Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 27.03.04 Управление в технических системах

Наименование образовательной программы: Автоматизированные системы управления

Уровень образования: высшее образование - бакалавриат

Форма обучения: Заочная

Оценочные материалы
по дисциплине
Методы и средства защиты информации

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бородкин А.А. Идентификатор: R2a2cc3a1-BorodkinAA-1ae5255b	А.А. Бородкин
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бобряков А.В. Идентификатор: R2c90f415-BobriakovAV-70dec1fa	А.В. Бобряков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-8 способностью использовать нормативные документы в своей деятельности

2. ОПК-9 способностью использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Вредоносные программы (Тестирование)
2. Понятие информационной безопасности (Тестирование)

Форма реализации: Письменная работа

1. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей (Лабораторная работа)
2. Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ (Лабораторная работа)
3. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации (Лабораторная работа)

БРС дисциплины

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %					
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5
	Срок КМ:	3	6	8	11	14
Комплексный подход к обеспечению информационной безопасности						
Введение и основные понятия		+				
Комплексный подход к защите информации		+				
Методы защиты от несанкционированного доступа к информации в компьютерных системах						
Организация регистрационных баз данных			+			

Аутентификация при локальном доступе		+			
Аутентификация при локальном и удаленном доступе		+			
Аутентификация при удаленном доступе		+			
Программно-аппаратные средства защиты от несанкционированного доступа к информации в компьютерных системах					
Разграничение прав пользователей компьютерных систем			+		
Средства защиты информации в операционных системах			+		
Криптографические методы и средства защиты информации					
Введение в криптографию				+	
Симметричная криптография				+	
Симметричная и асимметричная криптография				+	
Асимметричная криптография и ее применение				+	
Защита от вредоносных программ и несанкционированного копирования информационных ресурсов					
Криптография и стеганография					+
Защита от несанкционированного копирования					+
Защита от вредоносных программ					+
Вес КМ:	20	20	20	20	20

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-8	ОПК-8(Компетенция)	Знать: методы разграничения полномочий пользователей и управления доступом к ресурсам в компьютерных системах и сетях Уметь: применять методы разграничения полномочий пользователей и управления доступом к данным в компьютерных системах и сетях	Понятие информационной безопасности (Тестирование) Разработка программы разграничения полномочий пользователей на основе парольной аутентификации (Лабораторная работа)
ОПК-9	ОПК-9(Компетенция)	Знать: способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем Уметь: использовать методы и средства криптографической	Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей (Лабораторная работа) Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ (Лабораторная работа) Вредоносные программы (Тестирование)

		защиты информации анализировать, выбирать и применять методы и средства защиты от вредоносных программ	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Понятие информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Технология проверки связана с выполнением контрольного теста по изученной теме. Время, отведенное на выполнение задания, устанавливается не более 30 минут. Количество попыток не более 3-х. Тестирование проводится с использованием СДО "Прометей". К тестированию допускается пользователь, изучивший материалы, авторизованный уникальным логином и паролем

Краткое содержание задания:
Контрольная точка направлена на проверку знаний по общим вопросам информационной безопасности

Контрольные вопросы/задания:

Знать: методы разграничения полномочий пользователей и управления доступом к ресурсам в компьютерных системах и сетях	1.**Что такое информационная безопасность?** 1.Деятельность по предотвращению утечки информации, непреднамеренного и несанкционированного воздействия на информацию 2.Деятельность по обеспечению защищенности информации 3.Деятельность по созданию безопасных информационных систем 4.Состояние защищенности информационной среды объекта **Ответ: 4** 2.**Отметьте подход к защите компьютерной информации?** 1.Фрагментарный подход 2.Системный подход 3.Комплексный подход **Ответ: 1,2,3** 3.**Почему не может быть создана абсолютно надежная система защиты компьютерной информации?** 1.Из-за невозможности избежать ошибок при ее проектировании 2.Из-за невозможности избежать ошибок при ее реализации 3.Из-за очень большой сложности данной задачи 4.Из-за невозможности формально описать действия нарушителя 5.Такая система защиты может быть создана **Ответ: 4** 4.**В чем разница между компьютерными вирусами и червями?**

