Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный авиационный технический университет»
Уфимский авиационный техникум

УТВЕРЖДАЮ
Проректор по учебной работе
А.Н. Елизарьев
«17» 06 2020г.

Рабочая программа учебной дисциплины

ОП.14 Информационная безопасность

Наименование специальности

09.02.05 Прикладная информатика (по отраслям)

Квалификация выпускника

Техник-программист

Базовая подготовка
Форма обучения: очная

Уфа, 2020

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.05 Прикладная информатика (по отраслям), утверждённого приказом Министерства образования и науки Российской Федерации от 13.08.2014 №1001.

Организация-разработчик: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» Уфимский авиационный техникум.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена (далее – ППССЗ) в соответствии с ФГОС по специальности СПО 09.02.05 Прикладная информатика (по отраслям).

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена:

Дисциплина входит в вариативную часть цикла общепрофессиональных дисциплин ППССЗ по специальности среднего профессионального образования 09.02.05 Прикладная информатика (по отраслям).

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен уметь:

- создавать и удалять учетные записи;
- применять программный продукт Advanced Archive Password Recover для снятия парольной защиты с архивов WinZip и WinRAR;
- применять программные средства защиты от несанкционированного доступа;
- применять методы шифрования и дешифрования с симметричными ключами.

В результате освоения дисциплины обучающийся должен знать:

- основные понятия и определения информационной безопасности;
- источники и содержание основных угроз информационной безопасности;
- способы защиты от несанкционированного доступа и основные принципы защиты информации;
- модели обеспечения информационной безопасности;
- криптографические методы и средства обеспечения ИБ;
- проблемы вирусного заражения программ, структуру современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты;
- технические каналы утечки информации.

Техник-программист должен обладать общими компетенциями, включающими в себя способность:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Техник-программист должен обладать профессиональными компетенциями, соответствующими видам деятельности:

ПК 1.1. Обрабатывать статический информационный контент.

ПК 1.2. Обрабатывать динамический информационный контент.

ПК 1.3.Осуществлять подготовку оборудования к работе.

ПК 2.1. Осуществлять сбор и анализ информации для определения потребностей клиента.

ПК 3.2. Осуществлять продвижение и презентацию программного обеспечения отраслевой направленности.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 77часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 55часов;

самостоятельной работы обучающегося 22 часа;

консультаций 4 часа.

.

2. СТРУКТУРА ИСОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***	
	7 семестр	***8 семестр***
Максимальная учебная нагрузка (всего)	*28*	*46*
Обязательная аудиторная учебная нагрузка (всего)	*32*	*20*
в том числе:		
лабораторные занятия	-	*10*
практические занятия	-	-
курсовая работа (проект)	-	-
Самостоятельная работа обучающегося (всего)	-	*18*
в том числе:		
самостоятельная работа над курсовой работой (проектом) *(если предусмотрено)*	-	-
Домашняя работа: 1. Шифры простой замены: (полибианский квадрат, шифр Цезаря, шифрующие таблицы Трисемуса) 2. Шифры сложной замены (шифр Гронсфельда, шифр «двойной квадрат» Уинстона, шифрование методом Вернама)	*9* *9*	
Консультации	*2*	*2*
Итоговая аттестация	*Другие формы контроля*	*Дифференцированный зачет*

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) (если предусмотрены)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1 Основные понятия и определения информационной безопасности. Эволюция подходов к обеспечению информационной безопасности		**4**	
Тема 1.1 Информационная безопасность. Основные понятия и определения. Эволюция подходов к обеспечению информационной безопасности	Содержание учебного материала.	4	
	1 Введение в предмет. Основные понятия и определения информационной безопасности		1
	2 Эволюция подходов к обеспечению информационной безопасности		1
Раздел 2 Угрозы безопасности информации		**4**	
Тема 2.1 Угрозы безопасности информации	Содержание учебного материала	4	
	1 Источники и содержание основных угроз информационной безопасности России		1
	2 Информационные, программно-математические, физические и организационные угрозы		1
Раздел 3 Защита от несанкционированного доступа и основные принципы защиты информации		**14**	

Тема 3.1 Защита от несанкционированного доступа и основные принципы защиты информации	Содержание учебного материала		6	
	1	Защита информации. Методы и средства защиты процессов переработки информации		1
	2	Защита от несанкционированного доступа		2
	3	Идентификация и аутентификация. Основные понятия		2
	Лабораторные занятия		6	
	1	Создание и управление учетными записями пользователя. Настройка пароля		
	2	Изучение программных средств защиты от несанкционированного доступа		
	3	Защита информации с помощью пароля		
	Консультации		**2**	
Раздел 4 Модели обеспечения информационной безопасности			**4**	
Тема 4.1 Модели обеспечения информационной безопасности	Содержание учебного материала		4	
	1	Модели безопасности по разграничению доступа в систему		1
	2	Модели контроля целостности информации в системе, модели защиты при отказе в обслуживании, модели анализа безопасности программного обеспечения		1
Раздел 5 Криптографические методы и средства обеспечения ИБ			**30**	
Тема 5.1 Криптографические методы и средства обеспечения ИБ	Содержание учебного материала		8	
	1	История криптографической деятельности. Основные понятия, определения и композиции шифров		1
	2	Методы шифрования с симметричными ключами: шифрование методами замены (подстановки)		2
	3	Методы шифрования с симметричными ключами: шифрование с симметричными ключами методами перестановки, шифрование с симметричными ключами при помощи аналитических преобразований		2
	4	Методы шифрования с симметричными ключами: шифрование аддитивными методами (гаммирование), комбинированные методы шифрования с симметричными ключами. Системы с открытыми ключами		2
	Лабораторные занятия		4	
	1	Криптографические методы защиты информации		
	2	Криптографические методы защиты информации		

	Самостоятельная работа Шифры простой замены (полибианский квадрат, шифр Цезаря, шифрующие таблицы Трисемуса) Шифры сложной замены (шифр Гронсфельда, шифр «двойной квадрат» Уинстона, шифрование методом Вернама)		18	
Раздел 6 Проблемы вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты			**8**	
Тема 6.1 Проблемы вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты	Содержание учебного материала		8	
	1	Компьютерные вирусы. Проблемы вирусного заражения программ		1
	2	Основные классы антивирусных программ		1
	3	Методы антивирусной защиты		1
	4	Структура современных антивирусных программ		1
Раздел 7 Защита от утечки информации по техническим каналам			**4**	
Тема 7.1 Защита от утечки информации по техническим каналам	Содержание учебного материала		4	
	1	Общие понятия. Оптические и акустические каналы утечки информации		1
	2	Защита от утечки за счет электромагнитного излучения		1
Раздел 8 Организационно-			**2**	

правовое обеспечение информационной безопасности			
Тема 8.1 Организационно-правовое обеспечение информационной безопасности	Содержание учебного материала	2	
	1 Отечественные и зарубежные стандарты в области информационной безопасности Охрана персональных данных. Охрана интеллектуальной собственности		1
	Дифференцированный зачет	**2**	
	Консультации	**2**	
	Всего:	**74**	

2.3 Методические указания к лабораторным занятиям

Лабораторное занятие 1
Создание и управление учетными записями пользователя. Настройка пароля

I. Цель занятия:

Научиться создавать и управлять учетными записями пользователя, устанавливать ограничение доступа к ПК.

II. Задание:

1. Ознакомьтесь с дополнением к практическому занятию 1.
2. Создайте учетные записи пользователей: «Старший брат» и «Младшая сестра». Примените уникальный рисунок к каждой учетной записи.
3. Включите в отчет копии экранных форм.
4. Создайте пароль «**654321**» для пользователя «Старший брат» и пароль «**123456**» для пользователя «Младшая сестра».
5. Выберите новые рисунки для ваших учетных записей.
6. Включите в отчет копии экранных форм.
7. Войдите в систему под каждым пользователем для проверки правильности пароля и для создания папок профилей пользователей на диске (Папка профиля – это папка в «C:\Пользователи\...»).
8. Включите в отчет копии экранных форм.
9. Измените доступ к профилям так, чтобы пользователь «Старший брат» смог просматривать профиль пользователя «Младшая сестра», а наоборот нет.
10. Настройте защиту компьютера на время отсутствия пользователя на рабочем месте таким образом, чтобы можно было предотвратить доступ пользователей, не прошедших проверку, на компьютер.
11. Результат покажите преподавателю.
12. Удалите защиту.
13. Удалите созданные учетные записи.

III. Содержание отчета:

Отчет должен содержать:
- название и цель занятия;
- копии экранных форм.

IV. Контрольные вопросы:

1. Чем отличается учетная запись *Администратор* по умолчанию от любой другой учетной записи, входящей в группу *Администраторы*?
2. Какой длины может быть пароль?
3. Какими правами обладает пользователь?

V. Литература:

1. Шаньгин В. Ф. Информационная безопасность [Электронный ресурс]: / Шаньгин В.Ф. - Москва: ДМК Пресс, 2014 http://e.lanbook.com/books/element.php?pl1_id=50578

2. Мельников Д. А. Информационная безопасность открытых систем [Электронный ресурс]: / Мельников Д.А. - Москва: ФЛИНТА, 2014 http://e.lanbook.com/books/element.php?pl1_id=48368

Дополнение
Создание учетных записей

Учётная запись пользователя – это запись, которая содержит сведения, необходимые для идентификации пользователя при подключении к системе, а также информацию для авторизации и учёта. Это имя пользователя и пароль (или другое аналогичное средство аутентификации — например, биометрические характеристики). Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде (в целях его безопасности).

Для повышения надёжности наряду с паролем могут быть предусмотрены альтернативные средства аутентификации — например, специальный секретный вопрос (или несколько вопросов) такого содержания, что ответ может быть известен только пользователю. Такие вопросы и ответы также хранятся в учётной записи.

Учётная запись может содержать следующие дополнительные анкетные данные о пользователе:

- имя;
- фамилию;
- отчество;
- псевдоним (ник);
- пол;
- национальность;
- расовую принадлежность;
- вероисповедание
- группу крови;
- резус-фактор;
- возраст;
- дату рождения;
- адрес электронной почты;
- домашний адрес;
- рабочий адрес;
- номер домашнего телефона;
- номер рабочего телефона;
- номер мобильного телефона;
- номер ICQ;
- идентификатор Skype, ник в IRC;
- другие контактные данные систем обмена мгновенными сообщениями;
- адрес домашней страницы и/или блога в Интернете или интранете;
- сведения о хобби;
- сведения о круге интересов;
- сведения о семье;
- сведения о перенесённых болезнях;
- и многое другое.

Конкретные категории данных, которые могут быть внесены в такую анкету, определяются администраторами системы.

Учётная запись может также содержать одну или несколько фотографий пользователя, учитывать различные статистические характеристики поведения пользователя в системе: давность последнего входа в систему, продолжительность

последнего пребывания в системе, адрес использованного при подключении компьютера, интенсивность использования системы и так далее.

Обычная учетная запись или Администратор?

Перед тем, как начать создавать новые учетные записи, важно понять разницу между двумя типами аккаунтов (**Аккаунт (account)** в переводе с английского означает «учетная запись» и представляет собой набор данных о пользователе, которые тот вводит и хранит на каком-либо сайте или интернет-сервисе):

- *Обычный доступ*: Учетные записи с обычным доступом подходят для нормальной ежедневной работы. Пользователь с таким доступом может выполнять рядовые задачи, например, запускать программы или изменять настройки персонализации рабочего стола. Также, на такие аккаунты можно настроить родительский контроль.
- *Администратор*: Учетные записи с правами *Администратора* используются для внесения изменений в настройки системы и управление учетными записями пользователей. Они обладают полным доступом ко всем настройкам компьютера. На каждом компьютере есть, по крайней мере, одна учетная запись типа *Администратор*.

Таким образом, видно, что учетная запись *Администратора* обладает большими возможностями. Но, в тоже время, учетные записи с обычным доступом безопаснее, поэтому лучше использовать их для решения каждодневных задач.

Создание учетных записей пользователей

В операционной системе Windows 7 можно создавать несколькими способами как учетные записи пользователей для компьютеров, состоящих в рабочих группах, так и учетные записи пользователей для компьютеров, которые входят в состав домена. Домены, рабочие группы и домашние группы представляют разные методы организации компьютеров в сети. Основное их различие состоит в том, как осуществляется управление компьютерами и другими ресурсами.

Рабочая группа – это группа компьютеров, подключенных к сети, которые совместно используют ресурсы. При настройке сети операционная система Windows автоматически создает рабочую группу и присваивает ей имя по умолчанию.

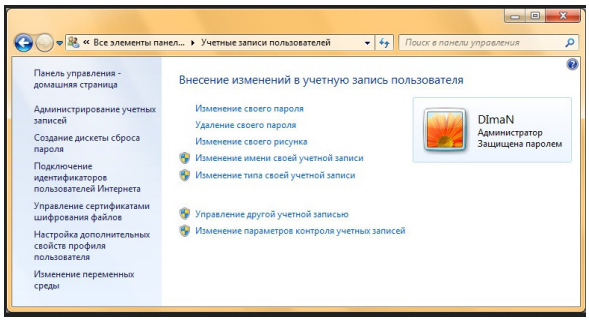
Домен — это группа компьютеров одной сети, имеющих единый центр, использующий единую базу пользователей, единую групповую и локальную политики, единые параметры безопасности, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров.

Создание учетных записей пользователей для компьютеров, состоящих в рабочей группе

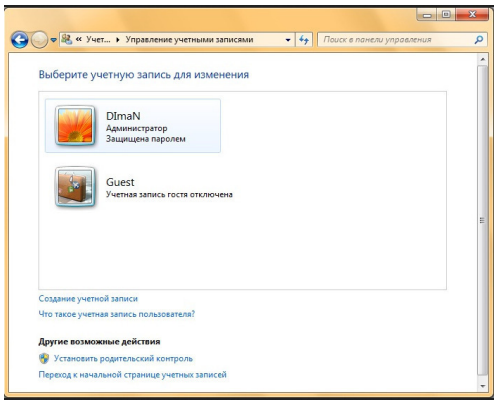
В операционной системе Windows 7 для компьютеров, которые состоят в рабочей или домашней группе, учетные записи можно создавать следующими способами:

Создание учетной записи при помощи диалога «Управление учетными записями пользователей»:

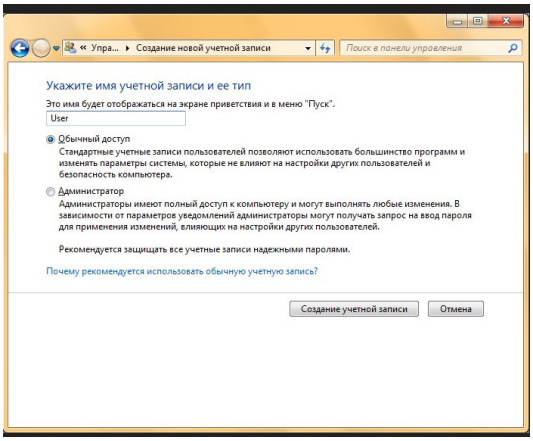
1. Нажмите на кнопку «Пуск» для открытия меню, откройте «Панель управления» и из списка компонентов панели управления выберите «Учетные записи пользователей»:



2. В диалоге «Учетные записи пользователей» перейдите по ссылке «Управление другой учетной записью», затем нажмите на «Создание учетной записью»:



3. Введите имя для учетной записи, выберите тип учетной записи и нажмите на кнопку «Создание учетной записи»:

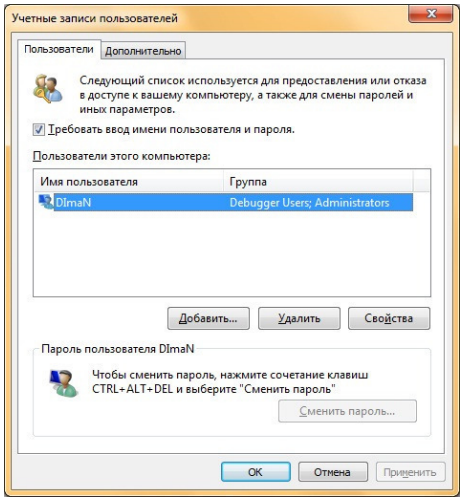


4. Имя пользователя не должно совпадать с любым другим именем пользователя или группы на данном компьютере. Оно может содержать до 20 символов верхнего или нижнего регистров, за исключением следующих: " / \ [ ] : ; | = , + * ? <> @, а также имя пользователя не может состоять только из точек и пробелов.
5. В этом диалоге можно выбрать одну из двух типов учетных записей: «обычные учетные записи пользователей», которые предназначены для повседневной работы или «учетные записи администратора», которые предоставляют полный контроль над компьютером и применяются только в необходимых случаях.

