команду Файл/Открыть;
- выделите файл базы данных;
- щелкните по стрелке, расположенной справа от кнопки Открыть . В раскрывающемся списке режимов открытия базы данных выделите элемент Монопольно. База данных откроется в режиме монопольного доступа;
- выберите команду Сервис/Защита/Задать пароль базы данных (см. рисунок11);

Рисунок 11 – Меню Задание пароля базы данных MS Access

- в появившемся диалоговом окне введите в поле Пароль пароль для защиты базы данных с учетом регистра символов;
- введите пароль еще раз в поле Подтверждение;
- нажмите кнопку ОК.

Теперь база данных защищена паролем, и всякий раз, когда пользователь будет открывать базу данных, будет отображаться диалоговое окно с требованием ввести пароль. Запомните или сохраните пароль в надежном месте. Если вы забудете пароль, базу данных будет невозможно открыть.

Контрольные вопросы:

1. Чем различается действие защиты от изменения текста документа, установленной с помощью защиты форм (команда Защитить документ) и защиты в режиме «только для чтения» (установка на файл пароля разрешения записи)?
2. Чем различается действие защиты от изменения в случае задания пароля разрешения записи и в случае рекомендации открытия документа в режиме «только для чтения»?

Задание для самостоятельного выполнения:

В приложении MS Word создайте короткий опросник (анкету) с защищенным от изменения текстом вопросов для получения от пользователей различных данных. Сформулировать вопросы так, чтобы требовались:

ответы в произвольной форме, подразумевающие ввод текста, (например, ФИО, какие-либо комментарии или пожелания, номер учебной группы, дата заполнения),

выбор даты (дата дня рождения, начала сессии, рекомендуемая дата мероприятия или посещения и т.п.),

выбор единственного варианта ответа из списка и с помощью переключателей (например, пол, возрастная группа, форма обучения, специальность),

выбор нескольких вариантов с помощью флажков (например, знания, предпочтения, сферы интересов, участие в мероприятиях и т.п.)

Для вставки в документ флажков и переключателей используйте инструменты из предыдущих версий Word – кнопка на вкладке Разработчик..

Описание формы отчета

Выполненное задание для самостоятельной работы и ответы на контрольные вопросы необходимо выслать для проверки преподавателю.

ЛАБОРАТОРНАЯ РАБОТА: ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ (RSA, СХЕМЫ ШНОРРА И ФЕЙГЕ-ФИАТА-ШАМИРА)

Цель: В лабораторной работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:
- на основе алгоритма RSA;
- по схеме Шнорра;
- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа (k или r) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

Теоретические сведения

Идентификация (англ. identification) - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов).

Аутентификация (англ. authentication) - проверка соответствия (подлинности) сущности предъявленному ею идентификатору. (Заметим, что происхождение русскоязычного термина «аутентификация» не совсем понятно. Английское «authentication» скорее можно прочитать как «аутентикация»; трудно сказать, откуда в середине взялось еще «фи» – может, из идентификации? Тем не менее, термин устоялся и закреплен в РД Гостехкомиссии РФ).

Для полноты картины приведем определение термина авторизация, который не следует путать с двумя вышеприведенными. Авторизация (англ. authorization) - предоставление сущности возможностей в соответствии с положенными ей правами или проверка наличия прав при попытке выполнить какое-либо действие.

Идентификация и аутентификация – это первая линия обороны, «входная дверь» в информационное пространство организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.

Идентификация сродни присвоении имени ребенку (не совсем точное сравнение, но все же). В любой ИС должны быть определены все субъекты, участвующие в информационном обмене. Часть из них может быть сгруппирована, если они наделены одинаковыми (схожими) правами и обладают одинаковыми (схожими) характеристиками. Каждый субъект (группа субъектов) должен обладать уникальным именем (обозначением).

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

Субъект может подтвердить свою подлинность, предъявив один из следующих аутентификаторов:
- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (паспорт, личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев, образец ДНК и т.п.).

В том случае, если в ходе процедуры аутентификации клиент должен предъявить сразу несколько аутентификаторов, аутентификация называется многофакторной. Например, в ходе двухфакторной аутентификации клиент должен знать пароль и воспользоваться личной карточкой.

Основные программно-технические способы реализации идентификации и аутентификации: пароли, с использованием хеш-функции, на основе шифрования с открытым ключом, идентификационные карты и электронные ключи, сервер аутентификации Kerberos/

Введенный пользователем пароль сравнивается с паролем, имеющимся в БД, хранящейся в защищаемой ИС, и если они совпадают, то дается разрешение на использование защищаемых ресурсов.

Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в ОС, СУБД и программные продукты. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Парольная аутентификация имеет массу недостатков:
- как правило, пароль генерируется в одном месте (например, на сервере) и должен быть передан во второе (например, клиенту). При передаче пароль может быть перехвачен злоумышленником;
- многие ОС и приложения имеют пароли, указанные производителем по умолчанию. После установки такой системы очень часто забывают их удалить. БД стандартных паролей можно найти в Интернете;

- злоумышленник может получить БД паролей, хранящихся в зашифрованном виде, и воспользоваться ей:
- в Windows NT/2000/XP учетные записи (пользователи и пароли) хранятся в файле «%System Root% \ System32 \ Config \ sam». При работающем ОС пользователь не может выполнять операции чтения/записи с данным файлом (блокируется процессом lsass.exe, «убить» который невозможно). Получить доступ к файлу можно, загрузив ОС с другого носителя. Другой вариант заключается в использовании файла «%System Root% \ Repair \ sam». Он доступен для чтения/записи, но, как правило, содержит пароли «столетней» давности;
- в ранних версиях Unix файл с учетными записями «/etc/passwd» был доступен для чтения любым желающим. В современных разновидностях Unix файл с паролями «/etc/shadow» или «etc/secure» доступен только с привилегиями супервизора. Другой способ получения доступа к паролям – обрушения процесса, обращающегося к файлу с паролями. При этом Unix создает файл «core dump», содержащий дамп памяти (с паролями) [26];
- после получения файла с зашифрованными паролями можно воспользоваться многочисленными программами-взломщиками. Одними из самых популярных взломщиков являются: для Windows – L0phtCrack, для Unix – John the Ripper. Время, требуемое для взлома пароля, зависит от его качества. Так, например, взлом пароля для L0phtCrack на компьютере с процессором Xeon 400 МГц при использовании [26]:
- цифр и латиницы – 5,5 часов;
- всех символов – 480 часов.
- кроме перечисленных выше приемов взлома паролей, их можно подсмотреть (например, с помощью оптических приборов), сообщить другу/подруге (если секрет знают двое – это уже не секрет), записать на бумажке и приклеить на клавиатуру или монитор и т.п.

Тем не менее, так как парольная защита используется во многих продуктах и системах, можно порекомендовать следующие меры, позволяющие повысить надежность парольной защиты:
- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.). Еще лучше воспользоваться программами - генераторами паролей (ключей);
- ограничение доступа к файлу с паролями;
- удаление резервных копий файлов с паролями («%System Root% \ Repair \ sam»);
- использование защищенных протоколов обмена ключами (например, основанные на протоколе обмена ключами Диффи-Хеллмана);
- ограничение числа неудачных попыток входа в систему (это затруднит применение «метода грубой силы»). В Windows 2000 и XP этот параметр устанавливается по пути «Администрирование / Локальная политика безопасности / Политики учетных записей / Политика блокировки учетной записи / Пороговое значение блокировки». Там же («Политики учетных записей») можно настроить срок блокировки учетной записи, минимальную длину пароля, сроки его действия и т.п.;
- управление сроком действия паролей, их периодическая смена, использование сеансовых ключей;
- удаление паролей уволенных или лишенных полномочий пользователей.

Напомним, что хеш-функция – легко вычислимая функция, преобразующая исходное сообщения произвольной длины (прообраз) в сообщение фиксированное длины (хеш-образ), для которой не существует эффективного алгоритма поиска коллизий.

При идентификации/аутентификации пользователь вводит пароль, а по каналу связи высылается его хеш-образ. Проверяющая система сравнивает введенный хеш-образ с образом, хранящемся в ИС для этого пользователя и в случае их совпадения разрешает доступ. Т.о. система не хранит паролей, что повышает ее защищенность (достоинство).

Недостаток приведенной схемы заключается в том, что все равно необходимо как-то передавать хеш-образ для хранения в системе или для аутентификации и на этом пути его может перехватить злоумышленник, а затем воспользоваться им/

Широкое распространение при идентификации и аутентификации получили протоколы на базе асимметричного шифрования. Существует десятки разновидностей таких протоколов, наиболее известными из которых являются протоколы на основе алгоритмов RSA, схемы Фейге-Фиата-Шамира, Эль-Гамаля, Шнорра и т.д.

Протокол на основе алгоритма RSA.

Этап 1. Генерация ключей.

1. А генерирует открытый и закрытый ключи ((e=5, n=91) и d=29).
2. А передает открытый ключ Б.

Этап 2. Аутентификация.

Таблица 13.1. Аутентификация на основе алгоритма RSA

№ п/п	Описание операции	Пример
1	Б выбирает случайное число $k \in \{1, \ldots, n-1\}$, вычисляет $r = k^e \bmod n$ и посылает r А.	$k = 23$ $r = 235 \bmod 91 = 4$
2	А вычисляет $k' = r^d \bmod n$ и посылает k’ Б.	$k' = 429 \bmod 91 = 23$
3	Б проверяет соотношение $k = k'$ и, если оно истинно, принимает доказательство, в противном случае - отвергает.	$k = 23$ $k' = 23$

Схема Клауса Шнорра.

Этап 1. Генерация ключей (выполняет А).
Таблица 13.2. Генерация ключей по схеме Клауса Шнорра
№ п/п Описание операции Пример
1 Выбираются два простых числа p и q такие, что (p - 1) mod q = 0. p = 23, q = 11
2 Выбирается секретный ключ x ∈ {1, …, q-1}. x = 8
3 Выбирается g такое, что gq mod p = 1. g=3
311 mod 23 = 1
4 Вычисляется открытый ключ y такой, что (gx * y) mod p = 1. y = 4
(38 * 4) mod 23 = 26244 mod 23 = 1
5 Публикация открытого ключа y.
Этап 2. Аутентификация.
Таблица 13.3. Аутентификация по схеме Клауса Шнорра
№ п/п Описание операции Пример
1 А выбирает случайное число k ∈ {1, …, q-1}, вычисляет r = gk mod p и посылает r Б. k = 6
r = 36 mod 23 = 16
2 Б выбирает случайное число e ∈ {0, …, 2t-1}, где t - некоторый параметр, и посылает e А. e = 4
3 А вычисляет s = (k + x * e) mod q и посылает s Б. s = (6 + 8 * 4) mod 11 = 5
4 Б проверяет соотношение r = (gs * ye) mod p и, если оно выполняется, принимает доказательство, в противном случае - отвергает. 16 = (35 * 44) mod 23
Для обеспечения стойкости протокола в 1989 г. Шнорр рекомендовал использовать p длиной 512 бит, q длиной 140 бит и t = 52.
Схема на основе протокола с нулевым разглашением.
Суть доказательства с нулевым разглашением очень популярно можно объяснить на примере «пещеры Аладдина» (авторы - Жан-Жак Кискатер и Луи Гийу).