	1.Червь не является автономной программой 2.Вирус не является автономной программой 3.Вирус обязательно заражает другие объекты, а червь нет 4.Червь обязательно заражает другие объекты, а вирус нет **Ответ: 3** 5.**Отметьте непосредственные каналы утечки, не требующие изменения элементов КС (без оставления следов):** 1.Хищение носителей информации 2.Сбор производственных отходов 3.Намеренное копирование файлов 4.Чтение остаточной информации после выполнения заданий других пользователей 5.Копирование носителей информации 6.Все перечисленные **Ответ: 6** 6.**Отметьте верное утверждение:** 1.Пассивное подключение легко предотвратить, но невозможно обнаружить 2.Пассивное подключение невозможно предотвратить, но легко обнаружить 3.Пассивное подключение невозможно предотвратить и невозможно обнаружить 4.Пассивное подключение легко предотвратить и легко обнаружить **Ответ: 1** 7.**Отметьте верное утверждение:** 1.Активное подключение невозможно обнаружить, но легко предотвратить 2.Активное подключение легко обнаружить, но невозможно предотвратить 3.Активное подключение невозможно обнаружить и невозможно предотвратить 4.Активное подключение легко обнаружить и легко предотвратить **Ответ: 2** 8.**Укажите технические средства охраны:** 1.Средства контроля и управления доступом (СКУД) 2.Средства охранной сигнализации 3.Средства видеонаблюдения (охранного телевидения, CCTV) **Ответ: 1,2,3** 9.**Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это:** 1.уязвимость информации 2.надежность информации

	3.защищенность информации 4.безопасность информации **Ответ: 4** 10.**Организационные требования к системе защиты:** 1.управленческие и идентификационные 2.административные и аппаратурные 3.административные и процедурные 4.аппаратурные и физические **Ответ: 3**

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации

Формы реализации: Письменная работа
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Отчет по лабораторной работе по вариантам отправляются в СДО "Прометей" в рамках функционала "Письменная работа"

Краткое содержание задания:
Контрольная точка направлена на рассмотрение умений по разработке программы разграничения полномочий пользователей. 1. Программа должна обеспечивать работу в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя. 2. В режиме администратора программа должна поддерживать следующие функции (при правильном вводе пароля): · смена пароля администратора (при правильном вводе старого пароля); · просмотр списка имен зарегистрированных пользователей и установленных для них параметров (блокировка учетной записи, включение ограничений на выбираемые пароли) – всего списка целиком в одном окне или по одному элементу списка с возможностью перемещения к его началу или концу; · добавление уникального имени нового пользователя к списку с пустым паролем (строкой нулевой длины); · блокирование возможности работы пользователя с заданным именем; · включение или отключение ограничений на выбираемые пользователем пароли (в соответствии с индивидуальным заданием, определяемым номером варианта); · завершение работы с программой. 3. В режиме обычного пользователя программа должна поддерживать только функции смены пароля пользователя (при правильном вводе старого пароля) и завершения работы, а все остальные функции должны быть

заблокированы. 4. После своего запуска программа должна запрашивать у пользователя в специальном окне входа ввод его имени и пароля. При вводе пароля его символы всегда должны на экране заменяться символом ‘*’. 5. При отсутствии введенного в окне входа имени пользователя в списке зарегистрированных администратором пользователей программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой. 6. При неправильном вводе пароля программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода. При трехкратном вводе неверного пароля работа программы должна завершаться. 7. При первоначальном вводе пароля (обязательном при первом входе администратора или пользователя с зарегистрированным ранее администратором именем) и при дальнейшей замене пароля программа должна просить пользователя подтвердить введенный пароль путем его повторного ввода. 8. Если выбранный пользователем пароль не соответствует требуемым ограничениям (при установке соответствующего параметра учетной записи пользователя), то программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность ввода другого пароля, завершения работы с программой (при первом входе данного пользователя) или отказа от смены пароля. 9. Информация о зарегистрированных пользователях, их паролях, отсутствии блокировки их работы с программой, а также включении или отключении ограничений на выбираемые пароли должна сохраняться в специальном файле. При первом запуске программы этот файл должен создаваться автоматически и содержать информацию только об администраторе, имеющем пустой пароль. 10. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния. 11. Для реализации указанных в пунктах 2-3 функций в программе должны использоваться специальные диалоговые формы, позволяющие пользователю (администратору) вводить необходимую информацию. 12. Программа для выполнения лабораторной работы составляется на основе выбранного студентом варианта Указаний по выполнению лабораторной работы (с учетом рекомендаций по использованию средств выбранного языка программирования, приведенных в конце этого описания лабораторной работы), после чего в исходный код созданной программы вносятся изменения в соответствии с индивидуальным заданием студента. 13. Все файлы проекта программы, включая файл с исполнимым кодом – exe-файлом – программы помещаются в один архив и отсылаются лектору

Контрольные вопросы/задания:

Уметь: применять методы разграничения полномочий пользователей и управления доступом к данным в компьютерных системах и сетях	1.Продемонстрируйте функционирование программы по обеспечению работы в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя 2.Покажите способность программы при выдавать соответствующее сообщение при неправильном вводе пароля 3.Продемонстрируйте файл с информацией о зарегистрированных пользователях, который создается при первом запуске программы 4.Продемонстрируйте организацию основного меню программы 5.Укажите обязательную часть основного меню

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-3. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей

Формы реализации: Письменная работа
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Отчет по лабораторной работе по вариантам отправляются в СДО "Прометей" в рамках функционала "Письменная работа"

Краткое содержание задания:
Контрольная точка направлена на рассмотрение программных средств защиты от несанкционированного доступа и разграничения прав пользователей. 1. Пункт выполняется в виртуальной машине Windows XP или с правами администратора. Запустить программу Редактор реестра Windows regedit.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра. 1.1. Включить в отчет, воспользовавшись, например, Справкой редактора реестра, краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE). 1.2. Включить в электронную версию отчета копии экранных форм, иллюстрирующих использование редактора реестра (рисунок с изображением активной формы помещается в буфер обмена с помощью комбинации клавиш Alt+Print Screen). 2. Пункт выполняются в виртуальной машине Windows XP или с правами администратора. Запустить программу Редактор локальной групповой политики gpedit.msc, позволяющую ограничить возможности пользователей ОС Windows. 2.1. Включить в отчет сведения о назначении и основных функциях программы. 2.2. Освоить управление настройками обозревателя Internet Explorer для пользователя (узел Политика «Локальный компьютер» | Конфигурация пользователя | Административные шаблоны | Компоненты Windows | Internet Explorer). 2.3. Освоить установку ограничений возможностей пользователя (узлы группы Политика «Локальный компьютер» | Конфигурация пользователя | Административные шаблоны) по изменению структуры Рабочего стола и Главного меню, использованию функций Панели управления и компонент Windows (Проводника, консоли управления Microsoft, планировщика задач, проигрывателя Windows Media и др.), работе с локальной сетью, использованию общих папок, использованию различных системных функций. 2.4. Включить в отчет, воспользовавшись, например, Справкой Редактора локальной групповой политики, ответ на вопрос, чем отличаются значения параметров «отключен» и «не задан». 2.5. Включить в электронную версию отчета копии экранных форм, используемых при работе с программой gpedit.msc. Завершить работу с программой gpedit.msc. 3. Пункт выполняется на компьютере с профессиональной версией Windows. С помощью процесса входа Winlogon, активизируемого комбинацией клавиш Ctrl+Alt+Del, заблокировать работу с используемой рабочей станцией на период временного отсутствия пользователя (если эта возможность не запрещена администратором). Разблокировать работу рабочей станции. 3.1. Включить в отчет сведения о порядке защиты рабочей станции на период временного отсутствия

пользователя и о других функциях Процесса входа, доступных при этом наряду с блокировкой. 3.2. С помощью функции Заставка в окне свойств или персонализации экрана, вызываемого из его контекстного меню, ознакомиться с другой возможностью блокировки компьютера на период временного отсутствия пользователя. Отразить полученные сведения в отчете. Включить в электронную версию отчета копии экранных форм, полученных при выполнении этого пункта. 4. Открыть (или создать) произвольный документ в текстовом процессоре Word. 4.1. Изучить порядок использования паролей для защиты документов в Microsoft Word от чтения и записи (два разных типа паролей) и включить в отчет соответствующие сведения (в Office 2013 использовать команду Файл | Сведения | Защита документа, в Office 2010 использовать команду Файл | Сведения | Защитить документ, в Office 2007 – Кнопка Microsoft Office | Подготовить и Рецензирование | Защитить документ, в Office 2003 – Сервис | Параметры | Безопасность). 4.2. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Word. 5. Открыть (или создать) произвольную таблицу Excel. 5.1. Изучить порядок использования паролей для защиты документов или их частей в табличном процессоре Microsoft Excel от чтения и записи и включить в отчет соответствующие сведения. 5.2. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Excel. 6. Пункты 6-8 выполняются в виртуальной машине Windows XP или с правами администратора. Скопировать в личную папку на локальном жестком диске файл whisper.msi. 7. Если программа Whisper 32 не установлена (соответствующий пункт отсутствует в меню в главном меню), то установить ее с помощью файла whisper.msi. 8. Запустить программу whisper.exe, предназначенную для создания и ведения базы данных паролей пользователя. 8.1. Изучить назначение и основные функции программы и включить в отчет соответствующие сведения. 8.2. Создать 2-3 записи о паролях к различным ресурсам (записи обязательно должны содержать фамилию и инициалы студента в полях имени или комментария). 8.3. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с программой whisper.exe. 9. Ознакомиться (на примере папок c: \ Пользователи \ Имя пользователя \ Мои документы \ Папка с фамилией студента и c: \ Пользователи \ Общие \ Общие документы или, при работе в Windows XP Professional, c:\ Documents and Settings \ Имя пользователя \ Документы \ Папка с фамилией студента и c:\ Documents and Settings \ All Users \ Документы) с порядком разграничения доступа к ресурсам в операционной системе Windows (с помощью команды Свойства | Безопасность контекстного меню объекта и элементов управления соответствующих диалоговых окон). Если команда Безопасность недоступна (при работе в ОС Windows XP Professional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки. 9.1. Включить в отчет сведения об особенностях управления доступом к папкам и файлам (родовых (generic, общих) правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности папки. 9.2. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. 10. Ознакомиться с порядком разграничения доступа к принтерам (с помощью Панели управления Windows | Устройства и принтеры | Свойства принтера). 10.1. Включить в отчет сведения об особенностях управления доступом к принтерам (родовых правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности объекта. 10.2. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. 11. Ознакомиться с