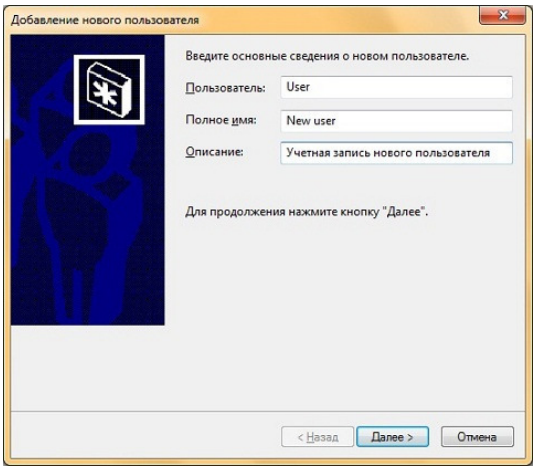
Создание учетной записи при помощи диалога «Учетные записи пользователей»:

Доступный через панель управления диалог «Управление учетными записями пользователей» имеет очень серьезное ограничение: оно предлагает на выбор только учетные записи типа *Обычный доступ* или *Администратор*. Для того чтобы при создании нового пользователя его можно было поместить в какую-либо определенную группу, нужно сделать следующее:

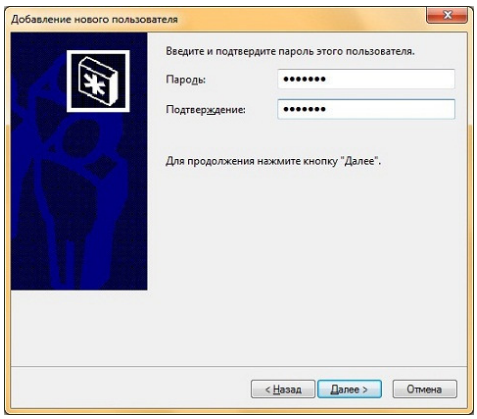
1. Воспользоваться комбинацией клавиш +R для открытия диалога «Выполнить»;
2. В диалоговом окне «Выполнить», в поле «Открыть» введите *control* userpasswords2 и нажмите на кнопку «ОК»:



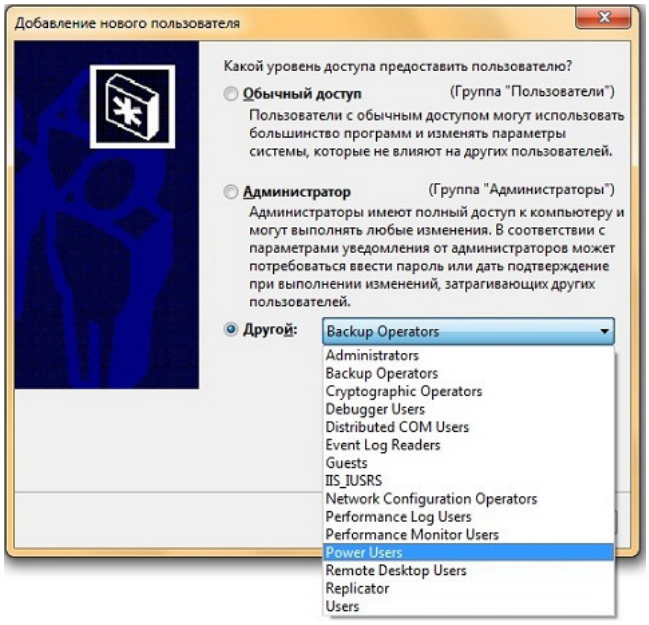
3. В диалоговом окне «Учетные записи пользователей» нажмите на кнопку «Добавить» для запуска мастера добавления нового пользователя:



4. В появившемся диалоговом окне «Добавление нового пользователя» введите имя пользователя. Поля «Полное имя» и «Описание» не являются обязательными, то есть их можно заполнять при желании. Нажмите на кнопку «Далее»:



5. В диалоге «Введите и подтвердите пароль этого пользователя» введите пароль для данной учетной записи, а затем продублируйте его в поле «Подтверждение», после чего нажмите на кнопку «Далее»:



6. Это последний диалог мастера добавления нового пользователя. Здесь необходимо установить переключатель, определяющий группу безопасности, к которой должна относиться данная учетная запись пользователя. Можно выбрать одну из следующих групп: *Обычный доступ*, *Администратор* или *Другой*. Последний переключатель стоит использовать в том случае, если нужно отнести пользователя к какой-то другой группе, созданной по умолчанию в операционной системе Windows 7.
7. В следующем списке перечислены 15 встроенных групп операционной системы Windows 7. Эти права назначаются в рамках локальных политик безопасности:
   - Administrators (*Администраторы*). Пользователи, входящие в эту группу, имеют полный доступ на управление компьютером и могут при необходимости назначать пользователям права пользователей и разрешения на управление доступом. По умолчанию членом этой группы является учетная запись администратора. Если компьютер подключен к домену, группа «Администраторы домена» автоматически добавляется в группу «Администраторы». Эта группа имеет полный доступ к управлению компьютером, поэтому необходимо проявлять осторожность при добавлении пользователей в данную группу;

- Backup Operators (*Операторы архива*). Пользователи, входящие в эту группу, могут архивировать и восстанавливать файлы на компьютере независимо от любых разрешений, которыми защищены эти файлы. Это обусловлено тем, что право выполнения архивации получает приоритет над всеми разрешениями. Члены этой группы не могут изменять параметры безопасности.
- Cryptographic Operators (*Операторы криптографии*). Членам этой группы разрешено выполнение операций криптографии.
- Debugger Users (*Группа удаленных помощников*). Члены этой группы могут предлагать удаленную помощь пользователям данного компьютера.
- Distributed COM Users (*Пользователи DCOM*). Членам этой группы разрешено запускать, активировать и использовать объекты DCOM на компьютере.
- Event LogReaders (*Читатели журнала событий*). Членам этой группы разрешается запускать журнал событий Windows.
- Guests (*Гости*). Пользователи, входящие в эту группу, получают временный профиль, который создается при входе пользователя в систему и удаляется при выходе из нее. Учетная запись «Гость» (отключенная по умолчанию) также является членом данной встроенной группы.
- IIS_IUSRS. Это *встроенная группа, используемая службами IIS*.
- Network Configuration Operators (*Операторы настройки сети*). Пользователи, входящие в эту группу, могут изменять параметры TCP/IP, а также обновлять и освобождать адреса TCP/IP. Эта группа не имеет членов по умолчанию.
- Performance LogUsers (*Пользователи журналов производительности*). Пользователи, входящие в эту группу, могут управлять счетчиками производительности, журналами и оповещениями на локальном или удаленном компьютере, не являясь при этом членами группы «Администраторы».
- Performance Monitor Users (*Пользователи системного монитора*). Пользователи, входящие в эту группу, могут наблюдать за счетчиками производительности на локальном или удаленном компьютере, не являясь при этом участниками групп «Администраторы» или «Пользователи журналов производительности».
- Power Users (*Опытные пользователи*). По умолчанию, члены этой группы имеют те же права пользователя и разрешения, что и учетные записи обычных пользователей. В предыдущих версиях операционной системы Windows эта группа была создана для того, чтобы назначать пользователям особые административные права и разрешения для выполнения распространенных системных задач. В этой версии операционной системы Windows учетные записи обычных пользователей предусматривают возможность выполнения большинства типовых задач настройки, таких как смена часовых поясов. Для старых приложений, требующих тех же прав опытных пользователей, которые имелись в предыдущих версиях операционной системы Windows, администраторы могут применять шаблон безопасности, который позволяет группе «Опытные пользователи» присваивать эти права и разрешения, как это было в предыдущих версиях операционной системы Windows.
- Remote Desktop Users (*Пользователи удаленного рабочего стола*). Пользователи, входящие в эту группу, имеют право удаленного входа на компьютер.
- Replicator (*Репликатор*). Эта группа поддерживает функции репликации. Единственный член этой группы должен иметь учетную запись пользователя домена, которая используется для входа в систему службы репликации контроллера домена. Не добавляйте в эту группу учетные записи реальных пользователей.

- Users (*Пользователи*). Пользователи, входящие в эту группу, могут выполнять типовые задачи, такие как запуск приложений, использование локальных и сетевых принтеров и блокировку компьютера. Члены этой группы не могут предоставлять общий доступ к папкам или создавать локальные принтеры. По умолчанию членами этой группы являются группы «Пользователи домена», «Проверенные пользователи» и «Интерактивные». Таким образом, любая учетная запись пользователя, созданная в домене, становится членом этой группы.

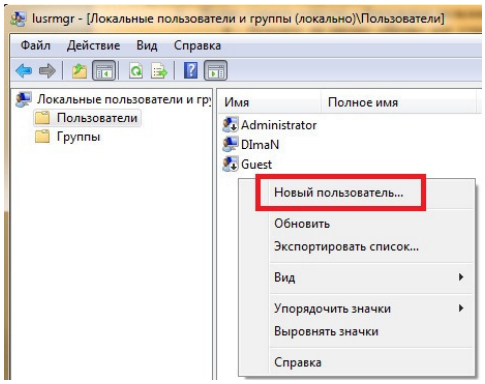
Создание учетной записи при помощи оснастки «Локальные пользователи и группы»

Оснастка «Локальные пользователи и группы» расположена в компоненте «Управление компьютером», представляющем собой набор средств администрирования, с помощью которых можно управлять одним компьютером, локальным или удаленным. Оснастка «Локальные пользователи и группы» служит для защиты и управления учетными записями пользователей и групп, размещенных локально на компьютере. Можно назначать разрешения и права для учетной записи локального пользователя или группы на определенном компьютере (и только на этом компьютере).

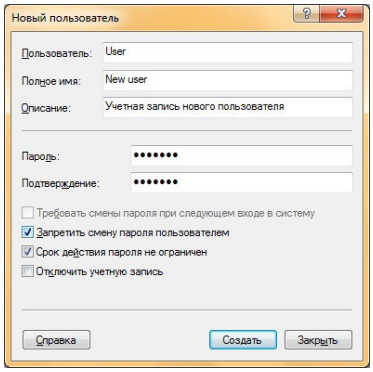
Использование оснастки «Локальные пользователи и группы» позволяет ограничить возможные действия пользователей и групп путем назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (обычно с файлом, папкой или принтером), которое определяет, каким пользователям, и какой доступ к объекту разрешен.

Для того чтобы создать локальную учетную запись пользователя при помощи оснастки «Локальные пользователи и группы», нужно сделать следующее:

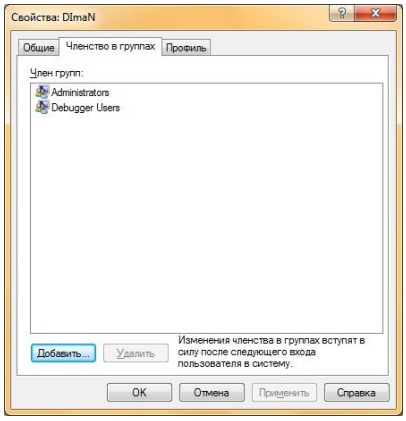
1. Откройте оснастку «Локальные пользователи и группы» одним из следующих способов:
2. Нажмите на кнопку «Пуск» для открытия меню, откройте «Панель управления» и из списка компонентов панели управления выберите «Администрирование», затем откройте компонент «Управление компьютером». В «Управлении компьютером» откройте «Локальные пользователи и группы»;
3. Открыть «Консоль управления MMC». Для этого нажмите на кнопку «Пуск», в поле поиска введите **mmc**, а затем нажмите на кнопку «Enter». Откроется пустая консоль MMC. В меню «Консоль» выберите команду «Добавить или удалить оснастку» или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге «Добавление и удаление оснасток» выберите оснастку «Локальные пользователи и группы» и нажмите на кнопку «Добавить». Затем нажмите на кнопку «Готово», а после этого - кнопку «ОК». В дереве консоли откройте узел «Локальные пользователи и группы (локально)»;
4. Воспользоваться комбинацией клавиш +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите lusrmgr.msc и нажмите на кнопку «ОК»;
5. Откройте узел «Пользователи» и либо в меню «Действие», либо из контекстного меню выбрать команду «Новый пользователь»:



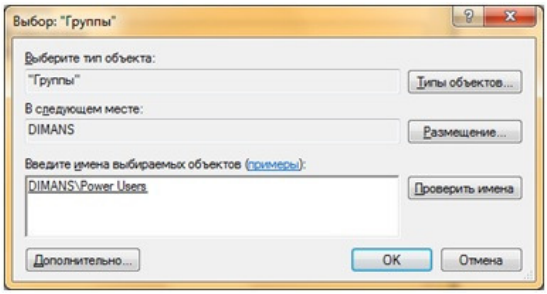
6. В диалоговом окне «Новый пользователь» введите соответствующие сведения. Помимо указанных данных, можно воспользоваться следующими флажками: Требовать смену пароля при следующем входе в систему, Запретить смену пароля пользователем, Срок действия пароля не ограничен, Отключить учетную запись и нажать на кнопку «Создать», а затем «Закрыть».



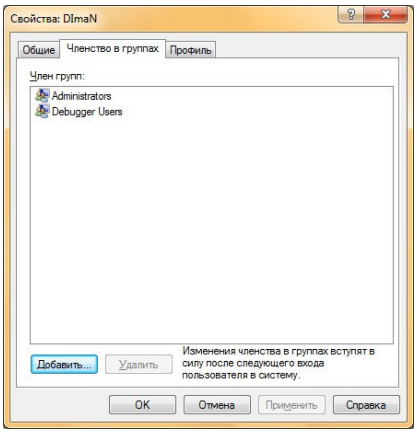
7. Для того чтобы добавить пользователя в группу, дважды щелкните имя пользователя для получения доступа к странице свойств пользователя. На вкладке «Членство в группах» нажмите на кнопку «Добавить».



8. В диалоге «Выбор группы» можно выбрать группу для пользователя двумя способами:
   - В поле «Введите имена выбираемых объектов» введите имя группы и нажмите на кнопку «Проверить имена», как показано на следующем скриншоте:



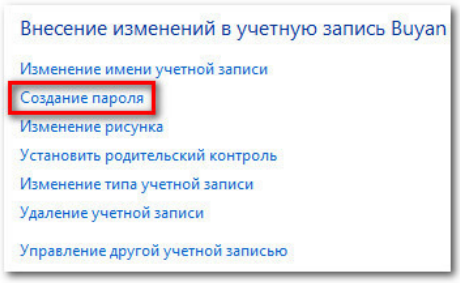
- В диалоге «Выбор группы» нажмите на кнопку «Дополнительно», чтобы открыть диалоговое окно «Выбор группы». В этом окне нажмите на кнопку «Поиск», чтобы отобразить список всех доступных групп, выберите подходящую группу и нажмите два раза на кнопку «ОК».



Изменение настроек учетной записи

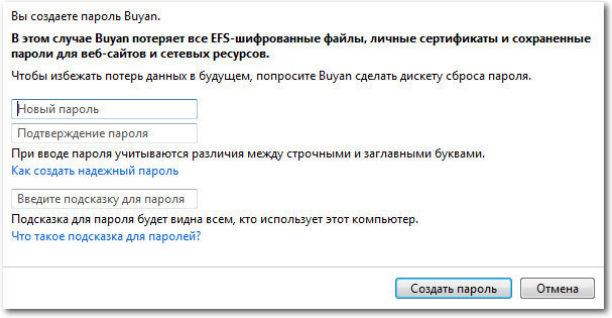
Для создания пароля:

1. На панели управления учетными записями нажмите на имя учетной записи или ее картинку.
2. Нажмите *Создание пароля*.



Создание пароля

3. Введите пароль в поле *Новый пароль* и в поле *Подтверждение пароля*.



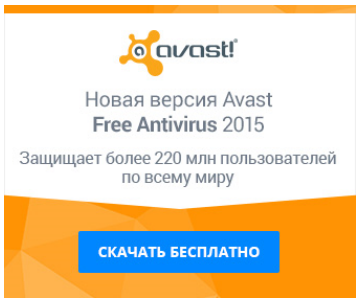
Ввод пароля и подсказки

4. При желании, вы можете создать подсказку, чтобы лучше помнить пароль.
5. Нажмите *Создание пароля*.
6. Чтобы вернуться на панель управления учетными записями, нажмите *Управление другой учетной записью*.

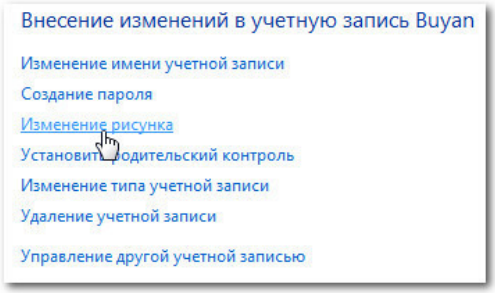
Пароли являются регистр зависимыми, то есть заглавные и строчные буквы считаются разными символами. Например, aBc1 не тоже самое, что abc1.