Рис.13.1. Пещера Аладдина
В пещере имеется потайная дверь C-D, открыть которую может только тот, кто знает волшебные слова. Алиса хочет доказать Бобу, что знает волшебные слова, но не хочет их раскрыть Бобу. Тогда Алиса может убедить Боба следующим образом.
1. Боб стоит в точке A.
2. Алиса проходит к точке C или D.
3. Боб проходит к точке B и предлагает Алисе появиться с левого прохода или с правого.
4. Алиса выполняет просьбу, используя, если необходимо, волшебные слова.
5. Алиса и Боб n раз повторяют шаги 1-4.
Если Алиса не знает секрета, то вероятность правильно выйти у нее в каждом раунде 50%:50%. Если шаги повторить t раз, то вероятность правильного выхода во всех случаях 1 шанс на 2t. Например, при t=16 у Алисы всего 1 шанс из 65536.
Практическая реализация протокола рассматривается на примере схемы аутентификации Фейге-Фиата-Шамира.
Упрощенная схема аутентификации Фейге-Фиата-Шамира.
Этап 1. Генерация ключей (выполняет Посредник).
Таблица 13.4. Генерация ключей по схеме Фейге-Фиата-Шамира
№ п/п Описание операции Пример
1 Выбирает модуль n, равный произведению двух простых чисел. p = 5, q = 7, n = 35
2 Выбирает число v (открытый ключ), являющееся квадратичным вычетом по модулю n и имеется обратное значение v-1 по модулю n.
Квадратный вычет – число, удовлетворяющее выражению x2 mod n = v, где $1 \le x \le n$. Для модуля n = 35, квадратными вычетами являются 1 (x = 1, 6, 29, 34), 4, 9, 11, 14, 15, 16, 21, 25, 29, 30.
Обратное значение вычисляется по формуле (v * v-1) mod n = 1.
У квадратных вычетов 14, 15, 21, 25 и 30 нет обратных значений по модулю.
Таким образом, v ∈ {1, 4, 9, 11, 16, 29}. v = 16
v-1 = 11
(16 * 11) mod 35 = 176 mod 35 = 1
3 Определяет закрытый ключ s, как наименьшее значение, удовлетворяющее следующему выражению s2 mod n = v-1. s = 9
92 mod 35 = 11
4 Публикация открытого ключа – v и n.
Передача закрытого ключа s A.
Этап 2. Аутентификация.
Таблица 13.5. Аутентификация по схеме Фейге-Фиата-Шамира
№ п/п Описание операции Пример
1 А выбирает случайное число r ∈ {1, …, n-1}, вычисляет z = r2 mod n и посылает z Б. r = 8
z = 82 mod 35 = 29
2 Б посылает А случайный бит b. b = 0 b = 1

3 Если b=0, то А посылает Б r, иначе - y = (r * s) mod n. r = 8 y = (8 * 9) mod 35 = 2
4 Если b=0, то Б проверяет, что z = r2 mod n, иначе - z = (y2 * v) mod n. 29 = 82 mod 35 29 = (22 * 16) mod 35
Рассмотренный порядок операций, выполненный 1 раз называется аккредитацией. Если первую операцию поменять местами со второй, то А, даже не зная закрытого ключа s, может подобрать такое значение r, которое будет приводить к успешной аккредитации в обоих случаях (b=0 и b=1). Подобрать же такое r, которое будет приводить к успешной аккредитации в обоих случаях одновременно невозможно. Таким образом, если А не знает закрытого ключа s, то вероятность успешной аккредитации (подбора r) равна 1/2. Аккредитация повторятся t раз, пока не будет достигнута требуемая вероятность 1/2t, что А не знает закрытого ключа s.

Контрольные вопросы:

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинтства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

ПРАКТИЧЕСКАЯ РАБОТА: «РОЛЕВАЯ МАТРИЦА ДОСТУПА»

Цель: ознакомиться с моделями управления доступом, научиться составлять матрицу доступа и иерархию ролей для учреждения профессионального учреждения для целей реализации политики безопасности, получить опыт принятия мотивированного решения.

Методы и приемы: изучение теоретических источников, контент-анализ сайтов образовательных учреждений, моделирование (политики безопасности), структурное программирование, кейс-метод.

Ключевые слова: политика безопасности, матрица доступа, ролевое управление доступом, мандатное управление доступом, объектно-ориентированный подход в ролевом управлении доступом, наследование ролей, инкапсуляция ролей

Краткие теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.

Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное (дискреционное, избирательное) управление доступом; мандатное (полномочное) управление доступом.

Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту.

На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту.

Матрица доступа является самым простым подходом к моделированию систем управления доступом. С ростом организации, увеличивается опасность хищения информации, в том числе сотрудниками, возрастают финансовые и репутационные риски, это приводит к ужесточению политик и систем контроля. Любые избыточные права доступа сотрудников ведут к увеличению риска утечки информации, в связи с чем, происходит ужесточение политики ИБ, так как увеличиваются риски утечки информации.

Избирательная политика безопасности широко применяется в автоматизированных системах коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя [5]. Полномочное управление доступом подразумевает, что:

1) все субъекты и объекты системы однозначно идентифицированы;
2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.
Чем важнее объект, тем выше его метка конфиденциальности, поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.
Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.
При выборе и реализации политики безопасности в автоматизированной системе проводится анализ угроз и рисков для информации и информационного обмена и определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей. Фрагмент матрицы доступа представлен в таблице 3.
Таблица 3 Пример матрицы доступа
Объект /
Субъект Файл_1 Файл_2 CD-RW Дисковод
Администратор Полные права Полные права Полные права Полные права
Гость Запрет Чтение Чтение Запрет
Пользователь_1 Чтение, передача прав Чтение, запись Полные права Запрет

Ролевое управление доступом
При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования, так как число связей в них пропорционально произведению количества пользователей на количество объектов, и тогда в этом случае принимаются решения в объектно-ориентированном стиле, способные эту сложность понизить. Таким решением является ролевое управление доступом.
Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 6).Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно. Ролевое управление доступом оперирует следующими основными понятиями: пользователь (человек, интеллектуальный автономный агент и т.п.); сеанс работы пользователя; роль (обычно определяется в соответствии с организационной структурой); объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД); операция (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными); право доступа (разрешение выполнять определенные операции над определенными объектами).

Рисунок 6. Схема ролевого управления доступом
Ролям приписываются пользователи и права доступа, то есть реализуется отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса раб0оты пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов. Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1.
Очевидно, что наследование ролей соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов. Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).
Можно представить формирование иерархии ролей, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), до роли "руководитель".
При формировании иерархии ролей учитывается принципом минимизации привилегий, то есть каждой роли разрешено только то, что необходимо для выполнения служебных обязанностей.
Порядок выполнение работы:
1. Изучить теоретические сведения
2. Найти сайт образовательного учреждения

3. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения.
4. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий.
5. Ответить на контрольные вопросы. Оформить отчет.

Контрольные вопросы

1. Что понимается под политикой безопасности?
2. В чем заключается модель дискреционной политики безопасности?
3. В чем заключается модель мандатной политики безопасности?
4. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
5. Как соотносятся матрица доступа и ролевой доступ?
6. В каких случаях целесообразно использовать ролевой доступ?
7. В чем состоит принцип минимизации привилегий?

Содержание отчета: Тема, цель, матрица доступа учреждения, ролевой доступ, ответы на контрольные вопросы.

Информационные источники:

1. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: http://citforum.ru/security/articles/galatenko/- (дата обращения -01.03.2017)
2. https://www.anti-malware.ru/node/13626#part4

Раздел 2. Протоколирование и аудит. Анализ защищенности. Экранирование. Шифрование.

Лабораторная работа : Назначение прав пользователей при произвольном управлении доступом в ОС Windows XP

Цель работы: Научиться создавать учетные записи пользователей, локальных групп, блокировать учетные записи пользователей и.т.д.

Краткие теоретические сведения:

После выполнения аутентификации идентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы. Обычно полномочия субъектов представляются списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Задание: Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись.

Алгоритм выполнения работы:

А. Создание учетной записи.

1. Откройте оснастку Настройка– Панель управления – Администрирование(рис. 1)– Управление компьютером(рис. 2).

2. В оснастке Локальные пользователи и группы установите указатель мыши на папку Пользователи и нажмите правую кнопку.
3. В появившемся контекстном меню выберите команду Новый пользователь(рис. 3). Появиться окно диалога Новый пользователь (рис. 4).

4. В поле Пользователь введите имя создаваемого пользователя, например, свою фамилию.

Примечание: Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:*[];:=.,<>? Имя пользователя не может состоять целиком из точек и пробелов.
5. В поле Полное имя введите полное имя создаваемого пользователя.
6. В поле Описаниевведите описание создаваемого пользователя или учетной записи, например, «студент ……».
7. В поле Парольвведите пароль пользователя и в поле Подтверждениеподтвердите его правильность вторичным вводом.
Примечание: Длина пароля не может превышать 14 символов.
8. Установите или снимите флажки:
· Потребовать смену пароля при следующем входе в систему
· Запретить смену пароля пользователем
· Срок действия пароля не ограничен
· Отключить учетную запись
9. Чтобы создать ещё одного пользователя, нажмите кнопку Создать и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку Создать и затем Закрыть.
B. Создание локальной группы.
1. В окне оснастки Локальные пользователи и группы установите указатель мыши на папке Группы и нажмите правую кнопку.
2. В появившемся контекстном меню выберите команду Новая группа.
3. В поле Имя группы (рис. 5) введите имя новой группы, например, Студенты.
Примечание:Имя локальной группы должно быть уникальным. Оно сможет содержать до 256 символов в верхнем и нижнем регистрах.
4. В поле Описание введите описание новой группы.
5. В поле Члены группы можно сразу добавить пользователей и группы, которые войдут в новую группу: для этого нужно нажать кнопку Добавить и выбрать их в списке. Для завершения нажмите кнопку Создать и затем Закрыть.

C. Изменение членства в локальной группе.
1. В окне оснастки Локальные пользователи и группы щелкните на папке Группы.
2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.
3. В появившемся контекстном меню выберите команду Добавить в группу или Свойства.
4. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку Добавить(рис. 6)

5. Далее следуйте указателям окна диалогаВыбор: Пользователи или группы.
6. Для того, чтобы удалить из группы некоторых пользователей, в поле Члены группы(рис. 6) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку Удалить.
Примечание: В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и локальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в неё пользователей.
D. Временная блокировка учетной записи.
1. Откройте оснастку Управление компьютером.
2. Для этого либо выберите на Рабочем столе ярлык Мой компьютер и нажмите правую кнопку мыши, после этого выберите пункт контекстного меню Управление, либо воспользуйтесь разделом Администрирование в Панели управления.
3. В открывшейся оснастке выберите пункты Служебные программы/Локальные пользователи и группы (рис. 3).
4. Откройте папку пользователи и выберите учетную запись Гость.
5. Нажмите правую кнопку мыши и выберите пункт свойства.
6. В открывшемся окне снимите отметку пункта Отключить учетную запись (рис. 7).
7. Нажмите кнопку ОК и сделайте вывод о состоянии учетной записи.
8. Выполните пункт 5 и отметьте пункт Отключить учетную запись.