порядком разграничения доступа к разделам реестра (с помощью редактора реестра | Правка | Разрешения, выполняется в виртуальной машине Windows XP или с правами администратора). 11.1. Включить в отчет сведения об особенностях управления доступом к разделам реестра (родовых правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности объекта. 11.2. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. 12. Пункты 11-14 выполняются в виртуальной машине Windows XP или с правами администратора. Ознакомиться (с помощью функции Панели управления Администрирование | Управление компьютером – административная оснастка compmgmt.msc, узел Локальные пользователи и группы) с порядком создания и изменения учетных записей пользователей и групп в защищенных версиях операционной системы Windows. 12.1. Включить в отчет соответствующие сведения. 12.2. Включить в электронную версию отчета копии соответствующих экранных форм. 13. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя – административная оснастка secpol.msc, узел Локальные политики | Назначение прав пользователя) с порядком назначения прав пользователям и группам. 13.1. Включить в отчет соответствующие сведения. 13.2. Включить в электронную версию отчета копии соответствующих экранных форм. 14. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей – административная оснастка secpol.msc, узел Политики учетных записей | Политика паролей) с порядком определения параметров безопасности для парольной аутентификации. 14.1. Включить в отчет соответствующие сведения. 14.2. Включить в электронную версию отчета копии соответствующих экранных форм. 15. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей – административная оснастка secpol.msc, узел Политики учетных записей | Политика блокировки учетных записей) с порядком определения параметров безопасности для политики блокировки учетных записей. 15.1. Включить в отчет соответствующие сведения. 15.2. Включить в электронную версию отчета копии соответствующих экранных форм. 16. Включить в отчет титульный лист и сохранить файл с электронной версией отчета. 17. Выслать преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания. 18. После проверки электронной версии отчета преподавателем включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта и прилагаемой ниже таблицей. 19. Выслать преподавателю для защиты лабораторной работы документ, содержащий ответы на контрольные вопросы

Контрольные вопросы/задания:

Уметь: использовать методы и средства криптографической защиты информации	1.Укажите административные программы (оснастки) Windows предназначены для разграничения прав пользователей 2.Продемонстрируйте удаление меню Файл из меню Проводника с помощью редактора групповой политики 3.Опишите что происходит с документом Microsoft Office после установки защиты от чтения с помощью паролей 4.Покажите какая информация указывается при

	добавлении новой записи в базу данных программы whisper.exe 5.Расскажите основные недостатки модели разграничения доступа к объектам, реализованной в защищенных версиях операционной системы Windows

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-4. Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ

Формы реализации: Письменная работа
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Отчет по лабораторной работе по вариантам отправляются в СДО "Прометей" в рамках функционала "Письменная работа"