Чтобы изменить рисунок учетной записи:

Вы можете изменить рисунок любой учетной записи. Этот рисунок отображается рядом с именем и позволяет легко находить учетную запись.



1. На **панели управления учетными записями** нажмите на имя учетной записи или ее картинку.
2. Нажмите **Изменение рисунка**.



Изменение рисунка

3. Выберите рисунок или нажмите **Поиск других рисунков**, чтобы выбрать из ваших личных рисунков.

Использование родительского контроля

Windows 7 предлагает функцию *Родительский контроль*, чтобы помочь вам управлять типами контента, к которому имеют доступ дети. Вы можете назначить родительский контроль на любую учетную запись с *Обычным доступом*, при этом у каждой из учетных записей могут быть свои настройки. Если у вас несколько детей, то каждому из них вы можете разрешить пользоваться разными типами контента. Также вы можете менять настройки по мере взросления детей.

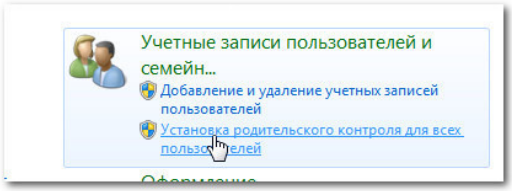
Перед тем как установить родительский контроль вам нужно создать учетную запись для вашего ребенка, если вы не сделали этого ранее. Это должна быть запись с *Обычным доступом*. Вы не сможете установить родительский контроль на учетную запись *Администратора*.

Когда вы устанавливаете родительский контроль, вам неважно, под какой учетной записью вы вошли. Однако, если вы зашли под учетной записью с обычным доступом, вам нужно будет ввести пароль *Администратора*, чтобы сделать какие-либо изменения.

Убедитесь, что вашим детям неизвестен пароль Администратора, в противном случае они смогут обойти ограничения родительского контроля.

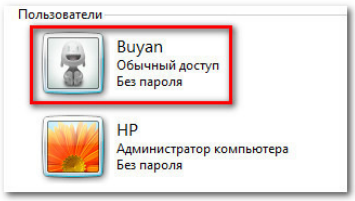
Чтобы установить родительский контроль:

1. Из меню *Пуск* перейдите в *Панель управления*.
2. Нажмите *Установка родительского контроля для всех пользователей.*



Переход к установке родительского контроля

3. Кликните по любой учетной записи с *обычным доступом*.

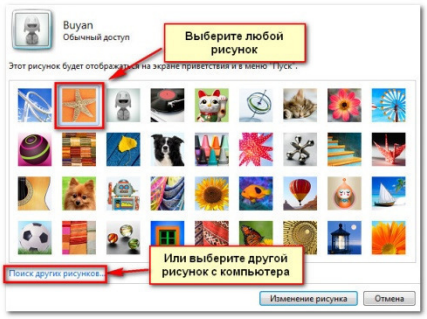


Выбор учетной записи

4. Нажмите *Включить, используя текущие параметры*.

Главная страница родительского контроля

5. Теперь вам доступны *Ограничения по времени*, *Игры* или *Разрешение и блокировка отдельных программ*.



Рисунки учетных записей

4. Нажмите *Изменение рисунка*.

Изменение настроек родительского контроля

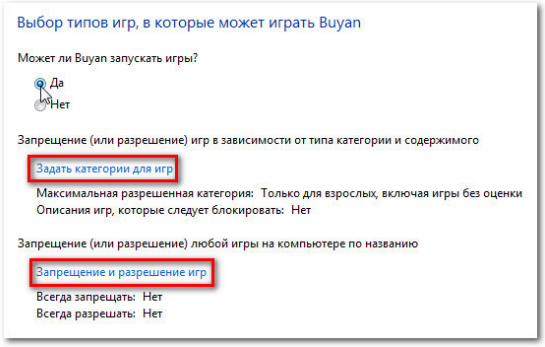
Ограничения по времени

Настройки ограничений времени позволяют вам контролировать, когда ваш ребенок пользуется компьютером. Кликните по любому блоку, чтобы разрешить или заблокировать доступ в это время. Если хотите, то можно задать разные ограничения времени на разные дни. Например, вы можете разрешить больше пользоваться компьютером в выходные.

Ограничения по времени

Игры

Настройка Игры, позволяет выбрать, какие категории игр или определенные игры разрешить или запретить. Сначала следует нажать *Да*, чтобы разрешить детям играть в игры, затем можно изменить настройки Игр.



Настройки игр

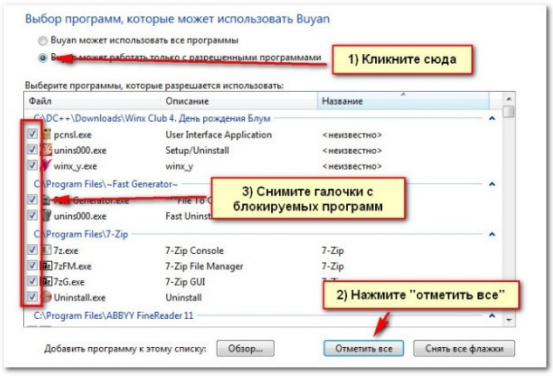
Здесь выбрано «Для всех» в качестве высшей категории разрешенных игр. Это означает, что ребенок может играть в игры категорий «Для всех» или «Для детей».

Категории игр

Чтобы разрешить или заблокировать определенные программы

Разрешите и заблокируйте определенные неигровые программы, которыми пользуется ваш ребенок. По умолчанию ваш ребенок может использовать все неигровые программы. Но могут быть программы, доступ к которым лучше ограничить, например, электронная почта или финансовые программы. Чтобы заблокировать определенные программы:

1. Нажмите *Дети может работать только с разрешенными программами*.
2. Нажмите *Отметить все*.
3. *Снимите выбор* с блокируемых программ.



Неигровые программы

Ограничение доступа к ПК

Другими способами защиты компьютера являются его блокировка на время отсутствия пользователя на рабочем месте и настройка экранной заставки, защищенной паролем. Нажав комбинацию клавиш Ctrl+Alt+Del, затем выбрать *Сменить пользователя* (либо комбинация клавиш *Windows+L*), можно предотвратить доступ пользователей, не прошедших проверку, на компьютер. Разблокировать его сможет только владелец и члены группы администраторов компьютера. (Для разблокирования компьютера нужно нажать Ctrl+Alt+Del, ввести пароль, а затем нажать кнопку OK.) Можно также настроить заставку таким образом, чтобы она открывалась и автоматически блокировала компьютер после того, как он простаивал в течение определенного времени.

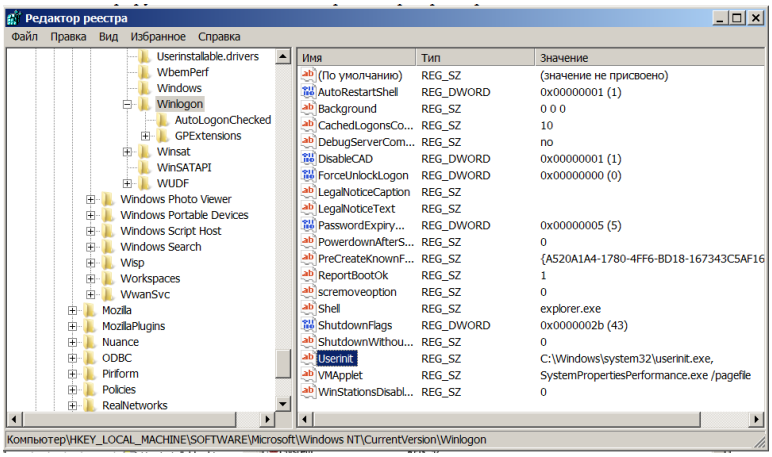
Лабораторное занятие 2
Изучение программных средств защиты от несанкционированного доступа

I. Цель занятия:

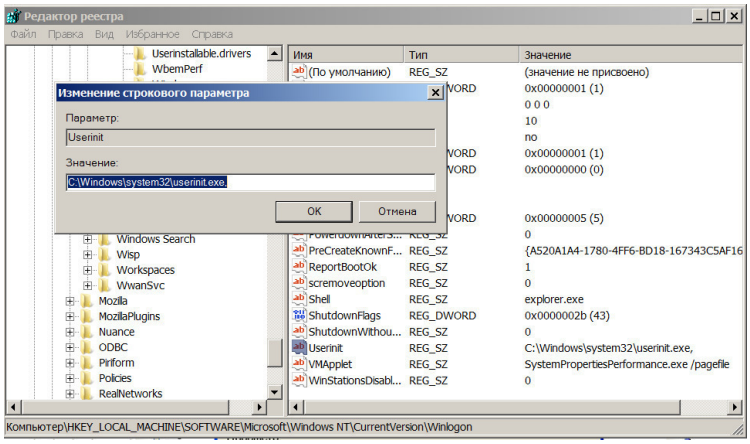
Изучить программные средства защиты от несанкционированного доступа.

II. Задание:

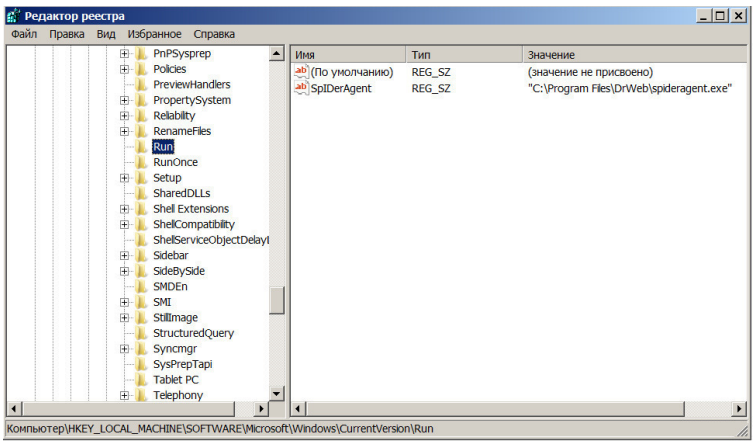
1. Ознакомьтесь с дополнением к практическому занятию 2.
2. Запустите программы просмотра и редактирования реестра Windows regedit.exe или regedit32.exe. Ознакомьтесь со структурой реестра, включите в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE). Включите в отчет копии экранных форм, иллюстрирующих использование редакторов реестра.
3. Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.
   Выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon.**
4. В правой половине открытого окна программы **regedit.exe** появится список ключей.
5. Найдите ключ **Userinit (REG_SZ)** и проверьте его содержимое.
6. По умолчанию этот ключ содержит следующую запись **C:\WINDOWS\system32\userinit.exe:**



7. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».
8. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.
9. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».
10. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду **Изменить** из меню **Правка** программы **regedit.exe).**
11. **В** открывшемся окне в поле **Значение** удалите ссылку на подозрительный файл.



12. Закройте программу **regedit.exe**.
13. Перейдите в папку с подозрительным файлом и удалите его.
14. Перезагрузите операционную систему и выполните пункты задания 3-5.
15. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.
16. Еще одним потенциальным местом записей на запуск «троянских программ» является *раздел автозапуска* ***Run*****.** Для его проверки выполните следующее.
17. Запустите программу **regedit.exe**.
18. В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE**и далее **Software\Microsoft\Windows\CurrentVersion\Run\... (REG_SZ):**



19. В рассматриваемом примере автоматически запускается резидентный антивирус (DrWeb).
20. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 7-15 предыдущего задания.
21. Включите в отчет копии экранных форм, иллюстрирующих потенциальные места записи «троянских программ» в системном реестре.
22. Запустите программу RESTrick.exe, позволяющую ограничить возможности пользователей ОС Windows, и выполните следующие действия:
    - скройте локальный диск С;
    - измените контекстное меню Создание нового документа (*Рабочий стол – Контекстное меню - Создать*);
23. Включите в отчет копии экранных форм, используемых при работе с программой RESTrick.exe.
24. Удалите все внесенные в программу изменения и завершите работу с RESTrick.exe.

III. Содержание отчета:

Отчет должен содержать:
- название и цель занятия;
- копии экранных форм.

IV. Контрольные вопросы:

1. Полномочия какого из пользователей ограничиваются с помощью программы RESTrick.exe?
2. Доступ к каким функциям Панели управления может быть ограничен с помощью программы RESTrick.exe?
3. Что такое реестр?
4. Потенциальные места записи «троянских программ» в системном реестре?

V. Литература:

1. Шаньгин В. Ф. Информационная безопасность [Электронный ресурс]: / Шаньгин В.Ф. - Москва: ДМК Пресс, 2014 http://e.lanbook.com/books/element.php?pl1_id=50578
2. Мельников Д. А. Информационная безопасность открытых систем [Электронный ресурс]: / Мельников Д.А. - Москва: ФЛИНТА, 2014 http://e.lanbook.com/books/element.php?pl1_id=48368

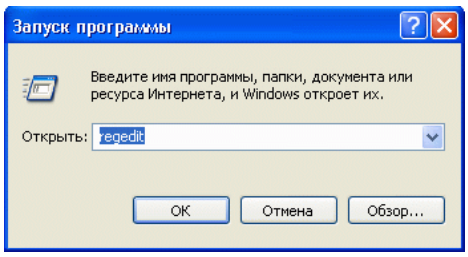
Дополнение

Общие сведения о реестре Windows

Реестр (системный реестр) - это иерархическая база данных, содержащая записи, определяющие параметры и настройки операционных систем Microsoft Windows. Реестр в том виде, как он выглядит при просмотре редактором реестра, формируется из данных, источниками которых являются файлы реестра и информация об оборудовании, собранная в процессе загрузки. В описании файлов реестра на английском языке используется термин "Hive". В некоторых работах его переводят на русский как "Улей". Microsoft в своих документах переводит это как "Куст". Файлы реестра создаются в процессе установки операционной системы и хранятся в папке %SystemRoot%\system32\config (обычно C:\windows\system32\config). Для операционных систем Windows это файлы с именами:

- default
- sam
- security
- software
- system

В процессе загрузки система получает монопольный доступ к данным файлам и, поэтому, стандартными средствами работы с файлами вы ничего с ними сделать не сможете (открыть для просмотра, скопировать, удалить, переименовать). Для работы с содержимым системного реестра используется специальное программное обеспечение - редакторы реестра (REGEDIT.EXE, REGEDT32.EXE), являющиеся стандартными компонентами операционной системы. Для запуска реестра используется "Пуск" "Выполнить" - regedit.exe



В левой половине окна вы увидите список корневых разделов реестра. Каждый корневой раздел может включать в себя вложенные разделы и параметры.

Коротко о назначении корневых разделов:

HKEY_CLASSES_ROOT (сокращенное обозначение **HKCR**) - в этом разделе содержится информация о зарегистрированных в Windows типах файлов, что позволяет открывать их по двойному щелчку мыши, а также информация для OLE и операций drag-and-drop.

HKEY_CURRENT_USER (**HKCU**) - настройки для текущего пользователя (рабочий стол, настройки сети, приложения). Этот раздел представляет собой ссылку на раздел HKEY_USERS\Идентификатор пользователя (SID) в виде S-1-5-21-854245398-1035525444-...
SID - уникальный номер, идентифицирующий учетную запись пользователя, группы или компьютера. Он присваивается учетной записи при ее создании. Внутренние процессы Windows обращаются к учетным записям по их кодам безопасности, а не по именам пользователей или групп. Если удалить, а затем снова создать учетную запись с тем же именем пользователя, то предоставленные прежней учетной записи права и разрешения не сохранятся для новой учетной записи, так как их коды безопасности будут разными. Аббревиатура SID образована от Security ID.

HKEY_LOCAL_MACHINE (**HKLM**) - глобальные аппаратные и программные настройки системы. Применимы ко всем пользователям. Это самая большая и самая важная часть реестра. Здесь сосредоточены основные параметры системы, оборудования, программного обеспечения.

HKEY_USERS (**HKU**) - индивидуальные настройки среды для каждого пользователя системы (пользовательские профили) и профиль по умолчанию для вновь создаваемых пользователей.

HKEY_CURRENT_CONFIG (**HKCC**) - конфигурация для текущего аппаратного профиля. Обычно профиль один единственный, но имеется возможность создания нескольких с использованием *Панель управления* - *Система – Оборудование* - *Профили оборудования*. На самом деле HKCC не является полноценным разделом реестра, а всего лишь ссылкой на раздел из HKLM.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware Profiles\Current

Все значения параметров реестра относятся к определённому типу.
Следующая таблица содержит типы данных, используемых в реестре Windows:

Тип данных	Краткое описание
REG_BINARY	Двоичные данные. Большинство сведений об аппаратных компонентах хранится в виде двоичных данных и выводится в редакторе реестра в шестнадцатеричном формате.
REG_DWORD	Целые числа размером в 4 байта. Многие параметры служб и драйверов устройств имеют этот тип и отображаются в двоичном, шестнадцатеричном или десятичном форматах.
REG_EXPAND_SZ	Строка данных переменной длины.
REG_MULTI_SZ	Многострочный текст. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами.
REG_SZ	Текстовая строка фиксированной длины
REG_FULL_ RESOURCE_DESCRIPTOR	Последовательность вложенных массивов, разработанная для хранения списка ресурсов железа или драйверов.