Задание для самостоятельной работы:
1. Создайте учетную запись с именем ПЗ-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера(для чего после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.
2. Создайте группу Информационная безопасность и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.
3. Заблокируйте учетную запись ПЗ-6 и после этого удалитею
Контрольные вопросы:

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя П38/44? Почему?

Задания для оценки владений

1. Отчет по лабораторной работе:

Лабораторная работа: Установка паролей в документы MSWord и MS Excel.

Цель: научиться ставить пароли на документы в MSWord и MS Excel.

Теоретические сведения

В документах MS Office предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным и их изменением.

Просмотр документов MS Word, книг MS Excel и баз данных MS Access может быть ограничен с помощью парольной защиты (пароль для открытия файла). При установке пароля на открытие документа содержимое файла шифруется (алгоритм шифрования AES).

Для документов MS Word и MS Excel также имеется возможность установки парольной защиты на сохранение внесенных изменений (пароль разрешения записи). Если пользователю не известен пароль разрешения записи, он может открыть документ в режиме «только для чтения». В этом случае возможно внесение изменений в текст документа, однако нельзя сохранить измененный файл документа под старым именем. Для сохранения изменений требуется ввести новое имя файла.

Пароль на открытие, пароль разрешения записи устанав-лива-ются на файл, то есть относятся к документу/книге в целом.

Кроме паролей на файл в целом, имеются возможности защиты отдельных элементов документов MS Office:

Парольная защита от просмотра элементов книги Excel (строк, столбцов, листов). Невозможно защитить от просмотра часть документа MS Word, отдельные ячейки книги MS Excel;

Парольная защита от изменения частей (разделов) документа Word, содержимого отдельных ячеек и их диапазонов в Excel, структуры листа (вставка, удаление и форматирование строк и столбцов),структуры книги (добавление и удаление листов, отображение, скрытые листов), изменение размеров, положения или видимости окна, настроенного для отображения книги Excel.

Разграничение доступа (возможность изменения) к диапазонам ячеек Excel для локальных и сетевых пользователей ОС Windows;

Разграничение доступа аутентифи-ци-ро-ванн-ных пользователей к фрагментам текста MS Word, задан ограничений на несанкционированное распространение документа (пересылка по электронной почте, изменение, копирование) требует установки дополнительного программного обеспечения (сервера аутентификации, WRM – клиента управления правами Windows).

Следует учитывать, что функциональные возможности парольной защиты на отдельные элементы MS Excel (скрытие данных и защита листов и книг) и MS Word (защита разделов) не предназначены для защиты данных или важных сведений в документах MS Office.

Они используются для более понятного представления сведений, скрывая сведения или формулы, которые могут сбить с толку некоторых пользователей. Эти средства служат также для предотвращения случайного изменения данных пользователями. Скрытые или защищенные паролем данные внутри документов MS Office не шифруются. При определенных усилиях и наличии времени пользователи смогут просмотреть и изменить все сведения внутри документа MS Office, если они имеют доступ к самому документу (пароль на открытие документа не установлен или известен).

Чтобы предотвратить изменение данных и обеспечить безопасность важных сведений, следует ограничить доступ к файлам (пароль на открытие файла), содержащим подобные сведения, сохранив их в расположениях, доступных только пользователям, прошедшим аутентификацию (разграничение доступа к файлам и папкам средствами ОС).

В документах MS Office имеется возможность заверять цифровой подписью как документ в целом, так и внедренный в документ код макросов на языке VBA. Наличие действительной цифровой подписи гарантирует целостность (неизменность) содержимого, а также аутентичность и неотрекаемость (подлинность авторства и невозможность отказа от авторства).

Полноценная проверка подлинности цифровых подписей возможна в том случае, если они выданы сетевым сервером аутентификации (в домене локальной сети), либо доверенным центром сертификации в Интернете. Если же используется локальный сертификат, создаваемый самим пользователем с помощью утилиты selfcert.exe (Digital Certificate for VBA Projects, Цифровой сертификат для проектов VBA), то проверить на другом компьютере подлинность подписи, созданной с его помощью, будет невозможно. Кроме того, другие пользователи локального компьютера также не будут доверять такой подписи.

Один из самых простых, но в то же время надежных способов защиты своих документов – это установить пароль на документ Microsoft Word. Человек, не знающий пароля, попросту не сможет этот документ открыть. Есть несколько способов установить пароль. Один из них – это использование стандартных средств Microsoft Office. Причем можно установить пароль как и на открытие документа MS Word, так и на изменение содержимого документа.
Для того чтобы установить пароль для своего документа Microsoft Word, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 6).

Рисунок 6 – Меню Сервис MS Word
После выполнения всех действий появится окно Microsoft Word – Параметры. В этом окне Microsoft Word - Параметры нужно перейти на закладку Безопасность (см. рисунок 7); далее в строке «пароль для открытия файла» ввести пароль. После ввода пароля нажмите кнопку ОК.
Рисунок 7 – Меню Безопасность MS Word
Для безопасности документа Microsoft Excel можно установить свой пароль на открытие документа. После того как вы установили пароль на открытие документа Microsoft Excel, Excel будет требовать пароль на открытие вашего документа.
Для того чтобы установить пароль для своего документа Microsoft Excel, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 8).

Рисунок 8 – Меню Сервис MS Excel
В этом окне Microsoft Excel – Параметры нужно перейти на закладку Безопасность(см. рисунок 9) далее в строке «пароль для открытия» ввести пароль. После ввода пароля нажмите кнопку ОК.

Рисунок 9 – Меню Безопасность MS Excel

После нажатия кнопки ОК появится окошко Microsoft Excel – «Подтверждения пароля», здесь вам нужно будет еще раз ввести пароль, который вы вводили, и нажать кнопку ОК (см. рисунок10).

Рисунок 10 – Меню Подтверждение пароля MS Excel
При установке пароля стоит помнить об очень важных моментах. Пароль можно «сломать». Для этого есть немало программ. Особенно легко «взламывать» короткие пароли. Поэтому желательно чтобы пароль был сложный. Лучше всего, чтобы пароль состоял как из латиницы, так и из кириллицы. Для надежности можно добавить еще несколько цифр. Желательно использовать пароль минимум из семи символов. Чем сложнее пароль, тем меньше шансов, что он будет «взломан». Но также не нужно слишком усердствовать, так как можно этот пароль забыть и самому. А еще лучше пароль записать и хранить в надежном месте, на случай если вы его забудете. Также для дополнительной защиты можно заархивировать документ и установить пароль к архиву. Тогда вероятность того, что кому-либо удастся сломать защиту, становится крайне низкой.
Чтобы установить пароль для защиты базы данных MS Access:
- закройте базу данных. Если база данных совместно используется в сети, убедитесь, что остальные пользователи ее закрыли;
- сделайте резервную копию базы данных и сохраните ее в надежном месте;
- в меню MS Access выберите команду Файл/Открыть;
- выделите файл базы данных;
- щелкните по стрелке, расположенной справа от кнопки Открыть . В раскрывающемся списке режимов открытия базы данных выделите элемент Монопольно. База данных откроется в режиме монопольного доступа;
- выберите команду Сервис/Защита/Задать пароль базы данных (см. рисунок11);

Рисунок 11 – Меню Задание пароля базы данных MS Access
- в появившемся диалоговом окне введите в поле Пароль пароль для защиты базы данных с учетом регистра символов;
- введите пароль еще раз в поле Подтверждение;
- нажмите кнопку ОК.
Теперь база данных защищена паролем, и всякий раз, когда пользователь будет открывать базу данных, будет отображаться диалоговое окно с требованием ввести пароль. Запомните или сохраните пароль в надежном месте. Если вы забудете пароль, базу данных будет невозможно открыть.
Контрольные вопросы:
1. Чем различается действие защиты от изменения текста документа, установленной с помощью защиты форм (команда Защитить документ) и защиты в режиме «только для чтения» (установка на файл пароля разрешения записи)?
2. Чем различается действие защиты от изменения в случае задания пароля разрешения записи и в случае рекомендации открытия документа в режиме «только для чтения»?
Задание для самостоятельного выполнения:

В приложении MS Word создайте короткий опросник (анкету) с защищенным от изменения текстом вопросов для получения от пользователей различных данных. Сформулировать вопросы так, чтобы требовались:
ответы в произвольной форме, подразумевающие ввод текста, (например, ФИО, какие-либо комментарии или пожелания, номер учебной группы, дата заполнения),
выбор даты (дата дня рождения, начала сессии, рекомендуемая дата мероприятия или посещения и т.п.),

выбор единственного варианта ответа из списка и с помощью переключателей (например, пол, возрастная группа, форма обучения, специальность),
выбор нескольких вариантов с помощью флажков (например, знания, предпочтения, сферы интересов, участие в мероприятиях и т.п.)
Для вставки в документ флажков и переключателей используйте инструменты из предыдущих версий Word – кнопка на вкладке Разработчик..
Описание формы отчета
Выполненное задание для самостоятельной работы и ответы на контрольные вопросы необходимо выслать для проверки преподавателю.

ЛАБОРАТОРНАЯ РАБОТА: ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ (RSA, СХЕМЫ ШНОРРА И ФЕЙГЕ-ФИАТА-ШАМИРА)
Цель: В лабораторной работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:
- на основе алгоритма RSA;
- по схеме Шнорра;
- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа (k или r) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

Теоретические сведения

Идентификация (англ. identification) - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов).
Аутентификация (англ. authentication) - проверка соответствия (подлинности) сущности предъявленному ею идентификатору. (Заметим, что происхождение русскоязычного термина «аутентификация» не совсем понятно. Английское «authentication» скорее можно прочитать как «аутентикация»; трудно сказать, откуда в середине взялось еще «фи» – может, из идентификации? Тем не менее, термин устоялся и закреплен в РД Гостехкомиссии РФ).
Для полноты картины приведем определение термина авторизация, который не следует путать с двумя вышеприведенными. Авторизация (англ. authorization) - предоставление сущности возможностей в соответствии с положенными ей правами или проверка наличия прав при попытке выполнить какое-либо действие.
Идентификация и аутентификация – это первая линия обороны, «входная дверь» в информационное пространство организации.
Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.
Идентификация сродни присвоении имени ребенку (не совсем точное сравнение, но все же). В любой ИС должны быть определены все субъекты, участвующие в информационном обмене. Часть из них может быть сгруппирована, если они наделены одинаковыми (схожими) правами и обладают одинаковыми (схожими) характеристиками. Каждый субъект (группа субъектов) должен обладать уникальным именем (обозначением).
Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.
Субъект может подтвердить свою подлинность, предъявив один из следующих аутентификаторов:
- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

- нечто, чем он владеет (паспорт, личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев, образец ДНК и т.п.).

В том случае, если в ходе процедуры аутентификации клиент должен предъявить сразу несколько аутентификаторов, аутентификация называется многофакторной. Например, в ходе двухфакторной аутентификации клиент должен знать пароль и воспользоваться личной карточкой.

Основные программно-технические способы реализации идентификации и аутентификации: пароли, с использованием хеш-функции, на основе шифрования с открытым ключом, идентификационные карты и электронные ключи, сервер аутентификации Kerberos/

Введенный пользователем пароль сравнивается с паролем, имеющимся в БД, хранящейся в защищаемой ИС, и если они совпадают, то дается разрешение на использование защищаемых ресурсов.

Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в ОС, СУБД и программные продукты. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Парольная аутентификация имеет массу недостатков:

- как правило, пароль генерируется в одном месте (например, на сервере) и должен быть передан во второе (например, клиенту). При передаче пароль может быть перехвачен злоумышленником;
- многие ОС и приложения имеют пароли, указанные производителем по умолчанию. После установки такой системы очень часто забывают их удалить. БД стандартных паролей можно найти в Интернете;
- злоумышленник может получить БД паролей, хранящихся в зашифрованном виде, и воспользоваться ей:
- в Windows NT/2000/XP учетные записи (пользователи и пароли) хранятся в файле «%System Root% \ System32 \ Config \ sam». При работающем ОС пользователь не может выполнять операции чтения/записи с данным файлом (блокируется процессом lsass.exe, «убить» который невозможно). Получить доступ к файлу можно, загрузив ОС с другого носителя. Другой вариант заключается в использовании файла «%System Root% \ Repair \ sam». Он доступен для чтения/записи, но, как правило, содержит пароли «столетней» давности;
- в ранних версиях Unix файл с учетными записями «/etc/passwd» был доступен для чтения любым желающим. В современных разновидностях Unix файл с паролями «/etc/shadow» или «etc/secure» доступен только с привилегиями супервизора. Другой способ получения доступа к паролям – обрушения процесса, обращающегося к файлу с паролями. При этом Unix создает файл «core dump», содержащий дамп памяти (с паролями) [26];
- после получения файла с зашифрованными паролями можно воспользоваться многочисленными программами-взломщиками. Одними из самых популярных взломщиков являются: для Windows – L0phtCrack, для Unix – John the Ripper. Время, требуемое для взлома пароля, зависит от его качества. Так, например, взлом пароля для L0phtCrack на компьютере с процессором Xeon 400 МГц при использовании [26]:
- цифр и латиницы – 5,5 часов;
- всех символов – 480 часов.
- кроме перечисленных выше приемов взлома паролей, их можно подсмотреть (например, с помощью оптических приборов), сообщить другу/подруге (если секрет знают двое – это уже не секрет), записать на бумажке и приклеить на клавиатуру или монитор и т.п.

Тем не менее, так как парольная защита используется во многих продуктах и системах, можно порекомендовать следующие меры, позволяющие повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.). Еще лучше воспользоваться программами - генераторами паролей (ключей);
- ограничение доступа к файлу с паролями;
- удаление резервных копий файлов с паролями («%System Root% \ Repair \ sam»);
- использование защищенных протоколов обмена ключами (например, основанные на протоколе обмена ключами Диффи-Хеллмана);
- ограничение числа неудачных попыток входа в систему (это затруднит применение «метода грубой силы»). В Windows 2000 и XP этот параметр устанавливается по пути «Администрирование / Локальная политика безопасности / Политики учетных записей / Политика блокировки учетной записи / Пороговое значение блокировки». Там же («Политики учетных записей») можно настроить срок блокировки учетной записи, минимальную длину пароля, сроки его действия и т.п.;
- управление сроком действия паролей, их периодическая смена, использование сеансовых ключей;
- удаление паролей уволенных или лишенных полномочий пользователей.

Напомним, что хеш-функция – легко вычислимая функция, преобразующая исходное сообщения произвольной длины (прообраз) в сообщение фиксированное длины (хеш-образ), для которой не существует эффективного алгоритма поиска коллизий.

При идентификации/аутентификации пользователь вводит пароль, а по каналу связи высылается его хеш-образ. Проверяющая система сравнивает введенный хеш-образ с образом, хранящемся в ИС для этого пользователя и в случае их совпадения разрешает доступ. Т.о. система не хранит паролей, что повышает ее защищенность (достоинство).

Недостаток приведенной схемы заключается в том, что все равно необходимо как-то передавать хеш-образ для хранения в системе или для аутентификации и на этом пути его может перехватить злоумышленник, а затем воспользоваться им/

Широкое распространение при идентификации и аутентификации получили протоколы на базе асимметричного шифрования. Существует десятки разновидностей таких протоколов, наиболее известными из которых являются протоколы на основе алгоритмов RSA, схемы Фейге-Фиата-Шамира, Эль-Гамаля, Шнорра и т.д.

Протокол на основе алгоритма RSA.

Этап 1. Генерация ключей.

1. А генерирует открытый и закрытый ключи ((e=5, n=91) и d=29).
2. А передает открытый ключ Б.

Этап 2. Аутентификация.

Таблица 13.1. Аутентификация на основе алгоритма RSA

№ п/п	Описание операции	Пример
1	Б выбирает случайное число k ∈ {1, …, n-1}, вычисляет r = ke mod n и посылает r А.	k = 23 r = 235 mod 91 = 4
2	А вычисляет k’ = rd mod n и посылает k’ Б.	k’ = 429 mod 91 = 23
3	Б проверяет соотношение k = k’ и, если оно истинно, принимает доказательство, в противном случае - отвергает.	k = 23 k’ = 23

Схема Клауса Шнорра.

Этап 1. Генерация ключей (выполняет А).

Таблица 13.2. Генерация ключей по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	Выбираются два простых числа p и q такие, что (p - 1) mod q = 0.	p = 23, q = 11
2	Выбирается секретный ключ x ∈ {1, …, q-1}.	x = 8
3	Выбирается g такое, что gq mod p = 1.	g=3 311 mod 23 = 1
4	Вычисляется открытый ключ y такой, что (gx * y) mod p = 1.	y = 4 (38 * 4) mod 23 = 26244 mod 23 = 1
5	Публикация открытого ключа y.	

Этап 2. Аутентификация.

Таблица 13.3. Аутентификация по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	А выбирает случайное число k ∈ {1, …, q-1}, вычисляет r = gk mod p и посылает r Б.	k = 6 r = 36 mod 23 = 16
2	Б выбирает случайное число e ∈ {0, …, 2t-1}, где t - некоторый параметр, и посылает e А.	e = 4
3	А вычисляет s = (k + x * e) mod q и посылает s Б.	s = (6 + 8 * 4) mod 11 = 5
4	Б проверяет соотношение r = (gs * ye) mod p и, если оно выполняется, принимает доказательство, в противном случае - отвергает.	16 = (35 * 44) mod 23

Для обеспечения стойкости протокола в 1989 г. Шнорр рекомендовал использовать p длиной 512 бит, q длиной 140 бит и t = 52.

Схема на основе протокола с нулевым разглашением.

Суть доказательства с нулевым разглашением очень популярно можно объяснить на примере «пещеры Аладдина» (авторы - Жан-Жак Кискатер и Луи Гийу).

Рис.13.1. Пещера Аладдина

В пещере имеется потайная дверь C-D, открыть которую может только тот, кто знает волшебные слова. Алиса хочет доказать Бобу, что знает волшебные слова, но не хочет их раскрыть Бобу. Тогда Алиса может убедить Боба следующим образом.

1. Боб стоит в точке А.
2. Алиса проходит к точке С или D.
3. Боб проходит к точке В и предлагает Алисе появиться с левого прохода или с правого.
4. Алиса выполняет просьбу, используя, если необходимо, волшебные слова.
5. Алиса и Боб n раз повторяют шаги 1-4.

Если Алиса не знает секрета, то вероятность правильно выйти у нее в каждом раунде 50%:50%. Если шаги повторить t раз, то вероятность правильного выхода во всех случаях 1 шанс на 2t. Например, при t=16 у Алисы всего 1 шанс из 65536.

Практическая реализация протокола рассматривается на примере схемы аутентификации Фейге-Фиата-Шамира.

Упрощенная схема аутентификации Фейге-Фиата-Шамира.

Этап 1. Генерация ключей (выполняет Посредник).

Таблица 13.4. Генерация ключей по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример

1 Выбирает модуль n, равный произведению двух простых чисел. p = 5, q = 7, n = 35
2 Выбирает число v (открытый ключ), являющееся квадратичным вычетом по модулю n и имеется обратное значение v-1 по модулю n.
Квадратный вычет – число, удовлетворяющее выражению x2 mod n = v, где $1 \leq x \leq n$. Для модуля n = 35, квадратными вычетами являются 1 (x = 1, 6, 29, 34), 4, 9, 11, 14, 15, 16, 21, 25, 29, 30.
Обратное значение вычисляется по формуле (v * v-1) mod n = 1.
У квадратных вычетов 14, 15, 21, 25 и 30 нет обратных значений по модулю.
Таким образом, $v \in \{1, 4, 9, 11, 16, 29\}$. v = 16
v-1 = 11
(16 * 11) mod 35 = 176 mod 35 = 1
3 Определяет закрытый ключ s, как наименьшее значение, удовлетворяющее следующему выражению s2 mod n = v-1. s = 9
92 mod 35 = 11
4 Публикация открытого ключа – v и n.
Передача закрытого ключа s A.
Этап 2. Аутентификация.
Таблица 13.5. Аутентификация по схеме Фейге-Фиата-Шамира
№ п/п Описание операции Пример
1 А выбирает случайное число $r \in \{1, \ldots, n-1\}$, вычисляет z = r2 mod n и посылает z Б. r = 8
z = 82 mod 35 = 29
2 Б посылает А случайный бит b. b = 0 b = 1
3 Если b=0, то А посылает Б r, иначе - y = (r * s) mod n. r = 8 y = (8 * 9) mod 35 = 2
4 Если b=0, то Б проверяет, что z = r2 mod n, иначе - z = (y2 * v) mod n. 29 = 82 mod 35 29 = (22 * 16) mod 35
Рассмотренный порядок операций, выполненный 1 раз называется аккредитацией. Если первую операцию поменять местами со второй, то А, даже не зная закрытого ключа s, может подобрать такое значение r, которое будет приводить к успешной аккредитации в обоих случаях (b=0 и b=1). Подобрать же такое r, которое будет приводить к успешной аккредитации в обоих случаях одновременно невозможно. Таким образом, если А не знает закрытого ключа s, то вероятность успешной аккредитации (подбора r) равна 1/2. Аккредитация повторятся t раз, пока не будет достигнута требуемая вероятность 1/2t, что А не знает закрытого ключа s.

Контрольные вопросы:

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинтства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

ПРАКТИЧЕСКАЯ РАБОТА: «РОЛЕВАЯ МАТРИЦА ДОСТУПА»

Цель: ознакомиться с моделями управления доступом, научиться составлять матрицу доступа и иерархию ролей для учреждения профессионального учреждения для целей реализации политики безопасности, получить опыт принятия мотивированного решения.
Методы и приемы: изучение теоретических источников, контент-анализ сайтов образовательных учреждений, моделирование (политики безопасности), структурное программирование, кейс-метод.
Ключевые слова: политика безопасности, матрица доступа, ролевое управление доступом, мандатное управление доступом, объектно-ориентированный подход в ролевом управлении доступом, наследование ролей, инкапсуляция ролей
Краткие теоретические сведения
Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.
Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.
Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.
Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.
В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное (дискреционное, избирательное) управление доступом; мандатное (полномочное) управление доступом.

Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.
Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту.
На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту.
Матрица доступа является самым простым подходом к моделированию систем управления доступом. С ростом организации, увеличивается опасность хищения информации, в том числе сотрудниками, возрастают финансовые и репутационные риски, это приводит к ужесточению политик и систем контроля. Любые избыточные права доступа сотрудников ведут к увеличению риска утечки информации, в связи с чем, происходит ужесточение политики ИБ, так как увеличиваются риски утечки информации.
Избирательная политика безопасности широко применяется в автоматизированных системах коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.
Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя [5]. Полномочное управление доступом подразумевает, что:
1) все субъекты и объекты системы однозначно идентифицированы;
2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;
3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.
Чем важнее объект, тем выше его метка конфиденциальности, поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.
Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.
При выборе и реализации политики безопасности в автоматизированной системе проводится анализ угроз и рисков для информации и информационного обмена и определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей. Фрагмент матрицы доступа представлен в таблице 3.
Таблица 3 Пример матрицы доступа

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

Ролевое управление доступом
При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования, так как число связей в них пропорционально произведению количества пользователей на количество объектов, и тогда в этом случае принимаются решения в объектно-ориентированном стиле, способные эту сложность понизить. Таким решением является ролевое управление доступом.
Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 6).Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно. Ролевое управление доступом оперирует следующими основными понятиями: пользователь (человек, интеллектуальный автономный агент и т.п.); сеанс работы пользователя; роль (обычно определяется в соответствии с организационной структурой); объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД); операция (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными); право доступа (разрешение выполнять определенные операции над определенными объектами).

Рисунок 6. Схема ролевого управления доступом

Ролям приписываются пользователи и права доступа, то есть реализуется отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса раб0оты пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов. Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1.

Очевидно, что наследование ролей соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов. Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить формирование иерархии ролей, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), до роли "руководитель".

При формировании иерархии ролей учитывается принципом минимизации привилегий, то есть каждой роли разрешено только то, что необходимо для выполнения служебных обязанностей.

Порядок выполнение работы:

1. Изучить теоретические сведения
2. Найти сайт образовательного учреждения
3. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения.
4. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий.
5. Ответить на контрольные вопросы. Оформить отчет.

Контрольные вопросы

1. Что понимается под политикой безопасности?
2. В чем заключается модель дискреционной политики безопасности?
3. В чем заключается модель мандатной политики безопасности?
4. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
5. Как соотносятся матрица доступа и ролевой доступ?
6. В каких случаях целесообразно использовать ролевой доступ?
7. В чем состоит принцип минимизации привилегий?

Содержание отчета: Тема, цель, матрица доступа учреждения, ролевой доступ, ответы на контрольные вопросы.

Информационные источники:

1. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: http://citforum.ru/security/articles/galatenko/- (дата обращения -01.03.2017)
2. https://www.anti-malware.ru/node/13626#part4

Раздел 2. Протоколирование и аудит. Анализ защищенности. Экранирование. Шифрование.

Лабораторная работа : Назначение прав пользователей при произвольном управлении доступом в ОС Windows XP

Цель работы: Научиться создавать учетные записи пользователей, локальных групп, блокировать учетные записи пользователей и.т.д.

Краткие теоретические сведения:

После выполнения аутентификации идентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы. Обычно полномочия субъектов представляются списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.
При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.
Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.
Задание: Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись.
Алгоритм выполнения работы:
А. Создание учетной записи.
1. Откройте оснастку Настройка– Панель управления – Администрирование(рис. 1)– Управление компьютером(рис. 2).

2. В оснастке Локальные пользователи и группы установите указатель мыши на папку Пользователи и нажмите правую кнопку.
3. В появившемся контекстном меню выберите команду Новый пользователь(рис. 3). Появиться окно диалога Новый пользователь (рис. 4).

4. В поле Пользователь введите имя создаваемого пользователя, например, свою фамилию.
Примечание: Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:*[];:=.,<>? Имя пользователя не может состоять целиком из точек и пробелов.
5. В поле Полное имя введите полное имя создаваемого пользователя.
6. В поле Описаниевведите описание создаваемого пользователя или учетной записи, например, «студент ……».
7. В поле Парольвведите пароль пользователя и в поле Подтверждениеподтвердите его правильность вторичным вводом.
Примечание: Длина пароля не может превышать 14 символов.
8. Установите или снимите флажки:
· Потребовать смену пароля при следующем входе в систему
· Запретить смену пароля пользователем
· Срок действия пароля не ограничен
· Отключить учетную запись
9. Чтобы создать ещё одного пользователя, нажмите кнопку Создать и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку Создать и затем Закрыть.
В. Создание локальной группы.
1. В окне оснастки Локальные пользователи и группы установите указатель мыши на папке Группы и нажмите правую кнопку.
2. В появившемся контекстном меню выберите команду Новая группа.
3. В поле Имя группы (рис. 5) введите имя новой группы, например, Студенты.
Примечание:Имя локальной группы должно быть уникальным. Оно сможет содержать до 256 символов в верхнем и нижнем регистрах.
4. В поле Описание введите описание новой группы.
5. В поле Члены группы можно сразу добавить пользователей и группы, которые войдут в новую группу: для этого нужно нажать кнопку Добавить и выбрать их в списке. Для завершения нажмите кнопку Создать и затем Закрыть.

С. Изменение членства в локальной группе.
1. В окне оснастки Локальные пользователи и группы щелкните на папке Группы.
2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.
3. В появившемся контекстном меню выберите команду Добавить в группу или Свойства.
4. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку Добавить(рис. 6)

5. Далее следуйте указателям окна диалогаВыбор: Пользователи или группы.
6. Для того, чтобы удалить из группы некоторых пользователей, в поле Члены группы(рис. 6) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку Удалить.

Примечание: В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и локальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в неё пользователей.
D. Временная блокировка учетной записи.
1. Откройте оснастку Управление компьютером.
2. Для этого либо выберите на Рабочем столе ярлык Мой компьютер и нажмите правую кнопку мыши, после этого выберите пункт контекстного меню Управление, либо воспользуйтесь разделом Администрирование в Панели управления.
3. В открывшейся оснастке выберите пункты Служебные программы/Локальные пользователи и группы (рис. 3).
4. Откройте папку пользователи и выберите учетную запись Гость.
5. Нажмите правую кнопку мыши и выберите пункт свойства.
6. В открывшемся окне снимите отметку пункта Отключить учетную запись (рис. 7).
7. Нажмите кнопку ОК и сделайте вывод о состоянии учетной записи.
8. Выполните пункт 5 и отметьте пункт Отключить учетную запись.

Задание для самостоятельной работы:
1. Создайте учетную запись с именем ПЗ-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера(для чего после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.
2. Создайте группу Информационная безопасность и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.
3. Заблокируйте учетную запись ПЗ-6 и после этого удалитею
Контрольные вопросы:
1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя П38/44? Почему?

Раздел: . Протоколирование и аудит. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств

Задания для оценки знаний

1. Тест:

15. Выберите все правильные варианты ответов
Отметьте правильные рекомендации по обеспечению безопасной работы на рабочей станции
- Выполнение обновлений операционной системы
- Выполнение обновлений прикладных программ
- Установка антивирусной программы
- Настройка персонального брандмауэра
- Установка пароля на BIOS и экранную заставку
- Шифрование конфиденциальной информации (EFS, PGP ...)
- Установка антивирусной программы и регулярное обновление антивирусных баз
- Работа под учетной записью пользователя с минимальным необходимым уровнем привилегий

16. Выберите правильный вариант ответа
Что является наилучшим методом аутентификации?
- Чем пользователь характеризуется (например, биометрия)
- Что пользователь имеет
- Что пользователь знает
- Другое

17 Выберите правильный вариант ответа
Какое утверждение наиболее справедливо?
- Чем сложнее механизм защиты, тем меньшую безопасность он гарантирует
- Чем сложнее механизм защиты, тем большую безопасность он гарантирует
- Сложность механизм защиты не связана с уровнем гарантируемой им безопасности

18.Выберите правильный вариант ответа
Это код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы. Он обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. О какой вредоносной программе идет речь?
- вирусы

 "черви"
 троянские программы
 "бомбы"

19. Это код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы). Они ориентированы в первую очередь на путешествия по сети.О какой вредоносной программе идет речь?

 вирусы
 "черви"
 троянские программы
 "бомбы"
 "змеи"

20.Примером какой атаки является перехват злоумышленником передаваемых данных с одновременной их модификацией "прозрачно" для обеих участвующих в обмене сторон?

 Прослушивание сети (sniffing)
 Подмена или спуфинг (spoofing)
 Перехват соединения (hijacking)
 Повторная передача (replay)
 Человек в середине (man in the middle)

Задания для оценки умений

Задания для оценки владений

1. Кейс-задачи:

Задача 1: У менеджера компании есть личный электронный ящик, также что она пользуется социальными сетями (Вконтакте, Одноклассники, КрасМама и пр). При этом она закрывает браузер не нажимая кнопку "выход", использует Internet Explorer, имеет 1-2 несложных пароля на все ресурсы, выходит в сеть в основном с рабочего места иногда из дома. Девушка коммуникабельная, активная участница форумов. На сайтах регестрируется под ником ***

Студенты делятся на 2 группы: "Защитники" (Админы) и "Злоумышленники" (Хакеры),

Каждая команда сообразно своим интересам определяет для менеджера:

- Риски по аспектам информационной безопасности: целостность, доступность, конфиденциальность
- Уязвимости
- Угрозы
- Уровень неприемлемого ущерба
- Контрмеры - политику безопасности (для защитников)
- Порядок атак (для злоумышленников)

После обсуждения, студентам сообщается имя девушки и её ник (он виртуальный). Студенты выходят в Интернет, и кто первый успеет (найти почту, поменять пароли, сменить данные, чтоб не нашли другие и пр), тот и победил.

Раздел: Шифрование. Криптография.

Задания для оценки знаний

Задания для оценки умений

1. Кейс-задачи:

Контрольная работа «КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ»
Вариант 2
Кодирование информации

1. Дана кодовая таблица азбуки Морзе

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

2. Закодируйте с помощью азбуки Морзе слова КРИПТОАНАЛИЗ, КЛЮЧ, ШИФР

3. Дана таблица ASCII-кодов
Расшифровать слово при помощи таблицы ASCIIrкодов:
32 2A 78 2B 79 3D 30.

4. Зашифрованная пословица.
Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).
4. Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .
5. Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.
6. Самый колючий зверь в лесу – это 12, 13.
А теперь прочитайте пословицу:
1, 2, 3, 4, 5, 1, 6
7, 8, 9, 10, 11
9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.
,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ!
Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

Шифры замены.

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

Какие сообщения закодированы с помощью этой таблицы?

8. При помощи таблицы Вижинера зашифровать текст «Криптографическая защита». Ключ «Шифр»

9. Шифры перестановки
a) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Криптоанализ
b) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Криптостойкость

10. Аналитические методы шифрования
Зашифровать слово БАР
Ключ-матрица
0 1 2
2 2 1
3 1 -1

A=

Выполнить проверку (расшифровать слово)

Задания для оценки владений

1. Задача:

Контрольная работа «КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ»
Вариант 3
Кодирование информации
1. Дана кодовая таблица азбуки Морзе

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

2. Закодируйте с помощью азбуки Морзе слова КРИПТОГРАФИЯ, ВИРУС, ДЕКОДИРОВАНИЕ

3. Дана таблица ASCII-кодов
Закодировать при помощи таблицы ASCII кодов следующий текст Password. Результат представить в шестнадцатеричной СС

4. Зашифрованная пословица.
Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).
7. Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .
8. Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.
9. Самый колючий зверь в лесу – это 12, 13.
А теперь прочитайте пословицу:
1, 2, 3, 4, 5, 1, 6
7, 8, 9, 10, 11
9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.
,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ!
Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

Шифры замены.

