Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: Экономическая безопасность
Профиль / специализация: специализация N 1 "Экономико-правовое обеспечение экономической
Дисциплина: Практикум по информационной безопасности

Формируемые компетенции: ОПК-6
ОПК-7
ПК-5

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при сдаче экзамена или зачета с оценкой

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания Экзамен или зачет с оценкой
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности	Хорошо

Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно- программного материала.	Отлично

Шкалы оценивания компетенций при сдаче зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно Не зачтено	Удовлетворительно Зачтено	Хорошо Зачтено	Отлично Зачтено
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.

Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей

2. Перечень вопросов и задач к экзаменам, зачетам, курсовому проектированию, лабораторным занятиям.

5 семестр

Примерный перечень вопросов к экзамену

Компетенция ОПК 6:

1. Общие сведения о хеш-функциях.
2. Криптографические хеш-функции.
3. Алгоритм MD5.
4. Алгоритм SHA-1.
5. Законы, регулирующие использование ЭП.
6. Основные принципы построения ЭП.
7. Алгоритм DSA.
8. Использование ЭП для защиты информации.

Компетенция ОПК 7:

1. Архивация и резервное копирование данных.
2. Программные средства архивации и резервного копирования данных.
3. Аппаратные средства архивации и резервного копирования данных.
4. Криптографические средства защиты информации.
5. Требования к программным продуктам, реализующим криптографическую защиту данных в РФ
6. Возможности операционной системы в области криптографической защиты данных
7. Российские средства криптографической защиты данных
8. Понятие сертификатов безопасности: определение, назначение.
9. Виды сертификатов безопасности, специфика их использования.

Компетенция ПК 5:

1. Административные шаблоны.
2. Пользовательские локальные групповые политики.
3. Автоматический и безопасный вход в систему.
4. Шифрованная файловая система EFS.
5. Архитектура доверенного платформенного модуля (TPM).
6. Технология шифрования диска BitLocker.
7. Защита папок и файлов паролем.
8. Управление специальными разрешениями доступа.
9. Владением файлом, наследование свойств

6 семестр

Примерный перечень вопросов к зачету

Компетенция ОПК 6:

1. Популярные антивирусные программы и их классификация.
2. Организация системы защиты информации экономических объектов.
3. Криптографические методы защиты информации.
4. Этапы построения системы защиты информации.
5. Оценка эффективности инвестиций в информационную безопасность.
6. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.
7. Управление информационной безопасности на государственном уровне.

Компетенция ОПК 7:

1. Аудит ИБ автоматизированных банковских систем.
2. Электронная коммерция и ее защита.
3. Менеджмент и аудит информационной безопасности на уровне предприятия.
4. Информационная безопасность предпринимательской деятельности.
5. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.
6. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
7. Доктрина информационной безопасности России.
8. Уголовно-правовой контроль над компьютерной преступностью в России.
9. Федеральные законы по ИБ в РФ.

Компетенция ПК 5:

1. Политика безопасности и ее принципы.
2. Фрагментарный и системный подход к защите информации.
3. Методы и средства защиты информации.
4. Организационное обеспечение ИБ.
5. Организация конфиденциального делопроизводства.
6. Комплекс организационно-технических информации.
7. Инженерно-техническое обеспечение компьютерной безопасности.
8. Организационно-правовой статус службы безопасности.
9. Защита информации в Интернете.
10. Электронная почта и ее защита.
11. Защита от компьютерных вирусов.

7 семестр

Примерный перечень вопросов к зачету

Компетенция ОПК 6:

1. Сетевые возможности ОС Windows.
2. Сетевое обнаружение и категории сетей. Сетевой проводник.
3. Центр управления сетями и общим доступом. Карта сети.
4. Управление локальными сетевыми подключениями.
5. Настройка ОС Windows на безопасную работу в сети.
6. Средства и методы сбора информации о вычислительной сети.
7. Идентификация узлов сетевых служб вычислительной сети.
8. Идентификация портов сетевых служб корпоративной сети.
9. Идентификация открытых портов вычислительной сети.
10. Идентификация уязвимостей сетевых приложений по косвенным признакам.
11. Эксплойты. Оценка стойкости паролей.