Возможности конкретного пользователя при редактировании данных реестра определяются его правами в системе. Предполагается, что пользователь имеет права администратора системы.

В процессе загрузки и функционирования операционной системы выполняется постоянное обращение к данным реестра как для чтения, так и для записи. Даже один неверный параметр в реестре может привести к краху системы, как и нарушение целостности отдельных файлов. Поэтому, прежде чем экспериментировать с реестром, позаботьтесь о возможности его сохранения и восстановления.

Ограничение доступа пользователя к ресурсам

В большинстве случаев, для того, чтобы изменения, внесенные в реестр, возымели действие, нужна перезагрузка или выход и повторный вход в систему. Параметры в разделе HKEY_CURRENT_USER относятся к текущему пользователю системы. Параметры в разделе HKEY_LOCAL_MACHINE - ко всем пользователям.

Скрытие логических дисков

Открываем раздел:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
и добавляем в него параметр NoDrives типа DWORD. Значение параметра определяет скрываемые диски A-Z. Наличие "1" начиная с младшего бита двойного слова означает отсутствие логического диска в "Мой компьютер"
00000001 - нет диска A, 00000002 - нет диска B, 00000004 - нет диска C, 0000000F - нет дисков A-F
Скрытые таким образом диски не видны только для Internet Explorer и в других программах могут быть доступны (например, в FAR).

Изменение меню кнопки "ПУСК"
NoRun =dword:00000001 нет кнопки "Выполнить"
NoLogOff=hex:01 00 00 00 (hedword a hex) нет "Завершение сеанса <Имя>"
NoFind =dword:00000001 - нет пункта "Найти"
NoFavoritesMenu =dword:00000001 нет "Избранное"
NoRecentDocsMenu=dword:00000001 нет "Документы"
NoSetFolders =dword:00000001 нет "Панели управления" в подменю "Настройка"

NoSetTaskbar=dword:00000001 нет "Панель задач" там же
NoPrinters =dword:00000001 нет "Принтеры" в Панели управления
NoAddPrinter=dword:00000001 нет "Добавить принтер"
NoDeletePrinter=dword:00000001 нет "Удалить принтер"
NoDesktop=dword:00000001 Пустой рабочий стол
NoNetHood=dword:00000001 нет "Сетевое окружение"
NoInternetIcon=dword:00000001 нет значка "Интернет" на Рабочем столе Windows
NoTrayContextMenu =hex:01,00,00,00 -Отключить меню, вызываемое правой кнопкой мыши на панели задач
NoViewContextMenu =hex:01,00,00,00 - Отключить меню, вызываемое правой кнопкой мыши на Рабочем столе: Чтобы включить обратно, надо 01 заменить на 00.
NoFileMenu=hex:01,00,00,00 скрыть " File " в верхней строке меню Проводника
ClearRecentDocsOnExit=hex:01,00,00,00 не сохранять список последних открываемых документов по выходу из системы.

Следующие параметры относятся к разделу реестра
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network

NoNetSetup=dword:00000001 отключает доступ к значку "Сеть" в Панели управления
NoFileSharingControl=dword:00000001 скрывает диалоговое окно управления совместным использованием файлов и принтеров, не позволяя пользователям управлять созданием новых совместных файлов или принтеров
NoNetSetupIDPage=dword:00000001 скрывает вкладку "Идентификация"
NoNetSetupSecurityPage=dword:00000001 скрывает вкладку "Управление доступом"
NoEntireNetwork=dword:00000001 скрывает элемент "Вся сеть" в Сетевом окружении
NoWorkgroupContents=dword:00000001 скрывает всё содержание Рабочей группы в Сетевом окружении

Следующие параметры относятся к ограничениям для всех пользователей, поскольку используется раздел HKEY_LOCAL_MACHINE, а не HKEY_CURRENT_USER.
Для редактирования данных нужно обладать правами администратора системы
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System

NoSecCPL =dword:00000001 отключает доступ к значку "Пароли" в Панели управления
NoAdminPage=dword:00000001 скрывает вкладку "Удаленное управление"
NoProfilePage =dword:00000001 скрывает вкладку "Профили пользователей"
NoPwdPage"=dword:00000001 скрывает вкладку "Смена паролей"
NoDispCPL=dword:00000001 отключает доступ к значку "Экран" в Панели управления
NoDispAppearancePage=dword:00000001 скрывает "Оформление" в окне свойств экрана
NoDispBackgroundPage=dword:00000001 скрывает "Фон" в окне свойств экрана
NoDispScrSavPage скрывает "Заставка" в окне свойств экрана
NoDispSettingsPage=dword:00000001 скрывает "Настройка" в окне свойств экрана
NoConfigPage=dword:00000001 скрывает "Профили оборудования" в окне свойств системы
NoDevMgrPage=dword:00000001 скрывает вкладку "Устройства" в окне свойств системы
NoFileSysPage=dword:00000001 скрывает кнопку "Файловая система..." на вкладке "Быстродействие" в окне свойств системы
NoVirtMemPage=dword:00000001 скрывает кнопку "Виртуальная память..." на вкладке "Быстродействие" в окне свойств системы

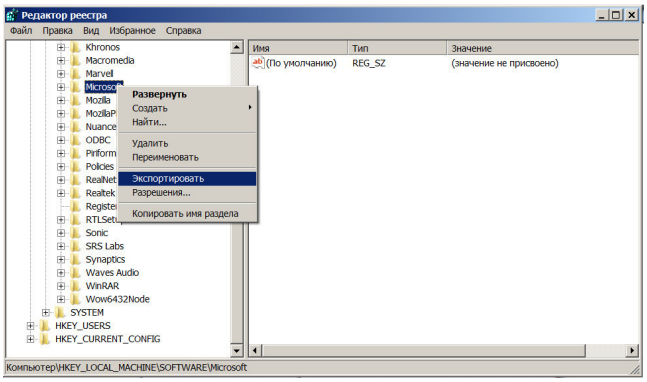
Некоторые из перечисленных запретов на действия пользователя используют не только системные администраторы, но и внедрившиеся в систему вирусы. Обычно выполняется запись в реестр данных, блокирующих возможность поиска и удаления

внедрившегося вредоносного программного обеспечения и, в качестве завершающего аккорда, запрет на запуск редактора реестра. Как следствие, даже обладая правами администратора, пользователь не имеет возможности что-либо сделать со своим собственным реестром.

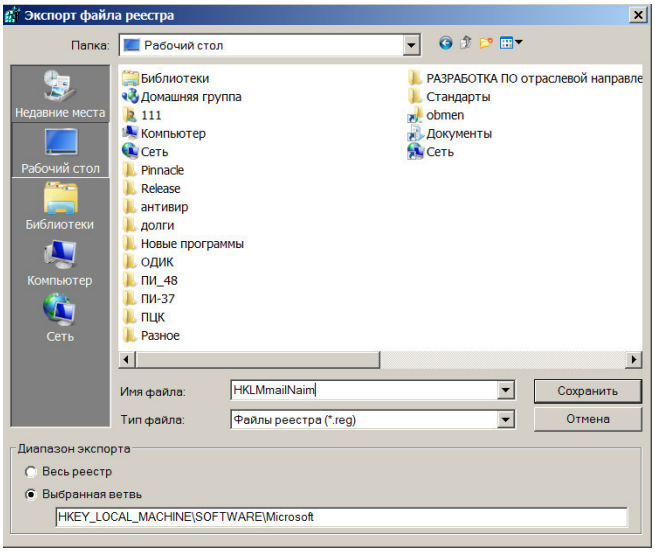
Создание резервной копии разделов реестра Windows

Чтобы создать резервную копию реестра, нужно запустить его. Для этого, в меню «Пуск» введите regedit или regedit.exe и нажмите кнопку OK/

Далее нужно найти раздел или подраздел, нажать правым кликом мышки на него и выбрать пункт «Экспортировать»:

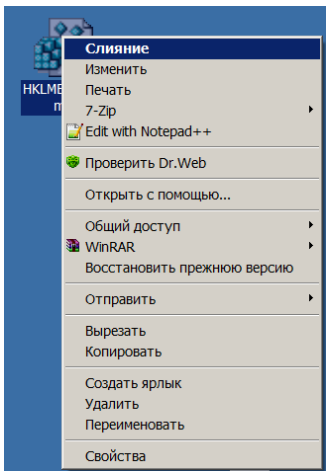


Теперь сталось лишь указать имя файла реестра и сохранить его в надежном месте:



Восстановление резервной копии разделов реестра Windows

Восстановление резервной копии разделов реестра Windows, очень простой процесс, так как для восстановления раздела можно лишь найти файл резервной копии, нажать правым кликом мышки на него, выбрать пункт «Слияние»:



В появившемся диалоговом окне, нужно подтвердить желание добавить информацию в реестр.

Этот метод восстановления не будет работать корректно при сохранение всего реестра или главных разделов.

О программе RESTrick

RESTrick - Апплет *Панели управления* (запускается из *Панели управления* Windows) для настройки различных параметров Windows. Интерфейс может быть как русским, так и английским (выбирается при инсталляции).

Панель управления RESTrick также позволит вам работать с профилями пользователей в системе. Это означает, что вы сможете настроить отдельно для каждого профиля свои собственные ограничения и параметры работы. Вы также сможете определить профиль "по умолчанию" - это профиль, который используется, если при загрузке системы был пропущен диалог входа в систему.

RESTrick включает в себя следующие основные элементы:

- установка ограничений, действующих в среде;
- работа с различными недокументированными и малодокументированными возможностями Windows;
- настройка профилей многопользовательской среды Windows;
- управление загрузкой Windows, работа со шрифтами и многое другое.

Программа дает вам доступ для настройки локальных дисков системы, которые необходимо отображать в Проводнике, позволяет настроить иконки на рабочем столе, задать опции загрузки системы и автоматического входа в систему, различные ограничения в рабочей среде, возможность запрета запуска определенных приложений в системе, а также другие опции.

Лабораторное занятие 3
Защита информации с помощью пароля

I. Цель занятия:

Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.

II. Задание:

1. Ознакомьтесь с дополнением к практическому занятию 3.

2. Проведение атаки перебором

   Используя программу Advanced Archive Password Recovery для вскрытия паролей, произведите атаку *перебором* на зашифрованный файл **perebor.rar**. Область перебора – все печатаемые символы, длина пароля от 4 до 7 символов. Проверьте правильность определенного пароля, распаковав исходный файл.
3. Проведение атаки по словарю

   Произведите *атаку по словарю* на файл **dictionary.rar**. Используйте русский словарь.
4. Проведение Plaintext атаки

   Произведите*Plaintext атаку* на файл **Plaintext.zip**. Для этого выберите вид атаки, а в закладке Plaintext-путь для файла plaintext **- Архив Plaintext**.

III. Содержание отчета:

Отчет должен содержать:
- название и цель занятия;
- копии экранных форм пунктов 2, 3, 4.

IV. Контрольные вопросы:

1. Какие виды атак на пароль вы знаете?
2. Что такое плохой пароль?
3. Как можно противостоять атаке полным перебором?
4. Как длина пароля влияет на вероятность раскрытия пароля?

V. Литература:

1. Шаньгин В. Ф. Информационная безопасность [Электронный ресурс]: / Шаньгин В.Ф. - Москва: ДМК Пресс, 2014 http://e.lanbook.com/books/element.php?pl1_id=50578
2. Мельников Д. А. Информационная безопасность открытых систем [Электронный ресурс]: / Мельников Д.А. - Москва: ФЛИНТА, 2014 http://e.lanbook.com/books/element.php?pl1_id=48368

Дополнение

Атаки на пароль

На сегодняшний день пароль является наиболее приемлемым и потому наиболее часто используемым средством установления подлинности, основанным на знаниях субъектов доступа.

В любой критической системе ошибки человека-оператора являются, чуть ли не самыми дорогостоящими и распространенными. В случае криптосистем, непрофессиональные действия пользователя сводят на нет самый стойкий криптоалгоритм, самую корректную его реализацию и применение.

В первую очередь, это связано с выбором паролей. Очевидно, что короткие или осмысленные пароли легко запоминаются человеком, но они гораздо проще для вскрытия. Использование длинных и бессмысленных паролей, безусловно, лучше с точки зрения криптостойкости, но человек обычно не может их запомнить и записывает на бумажке, которая потом либо теряется, либо попадает в руки злоумышленнику. Именно из того, что неискушенные пользователи обычно выбирают либо короткие, либо осмысленные пароли, существуют два метода их вскрытия: атака полным перебором и атака по словарю.

Защищенность пароля при его подборе зависит, в общем случае, от скорости проверки паролей и от размера полного множества возможных паролей, которое, в свою очередь, зависит от длины пароля и размера применяемого алфавита символов. Кроме того, на защищенность сильно влияет реализация парольной защиты.

В связи с резким ростом вычислительных мощностей атаки полным перебором имеют гораздо больше шансов на успех, чем раньше. Кроме того, активно используются распределенные вычисления, т.е. равномерное распределение задачи на большое количество машин, работающих параллельно. Это позволяет многократно сократить время взлома.

Однако вернемся на несколько лет назад, когда вычислительной мощности для полного перебора всех паролей не хватало. Тем не менее, хакерами был придуман остроумный метод, основанный на том, что в качестве пароля человеком выбирается существующее слово или какая-либо информация о себе или своих знакомых (имя, дата рождения и т.п.). Ну, а поскольку в любом языке не более 100000 слов, то их перебор займет весьма небольшое время, и от 40 до 80% существующих паролей может быть угадано с помощью простой схемы, называемой “атакой по словарю”. Кстати, до 80% этих паролей может быть угадано с использованием словаря размером всего 1000 слов!

Пусть сегодня пользователи уже понимают, что выбирать такие пароли нельзя, но, видимо, никогда эксперты по компьютерной безопасности не дождутся использования таких простых и радующих душу паролей, как 34jXs5U@bTa!6;). Поэтому даже искушенный пользователь хитрит и выбирает такие пароли, как ope, user2011, p.assword, toor, roottoor, parol, gfhjkm, asxz. Все они, как правило, базируются на осмысленном слове и некотором простом правиле его преобразования: прибавить цифру, прибавить год, перевести через букву в другой регистр, записать слово наоборот, прибавить записанное наоборот слово, записать русское слово латинскими буквами, набрать русское слово на клавиатуре с латинской раскладкой, составить пароль из рядом расположенных на клавиатуре клавиш и т.п.

Поэтому не надо удивляться, если такой «хитрый» пароль будет вскрыт хакерами - они не глупее самих пользователей, и уже вставили в свои программы те правила, по которым может идти преобразование слов. В самых «продвинутых» программах (JohnTheRipper, PasswordCrackinglibrary) эти правила могут быть программируемыми и задаваться с помощью специального языка самим хакером.

Приведем пример эффективности такой стратегии перебора. Во многих книгах по безопасности предлагается выбирать в качестве надежного пароля два осмысленных слова, разделенных некоторым знаком (например, good!password). Подсчитаем, за сколько времени в среднем будут сломаны такие пароли, если такое правило включено в набор программы-взломщика (пусть словарь 10000 слов, разделительными знаками могут быть 10 цифр и 32 знака препинания и специальных символа, машина класса Pentium со скоростью 15000 паролей/сек):

$10000 \cdot (32+10) \cdot 10000/15000 \cdot 2=140000$ секунд или менее 1.5 дня!

Чем больше длина пароля, тем большую безопасность будет обеспечивать система, так как потребуются большие усилия для его отгадывания. Это обстоятельство можно представить в терминах ожидаемого времени раскрытия пароля или ожидаемого безопасного времени. Ожидаемое безопасное время ($T_б$) - половина произведения числа возможных паролей и времени, требуемого для того, чтобы попробовать каждый пароль из последовательности запросов. Представим это в виде формулы:

$$T_б = \frac{A^S \cdot t}{2}, \quad (1)$$

где*t* - время, требуемое на попытку введения пароля, равное *E/R*;

E - число символов в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы); *R*- скорость передачи (символы/мин) в линии связи; *S* - длина пароля; *A*- число символов в алфавите, из которых составляется пароль. Если после каждой неудачной попытки подбора автоматически предусматривается десятисекундная задержка, то безопасное время резко увеличивается.

Поэтому при использовании аутентификации на основе паролей защищенной системой должны соблюдаться следующие правила:

- не позволяются пароли меньше 6–8 символов;
- пароли должны проверяться соответствующими контроллерами;
- символы пароля при их вводе не должны появляться в явном виде;
- после ввода правильного пароля выдается информация о последнем входе в систему;
- ограничивается количество попыток ввода пароля;
- вводится задержка времени при неправильном пароле;
- при передаче по каналам связи пароли должны шифроваться;
- пароли должны храниться в памяти только в зашифрованном виде в файлах, недоступных пользователям;
- пользователь должен иметь возможность самому менять пароль;
- администратор не должен знать пароли пользователей, хотя может их менять;
- пароли должны периодически меняться;
- устанавливаются сроки действия паролей, по истечении которых надо связаться с администратором.