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

Какие сообщения закодированы с помощью этой таблицы?

8. При помощи таблицы Вижинера зашифровать текст «Методы шифрования». Ключ «Шифр»

9. Шифры перестановки
c) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Кодирование
d) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Декодирование

10. Аналитические методы шифрования
Зашифровать слово ГАМ
Ключ – матрица
-1 0 4
0 2 2
3 1 -2

A=

Выполнить проверку (расшифровать слово)

Раздел: Экранирование. Классификация межсетевых экранов.

Задания для оценки знаний

1. Реферат:

Реферат — письменная работа, выполняемая обучающимся в течение длительного срока (от одной недели до месяца).

Реферат (от лат. referrer — докладывать, сообщать) — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу.

Реферат отвечает на вопрос — что содержится в данной публикации (публикациях).

Однако реферат — не механический пересказ работы, а изложение ее существа.

В настоящее время, помимо реферирования прочитанной литературы, от обучающегося требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата может предложить преподаватель или сам обучающийся, в последнем случае она должна быть согласованна с преподавателем.

В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания.

Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.

Структура реферата:

1. Титульный лист.
2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы.
4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифрой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал.
5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении.
6. Приложение может включать графики, таблицы, расчеты.
7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания.

Этапы работы над рефератом.

Работу над рефератом можно условно подразделить на три этапа:

1. Подготовительный этап, включающий изучение предмета исследования;
2. Изложение результатов изучения в виде связного текста;
3. Устное сообщение по теме реферата.

1. Подготовительный этап работы.

Формулировка темы. Подготовительная работа над рефератом начинается с формулировки темы. Тема в концентрированном виде выражает содержание будущего текста, фиксируя как предмет исследования, так и его ожидаемый результат. Для того чтобы работа над рефератом была успешной, необходимо, чтобы тема заключала в себе проблему, скрытый вопрос (даже если наука уже давно дала ответ на этот вопрос, студент, только знакомящийся с соответствующей областью знаний, будет вынужден искать ответ заново, что даст толчок к развитию проблемного, исследовательского мышления).

Поиск источников. Грамотно сформулированная тема зафиксировала предмет изучения; задача обучающегося — найти информацию, относящуюся к данному предмету и разрешить поставленную проблему. Выполнение этой задачи начинается с поиска источников. На этом этапе необходимо вспомнить, как работать с энциклопедиями и энциклопедическими словарями (обращать особое внимание на список литературы, приведенный в конце тематической статьи); как работать с систематическими и алфавитными каталогами библиотек; как оформлять список литературы (выписывая выходные данные книги и отмечая библиотечный шифр).

Работа с источниками. Работу с источниками надо начинать с ознакомительного чтения, т. е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции — это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Создание конспектов для написания реферата.

Подготовительный этап работы завершается созданием конспектов, фиксирующих основные тезисы и аргументы. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы).

По завершении предварительного этапа можно переходить непосредственно к созданию текста реферата.

2. Создание текста.

Общие требования к тексту.

Текст реферата должен подчиняться определенным требованиям: он должен раскрывать тему, обладать связностью и цельностью.

Раскрытие темы предполагает, что в тексте реферата излагается относящийся к теме материал и предлагаются пути решения содержащейся в теме проблемы; связность текста предполагает смысловую соотносительность отдельных компонентов, а цельность - смысловую законченность текста.

С точки зрения связности все тексты делятся на тексты-констатации и тексты-рассуждения. Тексты-констатации содержат результаты ознакомления с предметом и фиксируют устойчивые и несомненные суждения. В текстах-рассуждениях одни мысли извлекаются из других, некоторые ставятся под сомнение, дается им оценка, выдвигаются различные предположения.

План реферата.

Универсальный план реферата – введение, основной текст и заключение.

Требования к введению.

Во введении аргументируется актуальность исследования, -

т. е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками; перечисляются положения, которые должны быть обоснованы. Введение может также содержать обзор источников или экспериментальных данных, уточнение исходных понятий и терминов, сведения о методах исследования. Во введении обязательно формулируются цель и задачи реферата.

Объем введения - в среднем около 10% от общего объема реферата.

Основная часть реферата.

Основная часть реферата раскрывает содержание темы. Она наиболее значительна по объему, наиболее значима и ответственна. В ней обосновываются основные тезисы реферата, приводятся развернутые аргументы, предполагаются гипотезы, касающиеся существа обсуждаемого вопроса. Важно проследить, чтобы основная часть не имела форму монолога. Аргументируя собственную позицию, можно и должно анализировать и оценивать позиции различных исследователей, с чем-то соглашаться, чему-то возражать, кого-то опровергать. Текст основной части делится на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала: классификации (эмпирические исследования), типологии (теоретические исследования), периодизации (исторические исследования).

Заключение.

Заключение — последняя часть научного текста. В ней краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования. Здесь же могут намечаться и дальнейшие перспективы развития темы. Небольшое по объему сообщение также не может обойтись без заключительной части - пусть это будут две-три фразы. Но в них должен подводиться итог проделанной работы.

Список использованной литературы.

Реферат любого уровня сложности обязательно сопровождается списком используемой литературы. Названия книг в списке располагают по алфавиту с указанием выходных данных использованных книг.

Требования, предъявляемыек оформлению реферата

Объемы рефератов колеблются от 10-18 машинописных страниц. Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 35 мм.слева и 15 мм. справа, рекомендуется шрифт 12-14, интервал - 1,5. Все листы реферата должны быть пронумерованы. Каждый вопрос в тексте должен иметь заголовок в точном соответствии с наименованием в плане-оглавлении. При написании и оформлении реферата следует избегать типичных ошибок, например, таких:

– поверхностное изложение основных теоретических вопросов выбранной темы, когда автор не понимает, какие проблемы в тексте являются главными, а какие второстепенными,

– в некоторых случаях проблемы, рассматриваемые в разделах, не раскрывают основных аспектов выбранной для реферата темы,
– дословное переписывание книг, статей, заимствования рефератов из интернет и т. д.
При проверке реферата преподавателем оцениваются:
1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.
2. Характеристика реализации цели и задач исследования (новизна и актуальность поставленных в реферате проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).
3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).
4. Качество и ценность полученных результатов (степень завершенности реферативного исследования, спорность или однозначность выводов).
5. Использование литературных источников.
6. Культура письменного изложения материала.
7. Культура оформления материалов работы.

Задания для оценки умений

1. Ситуационные задачи:

Задача 6 История вирусов

Александр Квасов, начальник управления информационных технологий Нижегородского регионального центра-филиала ОАО АКБ «СОЮЗ»:

— В конце 90-х много вирусов было настроено на остановку работоспособности компьютера — уничтожение информации в BIOS, и на жестких дисках. На себе я испытал поражение жесткого диска вирусом W95.CIH «Чернобыль». На офисных компьютерах стояла операционная система Windows 95, доступ в Интернет имел один компьютер, остальные были связаны с ним в локальной сети. 26 апреля 1999 года не загрузились все офисные компьютеры, информация на дисках стала недоступной. Данные, к счастью, удалось восстановить, однако это было не так просто. Фирма понесла большие убытки.
Пометка для педагога: Напомним, что W95.CIH заражал исполняемые файлы и обладал крайне деструктивной функциональностью. Он полностью уничтожал содержимое жесткого диска и перезаписывал флэш-BIOS материнской платы, после чего заражённый компьютер вообще переставал загружаться. Наиболее уязвимы для вируса компьютеры на базе операционных систем Windows 95, 98 и Me. В этом случае вирус ищет файлы с расширением .EXE и записывает свой код в неиспользуемые части этих файлов. Размер зараженных файлов при этом практически не увеличивается, и у пользователя не возникает никаких подозрений.
Участникам обсуждения проблемы предлагается представить себя на месте сотрудников ОАО АКБ «СОЮЗ», предложить варианты обнаружения заражения, проверки, профилактики, защиты данных.

Задача7: Классификация вирусов

У журналиста-фрилансера возникли проблемы с программным обеспечением:
1. Большинство программ перестают работать и "вылетают" с критической ошибкой
2. Загрузка в безопасном режиме невозможна
3. Сайты kaspersky.ru, drweb.ru, viruslist.ru и пр. не загружаются
4. Значительно снизилась производительность компьютера.
Он решил, что это - результат деятельности вируса.
Участникам обсуждения предлагается по симптомам определить, что за вирус, как его лечить

Пометка для педагога: Вирус, который Kaspersky определяет как VIRUS.WIN32.Sality.z, а Dr. Web - win32.sector.5, win32.sector.7 (подробное описание). Даже у опытных пользователей его уничтожение вызывает трудности.
Пример решения:
1. Отключаем сеть. Т.е. отключаем ADSLm Dial-up, LAN - любые сетевые подключения. Просто выдергиваем кабель.

2. Идем к неинфицированному компьютеру, т.к. на инфицированном не удастся получить доступ к сайту, и скачиваем Dr.Web CureIt!. Это бесплатное приложение, которое может работать даже без установки. Скачанное приложение по возможности записываем на CD/DVD или флешку с защитой - дабы вирус не мог испортить программу. Если испортит - вместо приветственного окошка вы увидите окно стандартного распаковщика WinRAR SFX.
3. Чиним реестр с помощью установки ключа. Соглашаемся с внесением изменений в реестр.
4. Загружаемся в безопасном режиме, удерживая длительное время сразу после включения компьютера клавишу F8. Должно появиться меню с выбором вариантов загрузки. Нам нужен "Безопасный режим".
5. Лечим компьютер от вирусов. Для этого вставляем диск с записанным Dr.Web CureIt! и проводим полную проверку компьютера.
6. Перезагружаемся в обычном режиме.
7. Вновь проводим полную проверку.
8. Устанавливаем нормальный антивирус со свежими базами.

Задания для оценки владений

Раздел: Компьютерные вирусы как особый класс разрушающих программных воздействий и защита от них.

Задания для оценки знаний

Задания для оценки умений

Задания для оценки владений

1. Эссе:

Образец эссе.
Классификации современных программно-аппаратных комплексов
Бурное развитие средств вычислительной техники, автоматизированных информационных систем, появление новых информационных технологий в нашей стране сопровождается появлением таких малоприятных явлений, как промышленный шпионаж, компьютерная преступность и прежде всего несанкционированный доступ к конфиденциальной информации. Этим обуславливается актуальность и значимость проблемы защиты информации. Острая необходимость в защите информации нашла выражение в создании Государственной системы защиты информации (ГСЗИ). Развивается так же и правовая база информационной безопасности, а именно, приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных» и др. Целями защиты информации являются:
1. предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении;
2. реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими законами и нормативными документами по безопасности информации
3. создание определенных программно-аппаратных средств защиты, соответствующих потребностям владельцев (пользователей) информации.
Любое современное предприятие (учреждение, фирма и т.д.), независимо от вида деятельности и форм собственности, не может сегодня успешно развиваться и вести хозяйственную и иную деятельность без создания надежной системы защиты своей информации, включающей не только организационно-нормативные меры, но и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах, прежде всего, программно-аппаратные.
Большинство функций современных КС реализованы в виде программ, поддержание целостности которых при запуске системы и особенно в процессе функционирования является трудной задачей. Значительное число пользователей в той или иной степени обладают познаниями в программировании, осведомлены об ошибках в построении операционных систем. Поэтому существует достаточно высокая вероятность применения ими имеющихся знаний для атак на программное обеспечение. Проверка целостности одних программ при помощи других не является надежной. Необходимо четко представлять, каким образом обеспечивается целостность собственно программы проверки целостности. Если обе программы находятся на одних и тех же носителях, доверять результатам такой проверки нельзя. В связи с этим к программным системам защиты от несанкционированного доступа следует относиться с особой осторожностью.