Компетенция ОПК 7:

1. Управление распространением маршрутной информации.
2. Настройка и маршрутизация виртуальных ЛВС (VLAN).
3. Протоколы и механизмы оптимизации и защиты сетей.
4. Проектирование, развертывание и настройка механизмов защиты в коммутируемых ЛВС.
5. Защита сетевой инфраструктуры.
6. Защита периметра сети.
7. Криптографическая защита каналов передачи данных.
8. Управление и диагностика беспроводных сетей.
9. Методы и средства защиты беспроводных сетей.

Компетенция ПК 5:

1. Антивирусные программы. Программы-детекторы. Программы-доктора.
2. Антивирусы-полифаги. Эвристические анализаторы.
3. Программы-ревизоры. Программы-фильтры.
4. Цели, функции и задачи защиты информации в сетях. Угрозы безопасности для сетей передачи данных.
5. В чём заключаются задачи защиты в сетях передачи данных?
6. Проблемы защиты информации в вычислительных сетях.
7. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.
8. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.

Примерные практические задачи (задания) и ситуации

5 семестр
Компетенция ОПК 6, ОПК 7, ПК 5

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности»–«Локальные политики» средство «Политика аудита» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности»–«Локальные политики» средство «Назначение прав пользователей» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности»–«Локальные политики» средство «Параметры безопасности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Брандмауэр Windows в режиме повышенной безопасности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Политики диспетчера списка сетей» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Создать цифровой сертификат с автоподписью, подписать им любой макрос (если отсутствует – создать), закрыть документ с сохранением, затем вновь открыть и проверить цифровой сертификат макроса. По ходу выполнения задания составить отчет с копиями окон.

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Надежные издатели» и изучить его (F1). В отчете перечислить возможные настройки и назначение этого средства безопасности.

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Параметры блокировки файлов» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Параметры конфиденциальности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

6 семестр
Компетенция ОПК 6, ОПК 7, ПК 5

1. Встроенными средствами ОС Windows настроить расписание архивации (резервного копирования файлов) и создать на съемном носителе резервную копию файлов из папок «Мои документы» всех пользователей вашего ПК.
2. На внешнем носителе создать файл «Ваша_фамилия.docx». Добавить в созданный файл любой текст, сохранить изменения. Удалить созданный файл. С помощью сторонней программы восстановить удаленный файл.
3. С помощью брандмауэра Windows добавить приложение «Блокнот» в список исключений при обмене данными. Удалить созданное исключение.
4. Запретить пользователю, входящему в группу «Администраторы», запись в папку С:\Фамилия\КР-1.
5. Включить безопасный вход в систему.
6. Запретить пользователю, входящему в группу «Администраторы», чтение папки С:\Фамилия\КР-1. Проверить действие запрета.
7. Настроить автоматический вход в систему под вашей учетной записью.
8. Запретить пользователю, входящему в группу «Администраторы», полный доступ к папке С:\Фамилия\КР-1
9. Отключить одну из ваших учетных записей.
10. Запретить пользователю, входящему в группу «Администраторы», разрешение «Изменение» для папки С:\Фамилия\КР-1
11. Запретить одной из ваших учетных записей смену пароля.
12. Запретить пользователю, входящему в группу «Администраторы», разрешение «Чтение и выполнение» для папки С:\Фамилия\КР-1
13. Создать диск сброса пароля.
14. Запретить пользователю чтение папки С:\Фамилия\КР-1. Проверить действие запрета.
15. Настроить расписание архивации (резервного копирования файлов) и создать на съемном носителе резервную копию файлов из папок «Мои документы» всех пользователей.