Проблема выбора пароля

Выбор длины пароля в значительной степени определяется развитием технических средств, их элементной базы и ее быстродействием. В настоящее время широко применяются многосимвольные пароли, где S>10. В связи с этим возникают вопросы: как и где его хранить и как связать его с аутентификацией личности пользователя? На эти вопросы отвечает комбинированная система паролей, в которой код пароля состоит из двух частей. Первая часть состоит из 3–4-х десятичных знаков, если код цифровой, и более 3–4-х, если код буквенный, которые легко запомнить человеку. Вторая часть содержит количество знаков, определяемое требованиями к защите и возможностями технической реализации системы, она помещается на физическом носителе и определяет ключ-пароль, расчет длины кода которого ведется по указанной выше методике. В этом случае часть пароля будет недоступна для нарушителя.

Однако при расчете длины кода пароля не следует забывать о том, что при увеличении длины пароля нельзя увеличивать периодичность его смены. Коды паролей необходимо менять обязательно, так как за большой период времени увеличивается вероятность их перехвата путем прямого хищения носителя, снятия его копии, принуждения человека. Выбор периодичности необходимо определять из конкретных условий работы системы, но не реже одного раза в год. Причем желательно, чтобы дата замены и периодичность должны носить случайный характер.

Для проверки уязвимости паролей используются специальные контроллеры паролей. Например, известный контроллер Кляйна, осуществляет попытки взлома пароля путем проверки использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций, проверки использования в качестве пароля слов из различных словарей, начиная от наиболее употребительных в качестве пароля, проверки различных перестановок слов, а также проверки слов на языке пользователя–иностранца. Проверка паролей в вычислительных сетях с помощью контроллера Кляйна показала довольно высокие результаты - большинство пользователей используют простые пароли.

Показателен пример, когда контроллер Кляйна позволил определить 100 паролей из 5 символов, 350 паролей из 6 символов, 250 паролей из 7 символов и 230 паролей из 8 символов.

Приведенный анализ позволяет сформулировать следующие правила снижения уязвимости паролей и направленные на противодействие известным атакам на них:

- расширяйте применяемый в пароле алфавит - используйте прописные и строчные буквы латинского и русского алфавитов, цифры и знаки;
- не используйте в пароле осмысленные слова;
- не используйте повторяющиеся группы символов;
- не применяйте пароли длиной менее 6–8 символов, так как запомнить их не представляет большого труда, а пароль именно нужно запоминать, а не записывать. По той же причине не имеет смысла требовать длину неосмысленного пароля более 15 символов, так как запомнить его нормальному человеку практически невозможно;
- не используйте один и тот же пароль в различных системах, так как при компрометации одного пароля пострадают все системы;
- проверяйте пароли перед их использованием контроллерами паролей.

Для составления пароля можно дать рекомендации, которыми пользоваться надо очень осторожно:

- выберите несколько строк из песни или поэмы (только не те, которые Вы повторяете первому встречному) и используйте первую (или вторую) букву каждого слова - при этом пароль должен иметь большую длину (более 15 символов), иначе нужно менять регистры букв, применять латинские буквы вместо русских или наоборот, можно вставлять цифры и знаки;
- замените в слове из семи–восьми букв одну согласную и одну или две гласных на знаки или цифры. Это даст вам слово-абракадабру, которое обычно произносимо и поэтому легко запоминается.

Вывод:

Что такое плохой пароль:

- Собственное имя;
- Слово, которое есть в словаре;
- Идентификатор, присвоенный Вам какой-нибудь системой, или любые его вариации;
- Дата рождения;
- Повторенный символ (например, AAA);
- Пароль меньше 6 символов;
- Пароль, установленный Вам чужим человеком;
- Пароль, состоящий из символов, соседствующих на клавиатуре (например, QWERTY или ЙЦУКЕ);
- Пароль, состоящий из паспортных данных: персональный номер, номер водительских прав и т.д.

Что такое хороший пароль:

- Бессмысленная фраза;
- Случайный набор символов вперемешку с буквами.

Программный продукт Advanced Archive Password Recover для снятия парольной защиты с архивов

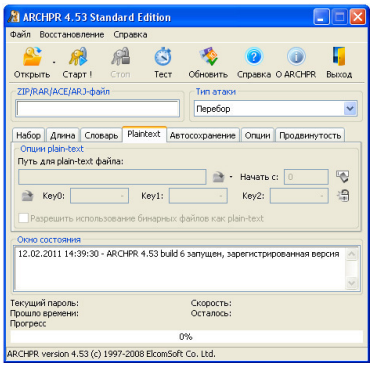
Advanced Archive Password Recovery восстанавливает доступ к зашифрованным архивам, снимая парольную защиту либо восстанавливая оригинальные текстовые пароли.

Понятный пользовательский интерфейс позволяет устанавливать множество масок и атак, в то время как оптимизированный под современные процессоры код обеспечивает лучшую производительность и скорейшее восстановление самых сложных паролей. Оптимизация кода позволила увеличить скорость перебора паролей. Миллион паролей в секунду - это в порядке вещей для ARCHPR.

Запуск Advanced Archive Password Recovery в фоновом режиме позволяет отыскивать пароли к архивам без прерывания основной работы в других приложениях. Остановка и продолжение процесса восстановления в любой момент позволяет эффективно распоряжаться ресурсами компьютера и подбирать пароли в то время, как вы работаете в других приложениях

Возможности Advanced Archive Password Recovery

- Поддержка всех версий ZIP/PKZip/WinZip, RAR/WinRAR, ARJ/WinARJ, а также ACE/WinACE (1.x);
- Архивы ZIP, созданные WinZip 8.0 и более ранними версиями, гарантированно расшифровываются в течение часа, если в архиве содержится не менее 5 файлов;
- Поддержка архивов размером 4 Гб и выше;
- Поддержка самораспаковывающихся архивов;
- Поддержка шифрования AES (архиватор WinRAR и новые версии WinZip);
- Использование всех найденных уязвимостей для ускорения расшифровки;
- При наличии хотя бы одного файла из архива, весь архив целиком будет расшифрован за минуту (для архивов в формате ZIP и ARJ);
- Возможность приостановки и перезапуска задач;
- Работа в фоновом режиме с низким приоритетом;
- Атаки по словарю и методом полного перебора паролей с поддержкой масок и шаблонов;
- Высочайшая производительность благодаря низкоуровневой оптимизации.



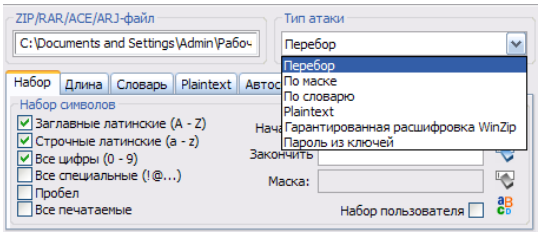
Панель управления:

- кнопка *Открыть* позволяет работать с проектом, в котором указан вскрываемый файл, набор символов, последний протестированный пароль.
- кнопки *Старт* и *Стоп* позволяют соответственно начинать и заканчивать подбор пароля.

- кнопка *Тест* позволяет провести оценку скорости подбора пароля, затраченное время, количество обработанных паролей.
- кнопка позволяет обновить версию программы.
- кнопка *Справка* выводит помощь по программе.
- кнопка *О ARCHPR* выводит информацию о программе.
- кнопка *Выход* позволяет выйти из программы.

Рассмотрим возможности программы:

1. Выбирается архив для вскрытия и тип атаки (см. рис).



Прямой перебор

В случае полного отсутствия информации о пароле осуществляется перебор всех возможных вариантов пароля определенной длины для восстановления доступа к документу. В Advanced Archive Password Recovery используются новейшие методы низкоуровневой оптимизации кода под современные процессоры, позволяющие достичь высокой производительности перебора по сравнению с конкурирующими продуктами.

Перебор по маске

В случае наличия дополнительной информации о пароле (известна длина пароля в символах или любая часть пароля, либо есть информация об использовании или отсутствии в пароле определенных символов и цифр) скорость восстановления может быть существенно увеличена методом перебора по заданной маске.

Атака по словарю

Согласно статистике, существенная часть паролей, используемых для защиты архивов, содержит одно или несколько слов из словаря. Метод подбора паролей по словарю позволяет в десятки раз сократить время, требуемое для восстановления пароля. Advanced Archive Password Recovery поддерживает атаку по словарю, перебирая пароли, состоящие из слов и их возможных комбинаций в разных регистрах и на нескольких языках. Поддерживается возможность подключения дополнительных словарей.

Plaintext

Как известно, ZIP-файлы шифруются по следующему алгоритму: пароль на архив не сохраняется внутри самого архива, а конвертируется в 32-битный ключ, который и используется для шифрования архива. В результате, итоговая сложность по перебору всех возможных вариантов равняется 2^{94}. Это слишком много: даже имея в своём распоряжении все компьютеры Земли, вы не узнаете этот пароль до конца своей жизни. Но этот алгоритм не так мощен, как, например, DES, RSA, IDEA и т.д. То есть, один из способов взлома защиты ZIP-файлов такой: нам нужен архив с точной копией одного из файлов из зашифрованного архива, сделанный тем же архиватором и с той же степенью компрессии.

Этот тип атаки не такой долгий, как простой перебор всех возможных паролей, что позволяет его использовать для более быстрого вскрытия паролей на ZIP и GZIP архивы.

Архив с этим файлом не должен быть меньше 12 байт.

Атака происходит в 2 этапа:

- отброс заведомо неподходящих ключей,
- поиск подходящих ключей.

На первой фазе работы, которая занимает от 1 до 3 минут (это зависит от размера архива с одним файлом и количества вашей оперативной памяти), оставшееся время не может быть вычислено, так что большую часть времени процесс-индикатор держится на нуле.

Гарантированная расшифровка WinZip

Эта атака аналогична предыдущей, но вам не надо иметь дополнительные архивы с файлами, а в самом защищенном паролем архиве должно быть, как минимум, 5 файлов. Атака работает с архивами, созданными при помощи WinZip, не выше версии 8.0 включительно, а также другими архиваторами на основе исходников Info-ZIP. Если архив создан при помощи «неправильного» архиватора или имеет менее 5 файлов, программа выдаст сообщение об ошибке.

Атака состоит из трёх этапов: первые два ищут подходящие ключи, а последний генерирует пароль (не более 10 символов) на основе этих ключей. Обычно, первая часть атаки длится несколько минут, вторая - около получаса, а последняя - 2-3 минуты. Атака работает с большинством ZIP-архивов, и даже если пароль достаточно длинен и не был найден на последней стадии атаки, программа сможет расшифровать архив, чтобы просто снять парольную защиту. Этот тип атаки базируется на генераторе случайных чисел, который использовался в WinZip до версии 8.1. Но даже версии WinZip ниже 8.1 в 0,4% случаях генерируют «нормальные» архивы, которые не могут быть взломаны этим типом атаки. В этом случае, программа выдаст предупреждение о том, что на первой стадии атаки не было найдено ни одного ключа.

Пароль из ключей

Два предыдущих метода атаки вначале пытаются найти ключи шифрования для защищенных паролем архивов. Они также могут расшифровать сам архив, если не было найдено ни одного пароля. Однако эти атаки могут использоваться только для архивов с паролями длиной менее 10 символов. Для архивов с более длинными паролями существует специальный тип атаки. Если у вас есть ключи шифрования для защищенного паролем архива, и вы хотите найти этот длинный пароль, выбирайте атаку «Пароль из ключей»и вводите эти ключи в закладке «Plaintext». Обычно эта атака используется для того, чтобы узнать пароль на архив длиной 14-15 символов. Лучше всего в свойствах атаки установить *Начать с* 7-го символа пароля, т.к. его (пароля) начало может быть восстановлено с «хвоста». Стоит помнить, что, в любом случае, атака начинается с конца пароля и об этом нужно помнить, вводя позицию для старта.

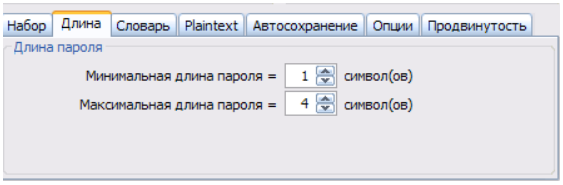
2. Выбираются параметры работы:

- Закладка *Набор*

Программа позволяет выбрать область перебора (набор символов). Это значительно сокращает время перебора. Можно использовать набор пользователя, заданный с помощью кнопки *Набор*. Можно ограничить количество тестируемых паролей, задав начальный пароль. В случае если известна часть пароля, очень эффективна атака по маске. Нужно выбрать соответствующий тип атаки, после этого станет доступным поле

маска. В нем нужно ввести известную часть пароля в виде P?s?W?r? , где на месте неизвестных символов нужно поставить знак вопроса. Можно использовать любой другой символ, введя его в поле символ маски.

- Закладка *Длина*



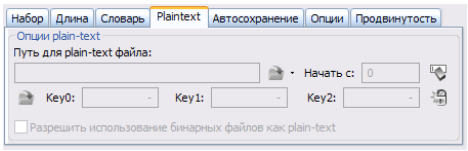
Позволяет выбрать длину пароля.

- Закладка *Словарь*

Позволяет выбрать файл-словарь. Выбирайте файл English.dic, он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

- ЗакладкаPlaintext

Используется для ввода ключей шифрования для защищенного паролем архива.



- Закладка *Автосохранение*

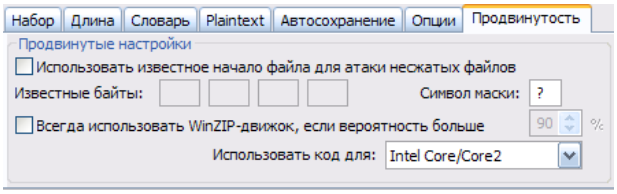
Можно выбрать имя файла для сохранения результатов работы и интервал автосохранения.

- Закладка *Опции*

Выбирается приоритет работы (фоновый или высокий), интервал обновления информации о тестируемом в данный момент пароле. Увеличение интервала повышает быстродействие, но снижает информативность. Также можно установить режим ведения протокола работы и возможность минимизации программы в tray.

- Закладка *Продвинутость*

Для продвинутых пользователей.



Лабораторное занятие 4
Криптографические методы защиты информации

I. Цель занятия:

Ознакомиться с основными методами криптографической защиты информации.

II. Задание:

1. Используя таблицу Вижинера, зашифруйте сообщения:
   1.1 «*РАСКИНУЛОСЬ МОРЕ ШИРОКО*», ключ «*МОНАСТЫРЬ*».
   1.2 «*АЛГОРИТМ ЛИНЕЙНОЙ СТРУКТУРЫ*», ключ «*ВАГОН*».
   1.3 «*КРАСОТА ТРЕБУЕТ ЖЕРТВ*», ключ «*РЕФЛЕКС*».
2. Используя перестановки с ключом,
   2.1 расшифруйте следующий текст:
   МЕТДЛЛЕСНЬЬСЕЕНУЮТОИЗСЛШМЕЧСНОЯОЯЧЖФРПТКГЩОАМЕНРУ ОЕРОЕЛТОИТЕАЕОБПВИ,
   если ключевое слово – «*МОДЕЛЬ*».
   2.2 зашифруйте текст:
   «*ПОДЛИННОСТЬ ДОКУМЕНТОВ ПОЛУЧЕННЫХ ЧЕРЕЗ АГЕНТА БАЙТИК ПОДТВЕРЖДАЮ ЮСТАС*»,
   используя в качестве ключевого слова слово «*ПАКЕТ*».
   2.3 расшифруйте следующий текст:
   НЕЕЯСВ СТИЩНА ТЕЕОНС БНЯОЯО ЕТЕЛПН ЕОЫНМО,

используя матричную перестановку символов: решетку 6×6.

3. При помощи аналитических преобразований расшифруйте текст:
   23 45 42 64 59 89

$$A = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 5 \\ 3 & 2 & 1 \end{pmatrix}$$

4. Используя метод гаммирования,
   4.1 расшифруйте *ЮСРББЩ*
   Гамма: *01 03 05 07 11 09* (Используемая операция - сложение по модулю 2)
   4.2 зашифруйте «*ШИФРЫ*» (*25 09 21 17 28*)
   Гамма: *04 01 13 13 01* (Используемая операция - сложение по модулю 2)
   4.3 расшифруйте *РЯУЦЦЖ*
   Гамма: *08 14 01 14 09 06*(Используемая операция - сложение по модулю 33)
5. При шифровании методом Френдберга был получен шифр: *РХООРР*.
   Первые значения датчика: *02 03 01 04 03 05*.