Использование аппаратных средств снимает проблему обеспечения целостности системы. В большинстве современных систем защиты от НСД применяется зашивка программного обеспечения в ПЗУ или в аналогичную микросхему. Таким образом, для внесения изменений вПО необходимо получить доступ к соответствующей плате и заменить микросхему. В случае использования универсального процессора реализация подобных действий потребует применения специального оборудования, что еще более затруднит проведение атаки. Использование специализированного процессора с реализацией алгоритма работы в виде интегральной микросхемы полностью снимает проблему нарушения целостности этого алгоритма.
Для того, чтобы защитить информацию от НСД, существует ряд специально проводимых мер:
- Применение аппаратных средств:
  - установка фильтров, межсетевых экранов;
  - блокировка клавиатуры;
  - устройства аутентификации;
  - использование электронных замков на микросхемах.
- Применение программных средств:
  - использование пароля для доступа к компьютеру;
  - использование средств парольной защиты BIOS — как на сам BIOS, так и на ПК в целом.
- Применение аппаратно-программных средств:
  - использование аппаратно-программных средств доверенной загрузки
- Применение шифрования:
  - Шифрование — это преобразование (кодирование) открытой информации в зашифрованную, для передачи закрытой информации или сведений, составляющих государственную тайну информации по незащищенным каналам связи. Зачастую, сам алгоритм шифрования известен всем, а ключ, с помощью которого можно расшифровать данное сообщение засекречен.
- Проведение организационных мероприятий:
  - осуществление пропускного режима;
  - хранение носителей информации в закрытом доступе;
  - ограничение лиц, имеющих доступ к компьютеру.

Рассмотрим несколько программно-аппаратных комплексов защиты информации.
1) Программно-аппаратный комплекс «Аккорд – 1.95».
Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа (ПАК СЗИ НСД) «Аккорд – 1.95», далее комплекс «Аккорд», предназначен для применения на ПЭВМ типа IBM PC в целях защиты ПЭВМ и информационных ресурсов от НСД и обеспечения конфиденциальности информации, обрабатываемой и хранимой в ПЭВМ при многопользовательском режиме ее эксплуатации. Комплекс разработан ОКБ САПР при участии фирмы «Инфокрипт» на основании лицензии Государственной технической комиссии при Президенте РФ (Гостехкомиссии России) от 02.06.95 N 56. Комплекс «Аккорд» состоит из программно-аппаратных средств «Аккорд АМДЗ» и ПО разграничения доступа «Аккорд 1.95-00». В настоящее время комплекс «Аккорд-1.95» выпускается в трех основных версиях в зависимости от модификации аппаратных средств (контроллеров):
- версия 2.0 – контроллер «Аккорд – 4++»;
- версия 3.0 – контроллер «Аккорд – 5»;
- версия 4.0 – контроллер «Аккорд – 4.5»; «Аккорд – СБ/2».

Все модификации могут использоваться на ПЭВМ с процессором 80386 и выше, объемом RAM 640 Кбайт и более. Для установки необходим свободный слот:
- ISA – для контроллеров «Аккорд – 4++»,«Аккорд – 4.5»;
- PCI – для контроллера «Аккорд – 5»;
- «Аккорд – СБ/2».

Используют для идентификации персональные ТМ-идентификаторы DS 199X с объемом памяти до 64 Кбит. Используют для аутентификации пароль до 12 символов. Блокируют загрузку с FDD, CD ROM, ZIP Drive. Предусматривают регистрацию от 16 до 32 пользователей. 147 Имеют аппаратный датчик случайных чисел (ДСЧ). Имеют возможность применения съемника, использующего внутреннее подключение к контроллеру (внутренний съемник). Обеспечивают контроль целостности программ, данных и системных областей жестких дисков. Имеют внутреннюю энергонезависимую память для хранения данных о зарегистрированных пользователях и журнала регистрации событий. Допускают изменение встроенного ПО (технологический режим) без замены платы контроллера. Обеспечивают режим доверенной загрузки ОС (выполнение процедур идентификации/аутентификации пользователя, контроль целостности аппаратной части ПЭВМ, системных файлов, программ и данных до загрузки ОС на аппаратном уровне).
2) Программно-аппаратный комплекс Secret Net NT 4.0.
Автономный вариант системы защиты информации Secret Net NT 4.0 предназначен для защиты ресурсов рабочей станции локальной сети или неподключенного к сети компьютера и разработан научно-инженерным предприятием «ИНФОРМЗАЩИТА».
Система Secret Net NT 4.0 дополняет стандартные защитные механизмы ОС Windows NT функциями, обеспечивающими:
- идентификацию пользователей при помощи специальных аппаратных средств (Touch Memory, Smart Card, Smarty);

• дополнительно к избирательному (дискреционному) управлению доступом, реализованному в ОС Windows NT, полномочное (мандатное) управление доступом пользователей к конфиденциальной информации на локальных и подключенных сетевых дисках;
• оперативный контроль работы пользователей компьютера путем регистрации событий, связанных с безопасностью ИС, удобные средства просмотра и представления зарегистрированной информации;
• контроль целостности программ, используемых пользователями и операционной системой;
• возможность создания для любого пользователя замкнутой программной среды (списка разрешенных для запуска программ);
• простоту управления объектами благодаря использованию механизма шаблонов настроек.

3) Комплекс КРИПТОН-ЗАМОК для ограничения доступа к компьютеру

Комплекс КРИПТОН-ЗАМОК предназначен для построения аппаратно- программных средств ограничения доступа к компьютеру с использованием УКЗД серии КРИПТОН. Комплекс позволяет организовать на базе персонального компьютера рабочее место с ограничением круга лиц, имеющих доступ к содержащейся в нем информации. Для работы комплекса КРИПТОН-ЗАМОК необходим персональный компьютер IBM PC с процессором не ниже i386 и операционной системой-MS DOS, Windows 95/98/NT, UNIX и другими, для которых имеется соответствующий драйвер, позволяющий под управлением MS DOS понимать формат установленной на компьютере файловой системы. Комплекс служит для защиты компьютеров с жесткими дисками, с файловыми системами в форматах FAT 12, FAT 16, FAT 32, NTFS, UNIX и т.д. Работа с дисками с файловыми системами FAT 12, FAT 16 и FAT 32 обеспечивается средствами комплекса без дополнительных драйверов. Работа с 121 дисками с нестандартными файловыми системами NTFS, HTFS, UNIX и т.д., не поддерживаемыми операционной системой MS-DOS, может производиться только при наличии на компьютере соответствующих DOS-драйверов.

4) Система защиты конфиденциальной информации Secret Disk.

Система защиты конфиденциальной информации Secret Disk разработана компанией Aladdin при участии фирмы АНКАД и предназначена для широкого круга пользователей компьютеров: руководителей, менеджеров, бухгалтеров, 125 аудиторов, адвокатов, т. е. всех тех, кто должен заботиться о защите личной или профессиональной информации.

При установке системы Secret Disk на компьютере создаются новые логические диски, при записи на которые информация автоматически шифруется, а при чтении-расшифровывается. Работа с секретными дисками совершенно незаметна и равносильна встраиванию шифрования во все запускаемые приложения (например, бухгалтерскую программу, Word, Excel и т.п.).

В системе Secret Disk используется смешанная программно-аппаратная схема защиты с возможностью выбора, соответствующего российским нормативным требованиям криптографического алгоритма ГОСТ 28147-89 с длиной ключа 256 бит (программный эмулятор платы КРИПТОН или криптоплата КРИПТОН фирмы АНКАД).

Важная особенность системы Secret Disk заключается в том, что для доступа к защищенной информации необходим не только вводимый пользователем пароль, но и электронный идентификатор. В качестве такого идентификатора может использоваться обычный электронный ключ для параллельного порта, карточка PCMCIA для ноутбуков или смарт-карта (в этом случае необходимо установить в компьютер специальный считыватель смарт- карт).

5) Система защиты данных Crypton Sigma

Система Crypton Sigma - это программный комплекс, предназначенный для защиты данных на персональном компьютере. По своим возможностям он во многом аналогичен системе Secret Disk. Будучи установленной на компьютере, система Crypton Sigma хранит конфиденциальные данные в зашифрованном виде, не допуская несанкционированный доступ и утечку данных. Для шифрования данных в системе Crypton Sigma используется алгоритм шифрования ГОСТ 28147-89.

Система защиты конфиденциальных данных Crypton Sigma ориентирована на широкий круг пользователей компьютеров-бизнесменов, менеджеров, бухгалтеров, адвокатов и др., т.е. всех тех, кто нуждается в защите профессиональной и личной информации.

Система Crypton Sigma легко устанавливается, проста и надежна в использовании, а также полностью "прозрачна"для всех программ и системных утилит операционной системы. При установке системы Crypton Sigma на компьютере создаются новые логические диски. При записи на эти диски информация автоматически шифруется, а при считывании-расшифровывается. Этот метод прозрачного шифрования позволяет полностью снять с пользователя заботу о защите данных. Работа с защищенными дисками незаметна для пользователя и равносильна встраиванию процедур шифрования/расшифрования в запускаемые приложения. Защищенные 127 системой диски на вид ничем не отличаются от обычных и могут использоваться в локальной или глобальной сети.

Список литературы:

1) Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. Издание 2-е испр. и доп.– М.:Машиностроение-1, 2006. − 260 с.

2) С.К. Варлатая, М.В. Шаханова. Программно-аппаратная защита информации: учеб. Пособие.- Владивосток: Изд-во ДВГТУ, 2007.
3) Саяркин Л. А., Зайцева А. А., Лапин С. П., Домбровский Я. А. Программно-аппаратные средства защиты автоматизированных систем от несанкционированного доступа // Молодой ученый. — 2017. — №13.