7 семестр
Компетенция ОПК 6, ОПК 7, ПК 5

1. Создать новую группу «КР-Фамилия», добавить в нее двух пользователей. Под пользователем, входящим в группу «Администраторы», зашифровать папку С:\Фамилия\КР-2. Включить аудит отказа для этой папки. От имени другого пользователя, входящего в группу «Администраторы», попытаться открыть папку С:\Фамилия\КР-2 и найти в журнале безопасности Windows информацию об этом событии.
2. Создать новую группу «КР-Фамилия», добавить в нее двух пользователей. Для вашего пользователя запретить выполнение файлов со съемных дисков, настроив параметр соответствующей политики.
3. Создать новую группу «КР-Фамилия», добавить в нее двух пользователей. Для вашего пользователя удалить список всех программ из меню «Пуск», настроив параметр соответствующей политики.
4. Создать новую группу «КР-Фамилия», добавить в нее двух пользователей. Включить аудит отказа для папки С:\Фамилия\КР-1. От имени пользователя, входящего в группу «Администраторы», попытаться открыть папку С:\Фамилия\КР-1 и найти в журнале безопасности Windows информацию об этом событии.
5. Создать новую группу «КР-Фамилия», добавить в нее двух пользователей. Включить аудит успеха для папки С:\Фамилия\КР-2. От имени пользователя, входящего в группу «Администраторы», открыть папку С:\Фамилия\КР-2 и найти в журнале безопасности Windows информацию об этом событии.

Образец экзаменационного билета

<table>
<tr><td colspan="3">Дальневосточный государственный университет путей сообщения</td></tr>
<tr><td>Кафедра
(к307) Финансы и бухгалтерский учёт
5
семестр, учебный год</td><td>Экзаменационный билет №
по дисциплине
Практикум по информационной безопасности
для направления подготовки / специальности
38.05.01 Экономическая безопасность
профиль/специализация
38.05.01 специализация N 1 "Экономико- правовое обеспечение экономической безопасности"</td><td>«Утверждаю»
Зав. кафедрой
Немчанинова М.А., канд. экон. наук, доцент
«___» _____ 20 __ г.</td></tr>
<tr><td colspan="3">1. Сетевые возможности ОС Windows (ОПК-6)</td></tr>
<tr><td colspan="3">2. Средства и методы сбора информации о вычислительной сети (ОПК-7)</td></tr>
<tr><td colspan="3">3. Запретить пользователю Student доступ к съемным запоминающим устройствам. (ПК-5)</td></tr>
</table>

Примечание. В каждом экзаменационном билете должны присутствовать вопросы, способствующих формированию у обучающегося всех компетенций по данной дисциплине.

3. Тестовые задания. Оценка по результатам тестирования.

Компетенция ОПК 6, ОПК 7, ПК 5

Вопросы тестирования. Модуль 1.

1. Задание {{ 63 }} Опр_инф_безоп

Выберите правильный ответ

Защищенность информационной среды общества посредством различных средств и методов - это …

- ☐информационная безопасность
- ☐ информационная угроза
- ☐ информатизация общества
- ☐ информационная среда

2. Задание {{ 64 }} Опр_информ_угроза

Выберите правильный ответ

Неблагоприятное событие в информационной среде - это …

- ☐ информационная угроза
- ☐ информационное обеспечение
- ☐ правовое обеспечение
- ☐ информационный ущерб

3. Задание {{ 65 }} Угрозы_в_ИС

Выберите четыре правильных ответа

В информационных системах существуют следующие виды угроз информационной безопасности:

- ☐ нарушение достоверности информации
- ☐ нарушение целостности информации
- ☐ нарушение доступности информации
- ☐ нарушение конфиденциальности информации
- ☐ нарушение актуальности информации

4. Задание {{ 66 }} Хар-ка_наруш_конфиденциальности

Выберите правильный ответ

Одной из наиболее серьезных угроз информационной безопасности, способной принести значительный моральный, политический и материальный ущерб, является …

- ☐ нарушение конфиденциальности информации
- ☐ нарушение достоверности информации
- ☐ нарушение целостности информации
- ☐ нарушение доступности информации