Расшифруйте исходное сообщение, если одноалфавитная замена выглядит следующим образом:

А	Е	К	Л	П
Х	Т	Р	К	О

III. Содержание отчета:

Отчет должен содержать:
- название и цель занятия;
- расшифрованные и зашифрованные сообщения.

IV. Контрольные вопросы:

1. Симметричные криптосистемы: шифры перестановки.
2. Симметричные криптосистемы: шифры простой замены.
3. Симметричные криптосистемы: гаммирование.
4. Симметричные криптосистемы: комбинированные методы шифрования.

V. Литература:

1. Адаменко, М.В. Основы классической криптологии : секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2012. — 256 с. — Режим доступа: https://e.lanbook.com/book/9123. — Загл. с экрана.
2. Адаменко, М.В. Основы классической криптологии: секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2016. — 296 с. — Режим доступа: https://e.lanbook.com/book/82817. — Загл. с экрана.

Талица Вижинера

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия лаборатории разработки, внедрения и адаптации программного обеспечения отраслевой направленности.

Оборудование лаборатории и рабочих мест лаборатории:

рабочие места по количеству обучающихся,
рабочее место преподавателя,
комплект учебно-методической документации;
наглядные пособия: демонстрационные плакаты, раздаточный материал;
лицензионное программное обеспечение: текстовый редактор MSWord 2013, программный продукт Advanced Archive Password Recover, архиваторы WinZip и WinRAR, панель управления RESTrick.

Технические средства обучения:

компьютеры, сканер, принтер, проектор, локальная и глобальная сеть.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Шаньгин В. Ф. Информационная безопасность [Электронный ресурс]: / Шаньгин В.Ф. - Москва: ДМК Пресс, 2014 http://e.lanbook.com/books/element.php?pl1_id=50578
2. Адаменко, М.В. Основы классической криптологии : секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2012. — 256 с. — Режим доступа: https://e.lanbook.com/book/9123. — Загл. с экрана.
3. Адаменко, М.В. Основы классической криптологии: секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2016. — 296 с. — Режим доступа: https://e.lanbook.com/book/82817. — Загл. с экрана.

Дополнительная литература

1. Мельников Д. А. Информационная безопасность открытых систем [Электронный ресурс]: / Мельников Д.А. - Москва: ФЛИНТА, 2014 http://e.lanbook.com/books/element.php?pl1_id=48368

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических и лабораторных занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля результатов обучения**
Умения	
создавать и удалять учетные записи; защищать информацию с помощью пароля;	выполнение и защита лабораторного занятия
применять программные средства защиты от несанкционированного доступа;	выполнение и защита лабораторного занятия
применять программный продукт Advanced Archive Password Recover для снятия парольной защиты с архивов WinZip и WinRAR;	выполнение и защита лабораторного занятия
применять методы шифрования и дешифрования с симметричными ключами.	выполнение и защита лабораторного занятия, контрольная работа
Знания	
основные понятия и определения информационной безопасности;	контрольная работа
источники и содержание основных угроз информационной безопасности;	контрольная работа
способы защиты от несанкционированного доступа и основные принципы защиты информации;	контрольная работа
модели обеспечения информационной безопасности;	контрольная работа
криптографические методы и средства обеспечения ИБ;	лабораторные занятия, контрольная работа, подготовка опорного конспекта по заданной теме(самостоятельная работа)
проблемы вирусного заражения программ, структуру современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты;	тестирование
технические каналы утечки информации.	Устный опрос
Итоговый контроль	*Дифференцированный зачет*

Форма контроля результатов обучения	**Критерии оценки результатов обучения**
Проверочная, контрольная работа	– «отлично» выставляется обучающемуся, если работа выполнена полностью, или в ней имеются несущественные ошибки; на качественные и теоретические вопросы дан полный, исчерпывающий ответ литературным языком с соблюдением технической терминологии в определенной логической

	последовательности, приводит новые примеры, устанавливает связь между изучаемым и ранее изученным материалом по курсу, умеет применить знания в новой ситуации; – «хорошо» выставляется обучающемуся, если работа выполнена полностью или не менее чем на 80 % от объема задания, но в ней имеются недочеты и несущественные ошибки; ответ на качественные и теоретические вопросы удовлетворяет вышеперечисленным требованиям, но содержит неточности в изложении фактов, определений, понятий, объяснении взаимосвязей, выводах и решении задач; учащийся испытывает трудности в применении знаний в новой ситуации, не в достаточной мере использует связи с ранее изученным материалом. – «удовлетворительно» выставляется обучающемуся, если выполнена в основном верно (объем выполненной части составляет не менее 2/3 от общего объема), но допущены существенные неточности; обучающийся обнаруживает понимание учебного материала при недостаточной полноте усвоения понятий и закономерностей; умеет применять полученные знания при решении простых задач с использованием готовых формул, но затрудняется при решении качественных задач и сложных количественных задач, требующих преобразования формул. – «неудовлетворительно» выставляется обучающемуся, если работа в основном не выполнена (объем выполненной части менее 2/3 от общего объема задания); обучающийся показывает незнание основных понятий, непонимание изученных закономерностей и взаимосвязей, не умеет решать количественные и качественные задачи.
Тестирование	Оценивается дифференцированно в соответствии с критериями оценок (см. таблицу из п.5)
Устный опрос	– «отлично» выставляется обучающемуся, если он полно раскрыл содержание материала в объеме, предусмотренном программой; изложил материал грамотным языком в определенной логической последовательности, точно используя математическую и специализированную терминологию и символику; правильно выполнил графическое изображение и иные чертежи и графики, сопутствующие ответу; показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания; продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков; отвечал самостоятельно без наводящих вопросов.

	– «хорошо» выставляется обучающемуся, если ответ имеет один из недостатков: в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа; нет определенной логической последовательности, неточно используется математическая и специализированная терминология и символика; допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию или вопросу преподавателя. – «удовлетворительно» выставляется обучающемуся, если неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, чертежах, блок-схем и выкладках, исправленные после нескольких наводящих вопросов преподавателя; обучающийся не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме; при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков. – «неудовлетворительно» выставляется обучающемуся, если не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, при использовании терминологии, в чертежах, блок-схемах и иных выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя.
Лабораторное занятие	– «зачтено» выставляется обучающемуся, не имеющему неудовлетворительных результатов по всем видам текущего контроля успеваемости, предусмотренным утвержденной рабочей программой дисциплины, и (или) показавшему знание основного учебно-программного материала в объеме, необходимом для дальнейшего обучения и профессиональной деятельности; – «незачтено» выставляется обучающемуся, имеющему неудовлетворительный результат по одному или нескольким видам текущего контроля успеваемости, предусмотренным рабочей программной дисциплины, и (или) показавшему пробелы в знании основного учебно-программного материала.

5. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

7 семестр обучения. Форма контроля – «Другие формы контроля» (контрольная работа)

Вопросы для проведения контрольной работы за 7 семестр
по дисциплине «Информационная безопасность»

1. Основные составляющие информационной безопасности.
2. Источники основных угроз информационной безопасности России.
3. Виды безопасности жизнедеятельности государства.
4. Умышленные и неумышленные угрозы на объекты информационной безопасности в Российской Федерации.
5. Физические и организационные угрозы безопасности информации.
6. Информационные и программно-математические угрозы безопасности информации.
7. Классификация угроз информационной безопасности по своей общей направленности.
8. Методы и средства защиты процессов переработки информации.
9. Идентификация/аутентификация с помощью биометрических данных.
10. Идентификация/аутентификация с помощью идентификационных карточек.
11. Идентификация/аутентификация посредством радиокодовых устройств.
12. Сервер аутентификации Kerberos.
13. Защита информации от исследования и копирования.
14. Одноразовые пароли.
15. Парольная аутентификация.

Оценка индивидуальных образовательных достижений по результатам текущего контроля производится в соответствии с универсальной шкалой (таблица).

Процент результативности (правильных ответов)	**Качественная оценка индивидуальных образовательных достижений**	
	балл (отметка)	**вербальный аналог**
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Критерии оценки:

– 90 ÷ 100% (5 баллов) присваивается обучающемуся, если он полностью выполнил задание контрольной работы;

– 80 ÷ 89% (4 балла) присваивается обучающемуся, если он полностью выполнил одно задание контрольной работы и допустил существенные ошибки при выполнении второго задания;
– 70 ÷ 79 % (3 балла) присваивается обучающемуся, если он полностью выполнил одно задание контрольной работы;
– Менее70% (2 балла) присваивается обучающемуся, если он не смог выполнить ни одного задания контрольной работы.

8 семестр обучения. Форма контроля – «Дифференцированный зачет»

Вопросы для подготовки к дифференцированному зачету
по дисциплине «Информационная безопасность»

1. Информационная безопасность. Основные понятия и определения.
2. Эволюция подходов к обеспечению информационной безопасности.
1. Источники и содержание основных угроз информационной безопасности России.
3. Информационные, программно-математические, физические и организационные угрозы.
4. Защита информации. Основные принципы защиты информации.
5. Методы и средства защиты процессов переработки информации.
6. Защита от несанкционированного доступа.
7. Идентификация и аутентификация. Основные понятия.
8. Модели обеспечения информационной безопасности - модели безопасности по разграничению доступа в систему.
9. Модели обеспечения информационной безопасности -модели контроля целостности информации в системе.
10. Модели обеспечения информационной безопасности- модели защиты при отказе в обслуживании.
11. Модели обеспечения информационной безопасности - модели анализа безопасности программного обеспечения.
12. Основные понятия, определения и композиции шифров.
13. Методы шифрования с симметричными ключами: шифрование методами замены (подстановки).
14. Методы шифрования с симметричными ключами: шифрование с симметричными ключами методами перестановки.
15. Методы шифрование с симметричными ключами при помощи аналитических преобразований.
16. Методы шифрования с симметричными ключами: шифрование аддитивными методами (гаммирование).
17. Комбинированные методы шифрования с симметричными ключами.
18. Системы с открытыми ключами.
19. Компьютерные вирусы. Проблемы вирусного заражения программ.
20. Структура современных антивирусных программ.
21. Основные классы антивирусных программ.

22. Методы антивирусной защиты.
23. Оптические и акустические каналы утечки информации.
24. Защита от утечки за счет электромагнитного излучения.
25. Отечественные и зарубежные стандарты в области информационной безопасности.
26. Организационное регулирование защиты процессов переработки информации: основные предметные направления защиты информации.
27. Создание учетных записей.
28. Ограничение доступа к ПК.
29. Общие сведения о реестре MS Windows.
30. Атаки на пароль.
31. Проблема выбора пароля.
32. Программный продукт Advanced Archive Password Recover для снятия парольной защиты с архивов.

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №1

по дисциплине Информационная безопасность
для четвертого курса

1. Модели обеспечения информационной безопасности – модели контроля целостности информации в системе.
2. Сервер аутентификации Kerberos.
3. Расшифруйте сообщение, полученное методом Френдберга: *C#B#NPPZHCBB*. Значения счетчика ПСЧ: *2341*.

Таблица подстановки:

A	B	E	K	H	O	П	P	C	T
I	J	#	J	Z	H	C	B	N	P

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.

Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №2

по дисциплине Информационная безопасность
для четвертого курса

1. Идентификация и аутентификация. Основные понятия.
2. Системы с открытыми ключами (СОК).
3. С помощью программы RESTrick.exe настройте создание нового документа MicrosoftOfficeWord таким образом, чтобы создавался не пустой документ.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №3

по дисциплине Информационная безопасность
для четвертого курса

2. Средства защиты процессов переработки информации.
3. Методы антивирусной защиты: методы обнаружения вирусов.
4. Расшифруйте сообщение, полученное методом Френдберга: *PSPTNPT*.

Значения датчика ПСЧ: *314631*,

таблица подстановки:

M	T	O	E	P	A
N	P	R	S	T	V

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №4

по дисциплине Информационная безопасность
для четвертого курса

1. Модели обеспечения информационной безопасности - модели безопасности по разграничению доступа в систему (модели предоставления прав).
2. Создание учетных записей.
3. Проведите атакуPlaintext атаку на файл **Архив3**.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №5

по дисциплине Информационная безопасность
для четвертого курса

1. Методы шифрования с симметричными ключами: шифрование методами замены (подстановки).
2. Информационные, физические и радиоэлектронные угрозы безопасности информации.
3. Используя метод гаммирования, расшифруйте *ЬВДЮЭГЛ*.
   ГАММА: *03 08 13 30 19 02 02*

(Используемая операция - сложение по модулю 2)

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №6

по дисциплине Информационная безопасность
для четвертого курса

1. Эволюция подходов к обеспечению информационной безопасности.
2. Основные виды антивирусных программ.
3. Создайте учетные записи пользователей: «Старший брат» и «Младший брат». Примените уникальный рисунок к каждой учетной записи. Создайте пароль «**1102**» для пользователя «Старший брат» и пароль «**2011**» для пользователя «Младший

брат» (*Срок действия пароля не ограничен*). Измените доступ к профилям так, чтобы пользователь «Старший брат» смог просматривать профиль пользователя «Младший брат», а наоборот нет. (Профиль «Младший брат» -*ограниченная учетная запись*).

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №7

по дисциплине Информационная безопасность
для четвертого курса

1. Основные понятия, определения и композиции шифров.
2. Оптические и акустические каналы утечки информации.
3. Проведите атаку по словарю (файл Архив8.rar),используйте русский словарь.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №8

по дисциплине Информационная безопасность
для четвертого курса

1. Информационные, программно-математические, физические и организационные угрозы.
2. Ограничение доступа к ПК.
3. Расшифруйте текст*6455123334223*при помощи аналитических преобразований:

$$A = \begin{pmatrix} 2 & 1 & 2 \\ 3 & 2 & 1 \\ 1 & 7 & 1 \end{pmatrix}$$

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №9

по дисциплине Информационная безопасность
для четвертого курса

1. Защита от несанкционированного доступа.
2. Атаки на пароль.
3. Используя матричную перестановку символов (решетка 6 × 6),зашифруйте "пример маршрутной перестановки".

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №10

по дисциплине Информационная безопасность
для четвертого курса

1. Методы защиты процессов переработки информации.
2. Защита от утечки за счет электромагнитного излучения.
3. Расшифруйте текст с помощью таблицы Виженера:
   СЮХУЩЬРФЗВХГ ключ «*ЗОНД*»

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №11

по дисциплине Информационная безопасность
для четвертого курса

1. Источники основных угроз информационной безопасности России. Случайные (неумышленные)и преднамеренные (умышленные) угрозы.
2. Общие сведения о реестре Windows.
3. Расшифруйте сообщение, полученное методом Френдберга*ETWWV*.
   Значения датчика ПСЧ: *4 1 4 5*,

таблица подстановки:

#	A	E	И	H	P	T
O	W	T	D	A	V	E

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №12

по дисциплине Информационная безопасность
для четвертого курса

1. Методы шифрования с симметричными ключами: шифрование аддитивными методами (гаммирование).
2. Основные принципы защиты информации.
3. С помощью программы RESTrick.exe настройте *Свойства экрана* таким образом, чтобы посторонний пользователь не смог изменить интерфейс *Рабочего стола*.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №13

по дисциплине Информационная безопасность
для четвертого курса

1. Модели обеспечения информационной безопасности- модели защиты при отказе в обслуживании.
2. Проблема выбора пароля.
3. Произведите атаку на зашифрованный файл Архив13.rar, Архив13.zip (по очереди). Область перебора – все печатаемые символы, длина пароля от 4 до 7 символов. Проверить правильность определенного пароля, распаковав файлы. Сократите область перебора до фактически используемого. Проведите повторное вскрытие. Сравните затраченное время.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №14

по дисциплине Информационная безопасность
для четвертого курса

1. Компьютерные вирусы. Основные классификационные признаки компьютерных вирусов.
2. Защита ПК от несанкционированного доступа.
3. Расшифруйте текст с помощью таблицы Вижинера:
   ПЬЙЫУЩАЭССЕМЪХЛН ключ «*АМБРОЗИЯ*»

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №15

по дисциплине Информационная безопасность
для четвертого курса

1. Методы шифрования с симметричными ключами: шифрование с симметричными ключами методами перестановки.
2. Основные составляющие информационной безопасности.
3. Проведите атакуPlaintext на файл **Архив15**.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №16

по дисциплине Информационная безопасность
для четвертого курса

1. Компьютерные вирусы. Способы вирусного заражения файлов.
2. Программный продукт AdvancedArchivePasswordRecover для снятия парольной защиты с архивов.
3. При помощи аналитических преобразований расшифруйте текст:
   7968 43867129

$$A = \begin{pmatrix} 4 & 1 & 2 \\ 3 & 2 & 3 \\ 1 & 1 & 5 \end{pmatrix}$$

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №17

по дисциплине Информационная безопасность
для четвертого курса

1. Модели обеспечения информационной безопасности - модели контроля целостности информации в системе.
2. Безопасность информационной системы (ИС).