Краткое содержание задания:
Контрольная точка направлена на изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ. 1. Этот пункт выполняется в виртуальной машине Windows XP или с правами администратора. Если пункт выполняется в операционной системе Windows XP. Скопировать в произвольную папку на локальном жестком диске файл citadel.zip. 1.1. Извлечь файлы из архива. 1.2. Если программа Citadel Safstor не установлена (отсутствует соответствующий пункт в главном меню), то запустить программу setup.exe для установки программы шифрования файлов Citadel Safstor. 1.3. На примере работы с произвольными (несистемными) файлами различного типа изучить функции программы шифрования файлов Citadel Safstor, учитывая, что: · доступ к шифрованию (расшифрованию) возможен через контекстное меню Проводника Windows. Если соответствующая команда не появилась в контекстном меню Проводника, то шифрование файла возможно с помощью команды главного меню Выполнить | ″C:\Program Files\Citadel Data Security\Citadel Safstor\csenc″ полный путь к шифруемому файлу (кавычки обязательны). Для расшифрования файла следует в этом случае использовать команду Выполнить | ″C:\Program Files\Citadel Data Security\Citadel Safstor\csdec″ полный путь к зашифрованному файлу с расширением .css (кавычки обязательны). Еще один способ выполнения шифрования или расшифрования файлов – «перетаскивание» их значков на значки программ csenc или csdec соответственно; · другие пользователи программы Citadel Safstor после ее установки могут быть созданы с помощью функции Citadel Safstor Панели управления (вкладка User Profiles, кнопка New User); · «переключение» на другого пользователя программы Citadel Safstor производится также с помощью Панели управления (функция Citadel Safstor, вкладка Current User). Если пункт выполняется в операционной системе Windows 7 или старше. Скопировать в произвольную папку на локальном жестком диске файл VeraCrypt Setup 1.17.exe. 1.1. Если программа VeraCrypt не установлена (отсутствует соответствующий пункт в главном меню), выполнить установку программы VeraCrypt,

согласившись со всеми параметрами установки по умолчанию. 1.2. Для русификации интерфейса программы выполнить после ее первого запуска команду меню Settings | Language | Русский. 1.3. На примере работы с произвольными (несистемными) файлами различного типа изучить функции программы шифрования VeraCrypt, учитывая, что: · перед шифрованием файлов необходимо создать том (зашифрованный файловый контейнер) с помощью кнопки «Создать том» и мастера создания томов VeraCrypt: выбрать тип тома – обычный том VeraCrypt, выбрать размещение тома (файл с произвольным именем в любой доступной папке на любом диске), выбрать алгоритмы шифрования и хеширования (любые из доступных в программе), выбрать размер тома (рекомендуется 10 МБ), ввести и подтвердить пароль тома (для генерации ключа его шифрования), выполнить форматирование тома (потребуется хаотичное перемещение курсора мыши внутри окна мастера); · выбрать незанятое имя (букву) для созданного тома и смонтировать его с помощью кнопки «Смонтировать», после чего ввести заданный при создании тома пароль; · с помощью команды «Открыть» контекстного меню имени (буквы) смонтированного тома открыть его в Проводнике, после чего добавить в него несколько файлов разного типа (один из них должен иметь имя, включающее фамилию студента); · размонтировать том с помощью соответствующей кнопки, после чего снова смонтировать и убедиться в наличии в нем добавленных ранее файлов. При выполнении в любой операционной системе. 1.4. Включить в электронную версию отчета о лабораторной работе копии экранных форм, полученных при использовании программы Citadel Safstor (VeraCrypt), после чего завершить работу с ней. Включить в отчет ответы на вопросы: · какие криптоалгоритмы реализованы в использованной программе (назвать имя и тип алгоритмов); · как генерируется и сохраняется ключ шифрования файла; · изменяется ли (если да, то как) размер файла после шифрования; · возможен ли (если да, то как) совместный доступ к зашифрованному файлу); · какие действия выполняет пользователь при установке программы. 2. Данный пункт выполняется на дисках, использующих файловую систему NTFS. На примере папок и файлов из папки Мои документы освоить средства обеспечения конфиденциальности информационных ресурсов с помощью шифрующей файловой системы (команда Свойства контекстного меню объекта, вкладка Общие, кнопка Другие, выключатель Шифровать содержимое для защиты данных). Включить в отчет ответы на вопросы: 2.1. скрывается ли наличие в системе зашифрованных файлов и папок; 2.2. где хранится ключ шифрования файла; 2.3. как обеспечивается в системе возможность восстановления зашифрованных файлов при невозможности входа пользователя в систему или при его отсутствии; 2.4. на дисках с какой файловой системой возможно использование функции шифрования файлов. 2.5. Освоить средства обеспечения совместного доступа нескольких пользователей к зашифрованным файлам (с помощью кнопки Подробно окна его дополнительных атрибутов) и включить в отчет сведения о порядке использования этих средств и ответ на вопрос, среди каких пользователей возможен выбор тех, кому будет разрешен доступ к зашифрованному файлу. 2.6. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 3. Начать работу с Microsoft Word из пакета Microsoft Office (версии XP или старше). Освоить средства шифрования конфиденциальных документов (команды Файл | Сведения | Защита документа | Зашифровать с использованием пароля в Office 2013, Файл | Сведения | Защитить документ | Зашифровать паролем в Office 2010, Кнопка Microsoft Office | Подготовка | Зашифровать документ в Office 2007, Сервис | Параметры | Безопасность и кнопка Дополнительно в Office 2003). Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 4. Повторить п. 3 для программы Microsoft Excel. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 5. С помощью программы selfcert.exe из пакета Microsoft Office (вызов этой программы возможен через меню Пуск | Программы | Средства