2. Оценочные средства для промежуточной аттестации

1. Зачет

Вопросы к зачету:

1. • Защита авторских прав на электронные документы в России. Правовая база.
2. • Применение электронной подписи (ЭП) в России (хранение ЭП, идентификация и аутентификация при помощи ЭП). Правовая база применения ЭП в России.
3. • Web-сайт. Выбор способа написания. Преимущества и недостатки.
4. • Продвижение сайта в поисковых системах.
5. • Защищенные централизованные хранилища данных (ЦХД): принципы построения, продукты-менеджеры, угрозы ЦХД.
6. • Утечка информации при помощи побочного электромагнитного излучения и наводок (ПЭМИН).
7. • Стандарт ISO/IEC 17799:2005.
8. • Стандарт ISO/IEC 27001:2005.
9. • Стандарт BS 7799-3:2006.
10. • Обзор новых и широко используемых криптографических стандартов и алгоритмов.
11. • Обзор современных программных средств криптографического управления данными (шифрование, удаление, создание защищенных дисков и т.д.).
12. • Протоколы шифрования при передаче по сети (в т.ч. беспроводной). Примеры (WPA и т.д.)
13. • Обзор программных средств выполнения активного аудита.
14. • Защита от копирования CD, DVD дисков.
15. • Целостность информации. Средства резервного копирования. Обзор имеющихся средств.
16. • Средства восстановления потерянных или удаленных файлов. Средства полного уничтожения информации.
17. • Виртуальные машины. Примеры. Работа с VMWare.
18. • Методы и средства идентификации и аутентификации в компьютерных системах.
19. • Устройство и работа бесконтактных карт, смарт-карт, электронных ключей и т.п.
20. • Наиболее известные и удачные попытки взлома последних двух лет. В лицах и фактах.
21. • Классификация вредоносных программ. Методы защиты, алгоритмы работы противоборствующих программ.
22. • Принцип работы программных и аппаратных межсетевых экранов (МЭ). Предлагаемые возможности.
23. • Решения по защите от несанкционированного использования мобильных устройств (мобильных телефонов, смартфонов, КПК и т.п.)
24. • Защита Web-сервера. Организация доступа к Web-серверу для просмотра информации.
25. • Возможность удаленного управления компьютером (УУК). Защита от несанкционированного УУК.
26. • Обзор локальных и сетевых программ-шпионов (клавиатурные, запуск программ, клавиатурные в окне конкретной программы и т.п.).
27. • Программные средства по контролю за действиями пользователей
28. • Защита от перехвата трафика, передаваемого по радиоканалам (wi-fi, bluetooth, и т.д.), защита точек доступа, построение беспроводных сетей.
29. • Организация и защита VPN-сетей.
30. • Безопасность VoIP.

2. Экзамен

Вопросы к экзамену:

1. • Понятие защищенной операционной системы.
2. • Подходы к организации защиты операционной системы.
3. • Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.
4. • Применение типовых моделей управления доступом в операционных системах.
5. • Управление доступом в UNIX.

6. • Управление доступом в Windows.
7. • Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты.
8. • Средства минимизации полномочий пользователей в Windows.
9. • Управление средствами аутентификации в Linux и Windows.
10. • Управление средствами аудита в Linux и Windows.
11. • Управление доменами Windows.
12. • Групповая политика в доменах Windows.
13. • Сетевые атаки.
14. • Адаптивная безопасность в вычислительных сетях.
15. • Пакетные фильтры и межсетевые экраны, их классификация и особенности применения.
16. • Виртуальные частные сети.
17. • Угрозы безопасности баз данных: общие и специфичные.
18. • Модели безопасности СУБД.
19. • Средства и методы обеспечения целостности данных СУБД.
20. • Ролевое разграничение доступа к данным в современных СУБД.
21. • Понятие программной закладки.
22. • Модели взаимодействия программной закладки с атакуемой компьютерной системой.
23. • Предпосылки к внедрению программных закладок.
24. • Метод внедрения программных закладок.
25. • Основные принципы построения политики безопасности, повышающей защищенность от программных закладок.
26. • Сигнатурное и эвристическое сканирование как метод выявления программных закладок.
27. • Контроль целостности как метод выявления программных закладок.
28. • Антивирусный мониторинг как метод выявления программных закладок.
29. • Изолированная программная среда как метод выявления программных закладок.
30. • Файловые вирусы: жизненный цикл, особенности функционирования, особенности противодействия файловым вирусам.
31. • Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам.
32. • Скриптовые вирусы: жизненный цикл, особенности функционирования, особенности противодействия Скриптовым вирусам.
33. • Стелс-технологии: назначение, методы противодействия.
34. • Основные компоненты подсистемы защиты Unix
35. • Файловая система – как основа подсистемы защиты.
36. o Права доступа к элементам файловой системы.
37. o Управление процессами. Создание и удаление бюджетов пользователей
38. • Основные компоненты подсистемы защиты ОС Windows
39. • Основы взаимодействия элементов гетерогенных сетей
40. • Методы и средства ограничения доступа к компонентам ЭВМ.

Раздел 4. Методические материалы, определяющие процедуры оценивания значни, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Для текущего контроля используются следующие оценочные средства:

1. Задача

Задачи позволяют оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины;
умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей.
Алгоритм решения задач:
1.Внимательно прочитайте условие задания и уясните основной вопрос, представьте процессы и явления, описанные в условии.
2.Повторно прочтите условие для того, чтобы чётко представить основной вопрос, проблему, цель решения, заданные величины, опираясь на которые можно вести поиск решения.
3.Произведите краткую запись условия задания.
4.Если необходимо, составьте таблицу, схему, рисунок или чертёж.
5.Установите связь между искомыми величинами и данными; определите метод решения задания, составьте план решения.
6.Выполните план решения, обосновывая каждое действие.
7.Проверьте правильность решения задания.
8.Произведите оценку реальности полученного решения.
9.Запишите ответ.

2. Кейс-задачи

Кейс – это описание конкретной ситуации, отражающей какую-либо практическую проблему, анализ и поиск решения которой позволяет развивать у обучающихся самостоятельность мышления, способность выслушивать и учитывать альтернативную точку зрения, а также аргументировано отстаивать собственную позицию.
Рекомендации по работе с кейсом:
1. Сначала необходимо прочитать всю имеющуюся информацию, чтобы составить целостное представление о ситуации; не следует сразу анализировать эту информацию, желательно лишь выделить в ней данные, показавшиеся важными.
2. Требуется охарактеризовать ситуацию, определить ее сущность и отметить второстепенные элементы, а также сформулировать основную проблему и проблемы, ей подчиненные. Важно оценить все факты, касающиеся основной проблемы (не все факты, изложенные в ситуации, могут быть прямо связаны с ней), и попытаться установить взаимосвязь между приведенными данными.
3. Следует сформулировать критерий для проверки правильности предложенного решения, попытаться найти альтернативные способы решения, если такие существуют, и определить вариант, наиболее удовлетворяющий выбранному критерию.
4. В заключении необходимо разработать перечень практических мероприятий по реализации предложенного решения.
5. Для презентации решения кейса необходимо визуализировать решение (в виде электронной презентации, изображения на доске и пр.), а также оформить письменный отчет по кейсу.

3. Опрос

Опрос представляет собой совокупность развернутых ответов студентов на вопросы, которые они заранее получают от преподавателя. Опрос может проводиться в устной и письменной форме.
Подготовка к опросу включает в себя:
- изучение конспектов лекций, раскрывающих материал, знание которого проверяется опросом;
- повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения;
- изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний;
- составление в мысленной форме ответов на поставленные вопросы.

4. Отчет по лабораторной работе

При составлении и оформлении отчета следует придерживаться рекомендаций, представленных в методических указаниях по выполнению лабораторных работ по дисциплине.

5. Реферат

Реферат − теоретическое исследование определенной проблемы, включающее обзор соответствующих литературных и других источников.
Реферат обычно включает следующие части:
1. библиографическое описание первичного документа;
2. собственно реферативная часть (текст реферата);
3. справочный аппарат, т.е. дополнительные сведения и примечания (сведения, дополнительно характеризующие первичный документ: число иллюстраций и таблиц, имеющихся в документе, количество источников в списке использованной литературы).

Этапы написания реферата
1. выбрать тему, если она не определена преподавателем;
2. определить источники, с которыми придется работать;
3. изучить, систематизировать и обработать выбранный материал из источников;
4. составить план;
5. написать реферат:

− обосновать актуальность выбранной темы;
− указать исходные данные реферируемого текста (название, где опубликован, в каком году), сведения об авторе (Ф. И. О., специальность, ученая степень, ученое звание);
− сформулировать проблематику выбранной темы;
− привести основные тезисы реферируемого текста и их аргументацию;
− сделать общий вывод по проблеме, заявленной в реферате.

При оформлении реферата следует придерживаться рекомендаций, представленных в документе «Регламент оформления письменных работ».

6. Ситуационные задачи

Ситуационная задача представляет собой задание, которое включает в себя характеристику ситуации из которой нужно выйти, или предложить ее исправить; охарактеризовать условия, в которых может возникнуть та или иная ситуация и предложить найти выход из нее и т.д.
При выполнении ситуационной задачи необходимо соблюдать следующие указания:
1. Внимательно прочитать текст предложенной задачи и вопросы к ней.
2. Все вопросы логично связаны с самой предложенной задачей, поэтому необходимо работать с каждым из вопросов отдельно.
3. Вопросы к задаче расположены по мере усложнения, поэтому желательно работать с ними в том порядке, в котором они поставлены.

7. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.
При самостоятельной подготовке к тестированию студенту необходимо:
− проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;
− выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.
− работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);
− в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.
− решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.
− оставить время для проверки ответов, чтобы избежать механических ошибок.

8. Эссе

Эссе - это прозаическое сочинение небольшого объема и свободной композиции, выражающее индивидуальные впечатления и соображения по конкретному поводу или вопросу и заведомо не претендующее на определяющую или исчерпывающую трактовку предмета.
Структура эссе определяется предъявляемыми к нему требованиями: мысли автора эссе по проблеме излагаются в форме кратких тезисов; мысль должна быть подкреплена доказательствами - поэтому за тезисом следуют аргументы . При написании эссе важно также учитывать следующие моменты:
Вступление и заключение должны фокусировать внимание на проблеме (во вступлении она ставится, в заключении - резюмируется мнение автора).
Необходимо выделение абзацев, красных строк, установление логической связи абзацев: так достигается целостность работы.
Стиль изложения: эссе присущи эмоциональность, экспрессивность, художественность. Должный эффект обеспечивают короткие, простые, разнообразные по интонации предложения, умелое использование "самого современного" знака препинания - тире.
Этапы написания эссе:
1. написать вступление (2–3 предложения, которые служат для последующей формулировки проблемы).
2. сформулировать проблему, которая должна быть важна не только для автора, но и для других;
3. дать комментарии к проблеме;
4. сформулировать авторское мнение и привести аргументацию;
5. написать заключение (вывод, обобщение сказанного).

При оформлении эссе следует придерживаться рекомендаций, представленных в документе «Регламент оформления письменных работ».

2. Описание процедуры промежуточной аттестации

Оценка за зачет/экзамен может быть выставлена по результатам текущего рейтинга. Текущий рейтинг – это результаты выполнения практических работ в ходе обучения, контрольных работ, выполнения заданий к лекциям (при наличии) и др. видов заданий.

Результаты текущего рейтинга доводятся до студентов до начала экзаменационной сессии.

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Зачет может проводиться как в формате, аналогичном проведению экзамена, так и в других формах, основанных на выполнении индивидуального или группового задания, позволяющего осуществить контроль знаний и полученных навыков.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

Экзамен преследует цель оценить работу обучающегося за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять их для решения практических задач.

Экзамен проводится в устной или письменной форме по билетам, утвержденным заведующим кафедрой (или в форме компьютерного тестирования). Экзаменационный билет включает в себя два вопроса и задачи. Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения обучающихся не позднее чем за один месяц до экзаменационной сессии.

В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп.

При любой форме проведения экзаменов по билетам экзаменатору предоставляется право задавать студентам дополнительные вопросы, задачи и примеры по программе данной дисциплины. Дополнительные вопросы также, как и основные вопросы билета, требуют развернутого ответа.