3. Используя перестановки с ключом, зашифруйте текст: «*ПРИХОДИ НЕМЕДЛЕННО*». Ключевое слово «*ХОЛМС*».

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №18

по дисциплине Информационная безопасность
для четвертого курса

1. Методы шифрование с симметричными ключами при помощи аналитических преобразований.
2. Отечественные и зарубежные стандарты в области информационной безопасности.
3. Проведите атаку по словарю (файл Архив18.rar).Используйте русский словарь.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №19

по дисциплине Информационная безопасность
для четвертого курса

1. Проблемы вирусного заражения программ.
2. Системы с открытыми ключами (СОК).
3. Используя метод гаммирования, расшифруйте *ЬВДЮЭГЛ*.
   ГАММА: *03 08 13 30 19 02 02*
   (Используемая операция - сложение по модулю 2)

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная
информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №20

по дисциплине Информационная безопасность
для четвертого курса

1. Модели обеспечения информационной безопасности - модели безопасности по разграничению доступа в систему (вероятностные модели).
2. Методы антивирусной защиты: условия безопасной работы компьютерных систем и технология обнаружения заражения вирусами.
3. Используя метод гаммирования, расшифруйте *ТМКЭШМ*.
   ГАММА: *КЛЮЧ*
   (Используемая операция - сложение по модулю 33)

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №21

по дисциплине Информационная безопасность
для четвертого курса

1. Основные классы антивирусных программ (по функциональным признакам).
2. Создание учетных записей.
3. Зашифруйте произвольное сообщение (не менее 20 знаков) с помощью шифра Вижинера. Ключевым словом является ваша фамилия в именительном падеже.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __

«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №22

по дисциплине Информационная безопасность
для четвертого курса

1. Методы шифрования с симметричными ключами: шифрование с симметричными ключами методами перестановки.
2. Методы антивирусной защиты: методы обнаружения вирусов.
3. Используя метод гаммирования, зашифруйте *ВИНОГРАД*
   ГАММА: *04 06 19 12 07 2111 05*
   (Используемая операция - сложение по модулю 2)

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №23

по дисциплине Информационная безопасность
для четвертого курса

1. Средства защиты процессов переработки информации.
2. Модели обеспечения информационной безопасности - модели безопасности по разграничению доступа в систему (модели, основанные на принципах теории информации К. Шеннона).
3. Произведите атаку на зашифрованный файл Архив25.rar. Область перебора – заглавные и прописные буквы.

Преподаватель _____ Н.Е. Карпова

УАТ ФГБОУ ВО «УГАТУ»

Рассмотрено на заседании
ПЦК «Прикладная информатика»
Протокол № __
«__» _____ 20__ г.
Председатель ПЦК
_____Н.Е. Карпова

БИЛЕТ №24

по дисциплине Информационная безопасность
для четвертого курса

1. Защита от утечки информации по техническим каналам. Общие понятия.
2. Идентификация и аутентификация. Основные понятия.
3. Используя метод гаммирования, зашифруйте *ГЕОРГИН*
   ГАММА: *05 08 19 12 07 21 11*
   (Используемая операция - сложение по модулю 2)

Преподаватель _____ Н.Е. Карпова

Оценка индивидуальных образовательных достижений по результатам текущего контроля производится в соответствии с универсальной шкалой (таблица).

Процент результативности (правильных ответов)	**Качественная оценка индивидуальных образовательных достижений**	
	балл (отметка)	**вербальный аналог**
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Критерии оценки:

- 90 ÷ 100% (5 баллов) присваивается обучающемуся, если он полностью выполнил задание билета: дал правильные ответы на все вопросы и решил все задачи;
- 80 ÷ 89% (4 балла) присваивается обучающемуся, если он полностью выполнил практическое задание билета и дал правильный ответ на один теоретический вопрос;
- 70 ÷ 79 % (3 балла) присваивается обучающемуся, если он полностью выполнил практическое задание билета и допустил существенные ошибки при ответе на теоретический вопрос;
- менее 70% (2 балла) присваивается обучающемуся, если он не смог выполнить ни одного задания билета.

6. АДАПТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ (ОВЗ)

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ПРИЛОЖЕНИЕ 1

Контрольно-измерительные материалы учебной дисциплины

Информационная безопасность

для специальности 09.02.05 «Прикладная информатика (по отраслям)»

Форма обучения: очная

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Контрольно-измерительные материалы разработаны на основе рабочей программы учебной дисциплины «Информационная безопасность» для специальностей среднего профессионального образования.

Тест предназначен для обучающихся 4 курса. Вопросы подобраны таким образом, чтобы можно было проверить усвоение обучающимися соответствующих знаний и умений.

Предлагается пакет тестовых заданий по оценке качества подготовки обучающихся. Пакет содержит 3 варианта проверочных тестов, с помощью которых преподаватель может проверить качество усвоения пройденного материала.

Тест состоит из двух частей:

- часть 1 – 20 заданий с кратким ответом – проверка теоретических знаний (задания закрытого типа). Среднее время выполнения заданий – 30 мин;
- часть 2 –тест с 5-ю заданиями открытого типа. Среднее время выполнения заданий – 30 мин;

Первая часть (проверка теоретических знаний) – информационный тест, включающий в себя 20 заданий следующих видов:

- выбор правильного ответа;
- множественный выбор;
- установление соответствия;

За каждый правильный ответ – 4 балла.

Максимальное количество баллов – 80.

Вторая часть–тест, включающий в себя пять заданий открытого типа следующего вида: свободное изложение.

За каждый правильный ответ – 4 балла.

Максимальное количество баллов – 20.

На выполнение тестовых заданий отводится 60 минут астрономического времени.

2. КОДИФИКАТОР ЭЛЕМЕНТОВ СОДЕРЖАНИЯ ДЛЯ СОСТАВЛЕНИЯ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ

Код раздела	Код контролируемого элемента (темы)	Элементы содержания, проверяемые задания КИМ	№ варианта, задания
1	2	3	4
1		**Основные понятия и определения информационной безопасности. Эволюция подходов к обеспечению информационной безопасности**	
	1.1	Тема 1.1 Информационная безопасность. Основные понятия и определения. Эволюция подходов к обеспечению информационной безопасности	Часть 1 В1 – 1, 2, 16 В2 – 5, 6, 10 В3 – 3, 5 Часть 2 В1 – 1, 2 В2 – 1, 2
2		**Угрозы безопасности информации**	
	2.1	Угрозы безопасности информации	Часть 1 В1 – 7, 16, 17 В2 – 11, 17 В3 – 4, 16 Часть 2 В1 – 4
3		**Защита от несанкционированного доступа и основные принципы защиты информации**	
	3.1	Тема 3.1 Защита от несанкционированного доступа и основные принципы защиты информации	Часть 1 В1 – 3, 5, 6, 8, 9 В2 – 1, 3, 4, 14, 16 В3 – 7, 8, 10, 11, 12, 13, 14, 15 Часть 2 В1 – 5
4		**Модели обеспечения информационной безопасности**	
	4.1	Тема 4.1Модели обеспечения информационной безопасности	Часть 2 В3 – 5
5		**Криптографические методы и средства обеспечения ИБ**	

	5.1	Тема 5.1 Криптографические методы и средства обеспечения ИБ	Часть 1 В1 – 4 В2 – 7, 13 Часть 2 В1 – 3 В2 – 3, 4, 5 В3 – 1
6		**Проблемы вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты**	
	6.1	Тема 6.1 Проблемы вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты	Часть 1 В1 – 14, 15,18, 19, 20 В2 – 9, 12, 15, 18, 19, 20 В3 – 6, 9, 17, 18, 19, 20 Часть 2 В3 – 3, 4
7		**Защита от утечки информации по техническим каналам**	
	7.1	Тема 7.1 Защита от утечки информации по техническим каналам	Часть 1 В1 – 5, 11,12, 13 В2 – 2, 8 В3 – 1, 2
8		**Организационно-правовое обеспечение информационной безопасности**	
	8.1	Тема 8.1 Организационно-правовое обеспечение информационной безопасности	Часть 1 В1 – 10

3. ТЕСТОВЫЕ ЗАДАНИЯ

Вариант 1

1. Как называется умышленно искаженная информация?
а) Дезинформация
б) Информативный поток
в) Достоверная информация
г) Перестает быть информацией

2. Как называется информация, к которой ограничен доступ?
а) Конфиденциальная
б) Противозаконная
в) Открытая
г) Недоступная

3. Что называют защитой информации?
а) Деятельность по предотвращению утечки защищаемой информации
б) Деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
в) Деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
г) Все ответы верны

4. Шифрование информации –это….
а) Процесс ее преобразования, при котором содержание информации изменяется на ложную
б) Процесс преобразования, при котором информация удаляется
в) Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
г) Процесс преобразования информации в машинный код

5. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений
а) защита от сбоев в электропитании
б) защита от сбоев серверов, рабочих станций и локальных компьютеров
в) защита от сбоев устройств для хранения информации
г) защита от утечек информации электромагнитных излучений

6. Можно выделить следующие направления мер информационной безопасности
а) Правовые
б) Организационные
в) Все ответы верны
г) Технические

7. Потенциальные угрозы, против которых направлены технические меры защиты информации, – это……
а) Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

б) Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.
в) Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей
г) Потери информации из-за не достаточной установки сигнализации в помещении
д) Процессы преобразования, при котором информация удаляется

8. Программные средства защиты информации
а) Технические средства защиты информации
б) Источники бесперебойного питания (UPS)
в) Смешанные средства защиты информации
г) Средства архивации данных, антивирусные программы

9. Виды защиты БД– это….
а) Защита паролем, защита пользователем,
б) Учётная запись группы администратора
в) Приложение, которое используется для управления базой данных
г) Группа Users

10. Международным стандартным кодом является
а) CP866
б) ASCII
в) Unicode
г) DOS
д) Altair

11. Надежная защита от утечек информации за счет влияния побочных электромагнитных излучений и наводок (ПЭМИН) через цепи электропитания, заземления или по радио эфиру это?
а) излучатели белого шума
б) генераторы белого шума
в) блокираторы белого шума
г) кодеры
д) декодеры

12. Система технических средств и среда распространения сигналов для односторонней передачи данных от источника к получателю– это….
а) Канал передачи
б) Канал связи
в) Средства защиты
г) Блокиратор связи
д) Деблокиратор связи

13. Какой вид защищен от помех, создаваемых источниками электромагнитного излучения, стойки к колебаниям температуры и влажности?
а) Тонкий коаксиал
б) Толстый коаксиал
в) Витая пара
г) Дуга
д) Оптическое волокно

14. Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак– …..
а) Российский центр по защите от вредоносных программ
б) Компания McAfeeSecurity
в) Лаборатория Касперского
г) Лаборатория доктора Веб
д) Компания Тумар

15. *Выберите несколько вариантов ответа:*
В классификацию вирусов по способу заражения входят
а) Опасные вирусы
б) Файловые вирусы
в) Резидентные вирусы
г) Загрузочные вирусы
д) Нерезидентные вирусы

16. *Соотнесите* основные понятия в области информационной безопасности:

Основные понятия			Определение	
1.	Атака		а	Некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы
2.	Уязвимость автоматизированной системы (АС)		б	Система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности
3.	Угроза безопасности АС		в	Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности
4.	Защищенная система		г	Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

17. *Соотнесите* функции, выполняемые техническими средствами защиты:

Вид защиты			В чем состоит	
1.	Внешняя		а	Защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации
2.	Опознавание		б	Защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД
3.	Внутренняя		в	Специфическая группа средств, предназначенных для опознавания людей по различным индивидуальным характеристикам

18. *Выберите несколько вариантов ответа:*
Какого типа антивирусные программы способны идентифицировать только известные им вирусы и требуют обновления антивирусной базы?
а) Сторожа
б) Детекторы
в) Ревизоры
г) Доктора

19. Антивирусная программа Dr. Web - это:
а) Программа-сторож
б) Программа-детектор

в) Программа-ревизор
г) Программа-доктор

20. Какого типа антивирусные программы подают сигнал тревоги, но лечить неспособны?
а) Сторожа
б) Детекторы
в) Ревизоры
г) Доктора

Вариант 2

1. Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе, может быть осуществлен только тем лицам, которые на это имеют право:
а) Управление доступом
б) Конфиденциальность
в) Аутентичность
г) Целостность
д) Доступность
2. Технические каналы утечки информации делятся на…
а) Акустические
б) Электрические
в) Оптические
г) Все перечисленное

3. Какие потери информации, связанные с несанкционированным доступом, бывают?
а) Несанкционированное копирование, уничтожение или подделка информации
б) Потери при заражении системы компьютерными вирусами
в) Случайное уничтожение или изменение данных
г) Сбои дисковых систем

4. Средства защиты данных, функционирующие в составе программного обеспечения
а) Технические средства защиты информации
б) Источники бесперебойного питания (UPS)
в) Программные средства защиты информации
г) Смешанные средства защиты информации

5. Обеспечение доступа к информации только авторизованным пользователям?
а) Конфиденциальность
б) Целостность
в) Доступность
г) Целесообразность

6. Для обеспечения сохранения целостности программного обеспечения в составе вычислительной системы служит(ат)….
а) корпус вычислительной системы
б) шифры
в) сигналы
г) пароль

7. В каких случаях криптография неэффективна?

а) Когда элементы текста известны в открытом и активном виде
б) Когда элементы текста известны в зашифрованном и исходном виде
в) Если есть пароль и логин
г) Когда элементы текста представлены в открытом и не полном виде

8. Генераторы белого шума, предназначенные для маскировки побочных электромагнитных излучений и наводок на линии электропитания и телефонной линии
а) Штора
б) Октава
в) Гром
г) Соната

9. Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак– …..
а) Российский центр по защите от вредоносных программ
б) Компания McAfeeSecurity
в) Лаборатория Касперского
г) Лаборатория доктора Веб
д) Компания Тумар
10. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена– это…..
а) Конфиденциальность
б) Целостность
в) Доступность

11. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое пользователь может запомнить и предъявить для прохождения процедуры аутентификации –это ….
а) Идентификатор пользователя
б) Пароль пользователя
в) Учетная запись пользователя
г) Парольная система

12. К вирусам, изменяющим среду обитания, относятся:
а) Черви
б) Студенческие
в) Полиморфные
г) Спутники

13. Исследование возможности расшифровки информации без знания ключей:
а) Криптология
б) Криптоанализ
в) Взлом
г) Несанкционированный доступ

14. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некоторой уникальной информации:
а) Авторизация
б) Обезличивание
в) Деперсонализация
г) Аутентификация

д) Идентификация

15. *Выберите несколько вариантов ответа:*
В соответствии с особенностями алгоритма вирусы можно разделить на два класса:
а) Вирусы, изменяющие среду обитания,но не распространяющиеся
б) Вирусы, изменяющие среду обитания при распространении
в) Вирусы, не изменяющие среду обитания при распространении
г) Вирусы, не изменяющие среду обитания и не способные к распространению в дальнейшем

16. *Соотнесите* степени сложности устройств:

Устройства			Что представляют	
1.	Простые		а	Комбинированные агрегаты, состоящие из некоторого количества простых устройств, способные к осуществлению сложных процедур защиты
2.	Системы		б	Несложные приборы и приспособления, выполняющие отдельные процедуры защиты
3.	Сложные		в	Законченные технические комплексы, способные осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение

17. *Соотнесите* классификацию угроз по ряду признаков:

Угрозы			Какие бывают	
1.	По природе возникновения		а	Пассивные и активные
2.	По непосредственному источнику		б	Направленные на использование прямого стандартного и скрытого нестандартного доступов к ресурсам АС
3.	По степени воздействия на АС		в	Естественные или искусственные
4.	По способу доступа к ресурсам АС		г	Природная среда, человек, санкционированные программные средства и несанкционированные программные средства

18. Самые опасные вирусы, разрушающие загрузочный сектор - это:
а) Троянские вирусы
б) Паразитические вирусы
в) Вирусы черви
г) Вирусы-невидимки (стелс-вирусы)

19. Какого типа антивирусные программы способны обнаруживать и лечить зараженные файлы?
а) Сторожа
б) Детекторы
в) Ревизоры
г) Доктора

20. Какие разновидности вирусов перехватывают обращения операционной системы к пораженным файлам?
а) Троянские вирусы

б) Паразитические вирусы
в) Вирусы черви
г) Вирусы-невидимки (стелс-вирусы)

Вариант 3

1. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?
а) Акустические
б) Электрические
в) Оптические
г) Радиоканалы

2. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?
а) Такого средства не существует
б) Установка источников бесперебойного питания (UPS)
в) Каждую минуту сохранять данные
г) Перекидывать информацию на носитель, который не зависит от энергии
3. Обеспечение достоверности и полноты информации и методов ее обработки
а) Конфиденциальность
б) Целостность
в) Доступность
г) Целесообразность

4. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем –это….
а) Информационная война
б) Информационное оружие
в) Информационное превосходство

5. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена– это…..
а) Конфиденциальность
б) Целостность
в) Доступность

6. К вирусам, изменяющим среду обитания, относятся:
а) Черви
б) Студенческие
в) Полиморфные
г) Спутники

7. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа –это…
а) Защита информации
б) Компьютерная безопасность
в) Защищенность информации
г) Безопасность данных

8. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
а) Конфиденциальность
б) Целостность
в) Доступность

9. Антивирусная программа, принцип работы которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:
а) Ревизор
б) Иммунизатор
в) Сканер
г) Доктор(фаг)

10. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некоторой уникальной информации:
а) Авторизация
б) Обезличивание
в) Деперсонализация
г) Аутентификация
д) Идентификация

11. Процесс проверки некоторых обязательных параметров пользователя и, при положительном результате, предоставление ему определенных полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом называется….
а) Авторизация
б) Идентификация
в) Аутентификация
г) Обезличивание
д) Деперсонализация

12. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:
а) Токен
б) Password
в) Пароль
г) Login
д) Смарт-карта

13. Для защиты от злоумышленников необходимо использовать:
а) Системное программное обеспечение
б) Прикладное программное обеспечение
в) Антивирусные программы
г) Компьютерные игры
д) Музыку, видеофильмы

14. *Соотнесите* интересы в области информационной безопасности:

Интересы			В чем состоят	
1.	Национальные		а	В реализации конституционных прав и свобод, в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина

2.	Личности		б	Обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями
3.	Государства		в	В незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.
4.	Общества		г	В упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России.