Microsoft Office | Средство создания цифровых сертификатов для проектов VBA) создать собственную пару ключей асимметричного шифрования и «самоподписанный» сертификат своего открытого ключа на имя, содержащее фамилию и инициалы студента. Если эта программа не установлена или создание сертификатов невозможно в соответствии с выбранной в системе политики безопасности, то создать самоподписанный сертификат с помощью утилиты makecert (makecert /r /n "cn=Фамилия И.О." /ss my), для вызова которой использовать командную строку Пуск | Программы | Microsoft Visual Studio | Visual Studio Tools | Visual Studio Command Prompt). Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 6. Освоить средства добавления электронной подписи к документам Microsoft Office на примере программы Microsoft Word (команды Файл | Сведения | Защита документа | Добавить цифровую подпись в Office 2013, Файл | Сведения | Защитить документ | Добавить цифровую подпись в Office 2010, Кнопка Microsoft Office | Подготовка | Добавить цифровую подпись в Office 2007, Сервис | Параметры | Безопасность, кнопки Цифровые подписи и Добавить). С помощью кнопки Просмотреть свойства сертификата ознакомиться с содержанием сертификата открытого ключа. Включить в отчет ответы на вопросы: 6.1. какая информация содержится в сертификате открытого ключа; 6.2. что такое путь сертификации. 6.3. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 7. Этот пункт выполняется в виртуальной машине Windows XP или с правами администратора. Если пункт выполняется в операционной системе Windows XP. Скопировать в произвольную папку на локальном жестком диске файл contrabd.zip и извлечь файлы из этого архива. 7.1. Если программа Contraband не установлена (отсутствует соответствующий пункт в главном меню), то запустить программу setup.exe для установки стеганографической программы Contraband. 7.2. Запустить стеганографическую программу contrab.exe. С произвольными файлами контейнеров (в формате полноцветных 24-битных изображений в формате BMP) и сообщений изучить функции программы и включить в электронную версию отчета копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней. Если пункт выполняется в операционной системе Windows 7 или старше. Скопировать в произвольную папку на локальном жестком диске файл QS12Setup.zip и извлечь файлы из этого архива. 7.1. Если программа QuickStego не установлена (отсутствует соответствующий пункт в главном меню), то запустить программу QS12Setup.exe для установки стеганографической программы QuickStego. 7.2. Запустить стеганографическую программу QuickStego. С произвольными файлами контейнеров (изображений) и сообщений (текстовых файлов, которые можно выбирать или создавать непосредственно в окне программы) изучить функции программы и включить в электронную версию отчета копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней. При выполнении в любой операционной системе. 7.3. Включить в отчет ответы на вопросы: · как происходит скрытие и извлечение сообщений из контейнеров; · в чем разница между методами криптографии и стеганографии; · каким должно быть соотношение между размерами файла-контейнера и файласообщения при использовании программы contrab.exe (QuickStego) и почему. 8. Запустить установленную в системе программу антивирусного сканирования и освоить работу с ней. Включить в электронную версию отчета о выполнении лабораторной работы копии экранных форм, полученных при использовании этой программы. Включить в отчет о лабораторной работе 8.1. сведения о назначении и основных функциях программы, а также ответы на вопросы: 8.2. как задаются области сканирования (диски, папки и т.п.); 8.3. как задаются объекты проверки на наличие вирусов (типы сканируемых файлов); 8.4. как определяется реакция сканера в случае обнаружения зараженного файла. Завершить работу с программой. 9. Начать работу с Microsoft Word. Включить средства защиты от вирусов в макросах в документах Word

(команды Файл или кнопка Microsoft Office | Параметры | Центр управления безопасностью | Параметры центра правления безопасностью | Параметры макросов в Office 2013, 2010 или 2007, Сервис | Параметры | Безопасность в Office 2003). Завершить работу с Word. 9.1. Включить в отчет сведения о способах защиты от вредоносных макросов в документах Word. 9.2. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 10. Повторить п. 9 для программы Microsoft Excel. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 11. Освоить средства добавления электронной подписи к макросам, включаемым в состав документов Microsoft Office (на примере программы Microsoft Word): добавить в документ автоматически выполняющийся макрос (команды Вид | Макросы | Макросы в Office 2013, 2010 и 2007, Сервис | Макрос | Макросы в Office 2003) и воспользоваться командой Редактора Visual Basic for Application Tools | Digital Signature. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта. 12. Включить в отчет титульный лист и сохранить файл с электронной версией отчета в произвольной папке на локальном жестком диске. 13. Выслать преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания. 14. После проверки электронной версии отчета о выполнении лабораторной работы преподавателем включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта и прилагаемой ниже таблицей. 15. Выслать преподавателю для защиты лабораторной работы документ, содержащий ответы на контрольные вопросы

Контрольные вопросы/задания:

Уметь: анализировать, выбирать и применять методы и средства защиты от вредоносных программ	1.Покажите разницу между симметричной и асимметричной криптографией 2.Продемонстрируйте как происходит генерация ключа шифрования при установке программы Citadel Safstor (VeraCrypt) 3.Оцените для решения каких задач защиты информации в первую очередь применяются асимметричные криптосистемы 4.Укажите для чего могут применяться методы компьютерной стеганографии 5.Продемонстрируйте как добавить электронную подпись к макросу в документе Microsoft Office

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-5. Вредоносные программы

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Технология проверки связана с выполнением контрольного теста по изученной теме. Время, отведенное на выполнение

задания, устанавливается не более 30 минут. Количество попыток не более 3-х. Тестирование проводится с использованием СДО "Прометей". К тестированию допускается пользователь, изучивший материалы, авторизованный уникальным логином и паролем

Краткое содержание задания:

Контрольная точка направлена на проверку знаний по защите от вредоносных программ и несанкционированного копирования информационных ресурсов

Контрольные вопросы/задания:

Знать: способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем	1.**Основные угрозы доступности информации:** 1.Непреднамеренные ошибки пользователей 2.злонамеренное изменение данных 3.хакерская атака 4.отказ программного и аппаратного обеспечения 5.разрушение или повреждение помещений 6.перехват данных **Ответ: 1;4;5** 2.**Суть компрометации информации:** 1.Внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации 2.Несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений 3.Внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений **Ответ: 3** 3.**Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она:** 1.С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды 2.С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации 3.Способна противостоять только информационным угрозам, как внешним так и внутренним 4.Способна противостоять только внешним информационным угрозам **Ответ: 1** 4.**Методы повышения достоверности входных данных:** 1.Замена процесса ввода значения процессом выбора значения из предлагаемого множества 2.Отказ от использования данных

	3.Проведение комплекса регламентных работ 4.Использование вместо ввода значения его считывание с машиночитаемого носителя 5.Введение избыточности в документ первоисточник 6.Многократный ввод данных и сличение введенных значений **Ответ: 1;4;5** 5.**Под угрозой удаленного администрирования в компьютерной сети понимается угроза:** 1.Несанкционированного управления удаленным компьютером 2.Внедрения агрессивного программного кода в рамках активных объектов Web-страниц 3.Перехвата или подмены данных на путях транспортировки 4.Вмешательства в личную жизнь 5.Поставки неприемлемого содержания **Ответ: 1** 6.**Наиболее эффективное средство для защиты от сетевых атак:** 1.Использование сетевых экранов или «firewall» 2.Использование антивирусных программ 3.Посещение только «надёжных» Интернет-узлов 4.Использование только сертифицированных программ-браузеров при доступе к сети Интернет **Ответ: 1** 7.**Информация, составляющая государственную тайну не может иметь гриф:** 1.«Для служебного пользования» 2.«Секретно» 3.«Совершенно секретно» 4.«Особой важности» **Ответ: 1** 8.**Средства защиты объектов файловой системы основаны на:** 1.Определении прав пользователя на операции с файлами и каталогами 2.Задании атрибутов файлов и каталогов, независящих от прав пользователей **Ответ: 1** 9.**Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование — … угроза:** 1.Активная 2.Пассивная **Ответ: 2** 10.**Концепция системы защиты от информационного оружия не должна включать:** 1.Средства нанесения контратаки с помощью информационного оружия

	2.Механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры 3.Признаки, сигнализирующие о возможном нападении 4.Процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей **Ответ: 1**

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

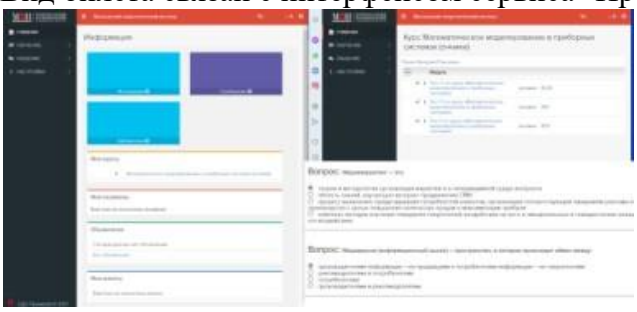
СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