15. *Соотнесите* основные методы получения паролей*:*

Метод			В чем состоит	
1.	Перебора		а	Для перебора используется словарь наиболее вероятных ключей
2.	Атака по словарю		б	Двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей
3.	Получение паролей из самой системы на основе программной и аппаратной реализации конкретной системы		в	Проверяются все ключи последовательно, один за другим
4.	Проверка паролей, устанавливаемых в системах по умолчанию		г	Пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе

16. *Выберите несколько вариантов ответа:*

Наиболее распространенные угрозы информационной безопасности:

а) Угрозы целостности
б) Угрозы защищенности
в) Угрозы безопасности
г) Угрозы доступности
д) Угрозы конфиденциальности

17. *Выберите несколько вариантов ответа:*

К вирусам, не изменяющим среду обитания, относятся:

а) Черви
б) Студенческие
в) Полиморфные
г) Спутники

18. Какой тип файлов компьютерный вирус не только портит, но и заражает?

а) Графические файлы

б) Программные файлы
в) Информационные файлы баз данных
г) Медиа-файлы

19. Резидентные вирусы:
а) Активны какое-то ограниченное время
б) Активизируются после нажатия на определенную комбинацию клавиш
в) Активны до выключения компьютера

20. Сколько функциональных модулей должен иметь любой вирус?
а) Четыре
б) Пять
в) Три

Часть 2

Вариант 1

1. *Продолжите фразу:*
   Информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира, называется ……

2. *Продолжите фразу:*
   Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена ……

3. *Продолжите фразу:*
   Наука о способах двунаправленного преобразования информации с целью конфиденциальной передачи ее по незащищенному каналу– …..

4. *Продолжите фразу:*
   Если информация искажена умышленно, то это называют ……

5. *Продолжите фразу:*
   Единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности называется …..

Вариант 2

1. *Продолжите фразу:*
   Гарантия того, что информация сейчас существует в ее исходном виде:

2. *Продолжите фразу:*
   Шифрование – это……..

3. *Продолжите фразу:*
   Симметричная криптография подразумевает …….

4. *Продолжите фразу:*
   При шифровании методом подстановки необходимо ……

5. *Продолжите фразу:*
   ГОСТ 28147-89 является стандартом ……

Вариант 3

1. *Продолжите фразу:*
   Асимметричная криптография подразумевает использование …..

2. *Продолжите фразу:*
   Целью аутентификации электронных документов является …..
3. *Продолжите фразу:*
   Сетевой червь – это …

4. *Продолжите фразу:*
   Особое хранилище, куда антивирус копирует все подозрительные файлы– …..

5. *Продолжите фразу:*
   Вероятность преодоления системы защиты за определенное время исследуют…..

Номера правильных ответов к тестовым заданиям части 1

Вариант 1

1.	а	11.	б
2.	а	12.	б
3.	г	13.	д
4.	в	14.	в
5.	г	15.	в, д
6.	в	16.	1г, 2а, 3в, 4б
7.	в	17.	1б, 2в, 3а
8.	г	18.	б, г
9.	а	19.	г
10.	в	20.	а

Вариант 2

1.	б	11.	б
2.	г	12.	в
3.	а	13.	б
4.	в	14.	г
5.	а	15.	б, в
6.	г	16.	1б, 2в, 3а
7.	б	17.	1в, 2г, 3в, 4а
8.	в	18.	а
9.	в	19.	г

10.	а	20.	г

Вариант 3

1.	а	11.	а
2.	б	12.	г
3.	б	13.	в
4.	а	14.	1б, 2а, 3в, 4г
5.	а	15.	1в, 2а, 3б, 4г
6.	в	16.	а, г, д
7.	а	17.	а, г
8.	б	18.	б
9.	в	19.	в
10.	г	20.	в

Ответы к заданиям части 2

Вариант 1

1. Ответ: истинной (достоверной)
2. Ответ: конфиденциальность
3. Ответ: криптография
4. Ответ: дезинформацией (ложной информацией)
5. Ответ: система защиты информации в КС

Вариант 2

1. Ответ: целостность
2. Ответ: процесс преобразования информации, при котором ее содержание становится непонятным для субъектов, не имеющих соответствующих полномочий
3. Ответ: для преобразования открытого текста в зашифрованный и для обратного расшифровывания используется один и тот же ключ
4. Ответ: заменить буквы исходного алфавита соответствующими буквами перестановочного алфавита
5. Ответ: симметричного шифрования, введённого в 1990 году

Вариант 3

1. Ответ: использование двух математически связанных ключей. Один ключ называют персональным (секретным), и он должен храниться в тайне, а парный ему ключ называют публичным (открытым), и доступ к нему должны иметь все участники информационного обмена
2. Ответ: Их защита от возможных видов злоумышленных действий
3. Ответ: разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от других типов компьютерных вирусов червь является самостоятельной программой
4. Ответ: Карантин
5. Ответ: Вероятностные модели

4. КРИТЕРИИ ПО ВЫСТАВЛЕНИЮ БАЛЛОВ

Сводная таблица с критериями баллов	
Часть	**Максимальный балл**
I	80
II	20
Итого	**100**

Оценка индивидуальных образовательных достижений по результатам выполнения тестовых заданий производится в соответствии с универсальной шкалой:

Процент результативности (набранные баллы)	**Качественная оценка индивидуальных образовательных достижений**	
	Отметка	**вербальный аналог**
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Критерии оценки:

- 90 ÷ 100% (5 баллов) присваивается обучающемуся, если он полностью выполнил задание теста, дал правильные ответы практически на все вопросы;
- 80 ÷ 89% (4 балла) присваивается обучающемуся, если он полностью выполнил задание теста, дал правильные ответы на половину вопросов;
- 70 ÷ 79 % (3 балла) присваивается обучающемуся, если он полностью выполнил задание теста, дал правильные ответы на основные вопросы;
- менее 70% (2 балла) присваивается обучающемуся, если он не полностью выполнил задание теста, не смог дать правильные ответы на некоторые вопросы.

ПРИЛОЖЕНИЕ 2

Методические указания по организации самостоятельной работы обучающихся по учебной дисциплине

Информационная безопасность

для специальности 09.02.05 «Прикладная информатика (по отраслям)»

Форма обучения: очная

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Внеаудиторная самостоятельная работа - планируемая учебная, учебно-исследовательская работа обучающихся, выполняемая вне занятий по заданию и при управлении преподавателем, но без его непосредственного участия.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации;
- формирования общих и профессиональных компетенций;
- развития исследовательских умений.

Методические рекомендации по выполнению внеаудиторных самостоятельных работ дисциплины «Информационная безопасность» раскрывают у обучающихся формирование системы знаний, практических умений и объяснения уровня образованности и уровня подготовки обучающихся по специальности 09.02.05 Прикладная информатика (по отраслям).

Изучение программного материала должно способствовать формированию у обучающихся знаний и навыков, необходимых для профессиональной деятельности.

Место дисциплины в структуре программы подготовки специалистов среднего звена (далее – ППССЗ): дисциплина входит в вариативную часть циклов ППССЗ по специальности среднего профессионального образования 09.02.05 Прикладная информатика (по отраслям).

Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен уметь:

- создавать и удалять учетные записи;
- применять программный продукт Advanced Archive Password Recover для снятия парольной защиты с архивов WinZip и WinRAR;
- применять программные средства защиты от несанкционированного доступа;
- применять методы шифрования и дешифрования с симметричными ключами.

В результате освоения дисциплины (модуля) обучающийся должен знать:

- основные понятия и определения информационной безопасности;

- источники и содержание основных угроз информационной безопасности;
- способы защиты от несанкционированного доступа и основные принципы защиты информации;
- модели обеспечения информационной безопасности;
- криптографические методы и средства обеспечения ИБ;
- проблемы вирусного заражения программ, структуру современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты;
- технические каналы утечки информации.

Техник-программист должен обладать общими компетенциями, включающими в себя способность:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Техник-программист должен обладать профессиональными компетенциями, соответствующими видам деятельности:

ПК 1.1. Обрабатывать статический информационный контент.

ПК 1.2. Обрабатывать динамический информационный контент.

ПК 1.3.Осуществлять подготовку оборудования к работе.

ПК 2.1. Осуществлять сбор и анализ информации для определения потребностей клиента.

ПК 3.2. Осуществлять продвижение и презентацию программного обеспечения отраслевой направленности.

Критерии оценки результатов самостоятельной работы

Критериями оценки результатов внеаудиторной самостоятельной работы обучающихся являются:

- уровень освоения учебного материала;
- уровень умения использовать теоретические знания при выполнении практических задач;
- уровень умения активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения материала;
- оформление материала в соответствии с требованиями стандарта предприятия;
- уровень умения ориентироваться в потоке информации, выделять главное;
- уровень умения четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- уровень умения определить, проанализировать альтернативные возможности, варианты действий;
- уровень умения сформулировать собственную позицию, оценку и аргументировать ее.

2. СТРУКТУРА И СОДЕРЖАНИЕ СРО

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***	
	7 семестр	***8 семестр***
Максимальная учебная нагрузка (всего)	*28*	*46*
Обязательная аудиторная учебная нагрузка (всего)	*32*	*20*
в том числе:		
лабораторныезанятия	-	*10*
практические занятия	-	-
курсовая работа (проект)	-	-
Самостоятельная работа обучающегося (всего)	-	*18*
в том числе:		
самостоятельная работа над курсовой работой (проектом) *(если предусмотрено)*	-	-
Домашняя работа: 1. Шифры простой замены: (полибианский квадрат, шифр Цезаря, шифрующие таблицы Трисемуса) 2. Шифры сложной замены (шифр Гронсфельда, шифр «двойной квадрат» Уинстона, шифрование методом Вернама)	*9* *9*	
Консультации	*2*	*2*
Итоговая аттестация	*Другие формы контроля*	*Дифференцированный зачет*

2.2. Тематический план и содержание внеаудиторной самостоятельной работы

Наименование разделов,тем	Вид внеаудиторной самостоятельной работы	Количество часов
Раздел 5 Криптографические методы и средства обеспечения ИБ		**18**
Тема 5.1 Криптографические методы и средства обеспечения ИБ	Составление опорного конспекта: традиционные симметричные	18

	криптосистемы (шифры простой и сложной замены)	
	Всего часов	**18**

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ОПОРНОГО КОНСПЕКТА

Составление опорного конспекта – представляет собой вид внеаудиторной СРО по созданию краткой информационной структуры, обобщающей и отражающей суть материала лекции, темы учебника. Опорный конспект призван выделить главные объекты изучения, дать им краткую характеристику, используя символы, отразить связь с другими элементами. Основная цель опорного конспекта – облегчить запоминание. В его составлении используются различные базовые понятия, термины, знаки (символы) – опорные сигналы. Опорный конспект – это наилучшая форма подготовки к ответу и в процессе ответа. Составление опорного конспекта к темам особенно эффективно у обучающихся, которые столкнулись с большим объёмом информации при подготовке к занятиям и, не обладая навыками выделять главное, испытывают трудности при её запоминании. Опорный конспект может быть представлен системой взаимосвязанных геометрических фигур, содержащих блоки концентрированной информации в виде ступенек логической лестницы; рисунка с дополнительными элементами и др.

Опорные конспекты могут быть проверены в процессе опроса по качеству ответа обучающегося, его составившего, или эффективностью его использования при ответе другими обучающимися.

Затраты времени при составлении опорного конспекта зависят от сложности материала по теме, индивидуальных особенностей обучающегося и определяются преподавателем.

Критерии оценки опорного конспекта

Оценка «Отлично» – полнота использования учебного материала. Объём конспекта – 1 тетрадная страница на один раздел или один лист формата А4. Логика изложения (наличие схем, количество смысловых связей между понятиями). Наглядность (наличие рисунков, символов, и пр.); аккуратность выполнения, читаемость конспекта. Грамотность (терминологическая и орфографическая). Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Самостоятельность при составлении.

Оценка «Хорошо» – использование учебного материала не полное. Объём конспекта – 1 тетрадная страница на один раздел или один лист формата А4. Недостаточно логично изложен материал. Наглядность (наличие рисунков, символов, и пр.); аккуратность выполнения, читаемость конспекта. Грамотность (терминологическая и орфографическая). Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Самостоятельность при составлении.

Оценка «Удовлетворительно» – использование учебного материала не полное. Объём конспекта – менее одной тетрадной страницы на один раздел

или один лист формата А4. Недостаточно логично изложен материал. Наглядность (наличие рисунков, символов, и пр.); аккуратность выполнения, читаемость конспекта. Грамотность (терминологическая и орфографическая). Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Самостоятельность при составлении. Неразборчивый почерк.

Оценка «Неудовлетворительно» – использование учебного материала неполное. Объём конспекта – менее одной тетрадной страницы на один раздел или один лист формата А4. Отсутствуют схемы, количество смысловых связей между понятиями. Отсутствует наглядность (наличие рисунков, символов, и пр.); аккуратность выполнения, читаемость конспекта. Допущены ошибки терминологические и орфографические. Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Несамостоятельность при составлении. Неразборчивый почерк.

4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ СРО

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Шаньгин В. Ф. Информационная безопасность [Электронный ресурс]: / Шаньгин В.Ф. - Москва: ДМК Пресс, 2014 http://e.lanbook.com/books/element.php?pl1_id=50578
2. Адаменко, М.В. Основы классической криптологии : секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2012. — 256 с. — Режим доступа: https://e.lanbook.com/book/9123. — Загл. с экрана.
3. Адаменко, М.В. Основы классической криптологии: секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2016. — 296 с. — Режим доступа: https://e.lanbook.com/book/82817. — Загл. с экрана.

Дополнительная литература

Мельников Д. А. Информационная безопасность открытых систем [Электронный ресурс]: / Мельников Д.А. - Москва: ФЛИНТА, 2014 http://e.lanbook.com/books/element.php?pl1_id=48368

5. ЗАДАНИЯ ДЛЯ ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа 1
Традиционные симметричные криптосистемы
(шифры простой и сложной замены)

I. Цель работы:

Научиться самостоятельно искать, отбирать, систематизировать и оформлять информацию по заданной теме. Расширить представление о традиционных симметричных криптосистемах.

II. Задание:

Подготовить опорный конспект «Традиционные симметричные криптосистемы (шифры простой замены: полибианский квадрат, шифр Цезаря, шифрующие таблицы Трисемуса; шифры сложной замены: шифр Гронсфельда, шифр «двойной квадрат» Уинстона, шифрование методом Вернама).

III. Методические рекомендации по подготовке опорного конспекта (см. п.3)

IV. Критерии оценки опорного конспекта (см. п.3)

V. Рекомендуемые источники:

1. Адаменко, М.В. Основы классической криптологии : секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2012. — 256 с. — Режим доступа: https://e.lanbook.com/book/9123. — Загл. с экрана.
2. Адаменко, М.В. Основы классической криптологии: секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2016. — 296 с. — Режим доступа: https://e.lanbook.com/book/82817. — Загл. с экрана.

Приложение

Образец оформления опорного конспекта (фрагмент)

Опорный конспект темы
«……..»

выполнил Ф.И.О. обучающегося, группа