Вид билета связан с интерфейсом сервиса "Прометей"



Процедура проведения

В тесте 20 вопросов встречаются вопросы следующих типов: 1. с одним вариантом ответа (в вопросах «один из многих», система сравнивает ответ слушателя с правильным ответом и автоматически выставляет за него назначенный балл) 2. с выбором нескольких вариантов ответов (в вопросах «многие из многих» система оценивает каждый ответ отдельно; есть возможность разрешить слушателю получить за вопрос 0,75 балла, если он выберет 3 правильных ответа из 4) 3. на соответствие слушатель должен привести в соответствие левую и правую часть ответа (в вопросах «соответствие» система оценивает каждый ответ отдельно; можно разрешить слушателю получить за вопрос 0,75 балла, если он выберет 3 правильных ответа из 4) 4. развернутый ответ, вводится в вручную в специально отведенное поле (ручная оценка преподавателем)

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ОПК-8(Компетенция)

Вопросы, задания

1.Биометрическая аутентификация
2.Политика безопасности на предприятии
3.Требованиям уровня безопасности С2, в соответствии с “оранжевой книгой”
4.Основные правила при мандатном управлении доступом
5.Аудит событий безопасности в компьютерной системе

Материалы для проверки остаточных знаний

1.**Что не относится к недостаткам программных средств защиты информации?**

Ответы:

1. Снижение эффективности работы компьютерных систем 2. Возможность “обхода” механизма защиты 3. Сложность тиражирования 4. Возможность злоумышленного изменения в ходе эксплуатации

Верный ответ: 3

2.**Что означает термин “аутентификация”?**

Ответы:

1. Проверка регистрации в базе данных 2. Подтверждение подлинности 3. Ограничение прав 4. Учет и регистрация событий

Верный ответ: 2

3.**Какие методы и средства защиты информации являются обязательными в любой системе защиты?**

Ответы:

1. Криптографические 2. Программно-аппаратные 3. Инженерно-технические 4. Организационные

Верный ответ: 4

4.**Что не относится к способам аутентификации пользователей, основанных на общем секрете?**

Ответы:

1. Использование смарт-карт 2. Парольная аутентификация 3. Модель рукопожатия 4. Запрос-отклик

Верный ответ: 1

5.**Как должны храниться пароли в базе учетных записей?**

Ответы:

1. В открытом виде 2. В зашифрованном виде 3. В хешированном виде 4. Защищенные помехоустойчивым кодом

Верный ответ: 3

2. Компетенция/Индикатор: ОПК-9(Компетенция)

Вопросы, задания

1.Программно-аппаратная защита от локального несанкционированного доступа (работа так называемого «электронного замка»)

2.Недостаток дискреционного управления доступом к объектам

3.Построении идеального шифра (по К. Шеннону)

4.Модель разграничения доступа к объектам в ОС Windows

5.LSB

Материалы для проверки остаточных знаний

1.**Что понимается под затенением файла с паролями пользователей?**

Ответы:

1. Перенос на защищенный от несанкционированного чтения носитель 2. Замена * символов паролей 3. Запрет доступа к файлу для непривилегированных пользователей 4. Запрет доступа к файлу для любых процессов

Верный ответ: 3

2.**Зачем в учетной записи пользователя может храниться случайное значение?**

Ответы:

1. Для увеличения стойкости функции хеширования 2. Для упрощения администрирования 3. Чтобы нельзя было восстановить пароль 4. Для исключения возможности установления факта совпадения паролей пользователей с разными правами

Верный ответ: 4

3.**Что такое модель “рукопожатия”?**

Ответы:

1. Аутентификация пользователя, основанная на знании им правила выработки ответа на случайный запрос 2. Аутентификация пользователя, основанная на одноразовых паролях 3. Аутентификация пользователя, основанная на биометрии 4. Аутентификация пользователя, основанная на применении элементов аппаратного обеспечения

Верный ответ: 1

4.**Что является основным критерием при выборе элемента аппаратного обеспечения для аутентификации пользователей?**

Ответы:

1. Стоимость изготовления 2. Сложность копирования 3. Скорость считывания ключевой информации 4. Объем памяти и наличие микропроцессора

Верный ответ: 2

5.**Что не может использоваться при биометрической аутентификации?**

Ответы:

1. Тембр голоса 2. Геометрическая форма руки 3. Отпечатки пальцев 4. Температура тела 5. Все указанные параметры могут использоваться

Верный ответ: 4

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 80

Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и аттестационной составляющих.