5. Задание {{ 67 }} Действия_для_нарушения_конфиденц

Выберите правильный ответ

Действие, в результате которого НЕ происходит нарушение конфиденциальности информации:

- ☐ разглашение информации
- ☐ утечка информации
- ☐ несанкционированный доступ к информации
- ☐ потеря части хранимой информации

6. Задание {{ 68 }} Соотв_угроз_и_примеров

Соответствие между информационными угрозами в информационных системах и иллюстрирующими их примерами:

Нарушение конфиденциальности информации	сбор сведений разведками иностранных государств
Нарушение достоверности информации	подделка сведений об абонентах в базе данных сотовой компании
Нарушение целостности информации	потеря части текстового документа при его передаче по электронной почте
Нарушение доступности информации	стирание информации на магнитных носителях в банковской системе

7. Задание {{ 69 }} Нарушение_целостности_информации

Выберите правильный ответ

Искажение, возникновение ошибок и потеря части передаваемой или хранимой информации, происходящие в каналах передачи или в хранилищах информации, - это …

- ☐ нарушение конфиденциальности информации
- ☐ нарушение достоверности информации
- ☐ нарушение целостности информации
- ☐ нарушение доступности информации

8. Задание {{ 70 }} Нарушение_достоверности

Выберите правильный ответ

Действие, НЕ приводящее к нарушению достоверности информации:

- ☐ фальсификация
- ☐ подделка
- ☐ мошенничество
- ☐ разглашение

9. Задание {{ 71 }} Нарушение_доступности

Выберите правильный ответ

Блокирование, невосстановимое искажение или уничтожение информации - это …

- ☐ нарушение конфиденциальности информации
- ☐ нарушение достоверности информации
- ☐ нарушение целостности информации
- ☐ нарушение доступности информации

10. Задание {{ 72 }} Способы_защиты_информации

Выберите четыре правильных ответа

В информационных системах существуют следующие способы защиты информации:

- ☐ препятствие
- ☐ маскировка
- ☐ принуждение
- ☐ обновление
- ☐ управление (регламентация)

11. Задание {{ 73 }} Способы_защиты_информации

Выберите четыре правильных ответа

В информационных системах существуют следующие способы защиты информации:

- ☐ нападение
- ☐ побуждение
- ☐ маскировка
- ☐ принуждение
- ☐ исключение

12. Задание {{ 74 }} Способы_защит_инф_Препятствие

Выберите правильный ответ

Способ защиты информации, при котором на пути возникновения или распространения информационной угрозы создается барьер, не позволяющий угрозе принять опасные размеры, - это …

- ☐ препятствие
- ☐ нападение
- ☐ маскировка
- ☐ принуждение

13. Задание {{ 75 }} Способы_защит_инф_Управлениие

Выберите правильный ответ

Способ защиты информации, определяющий процедуры и правила работы предприятий и учреждений, а также алгоритмы функционирования систем обработки информации, которые препятствуют возникновению информационных угроз, - это …

- ☐ препятствие
- ☐ управление (регламентация)
- ☐ маскировка
- ☐ принуждение

14. Задание {{ 76 }} Способы_защит_инф_Маскировка

Выберите правильный ответ

Способ защиты информации, связанный с преобразованием информации или скрываемого объекта с целью снижения степени их распознавания и затруднения к ним доступа, - это …

- ☐ препятствие
- ☐ управление (регламентация)
- ☐ маскировка
- ☐ принуждение

15. Задание {{ 77 }} Способы_защит_инф_Принуждение

Выберите правильный ответ

Способ защиты информации, связанный с соблюдением пользователями и персоналом информационной системы определенных правил обработки, передачи и применения информации под угрозой материальной, административной или уголовной ответственности, - это …

- ☐ препятствие
- ☐ управление (регламентация)
- ☐ маскировка
- ☑ принуждение

16. Задание {{ 78 }} Способы_защит_инф_Побуждение

Выберите правильный ответ

Способ защиты информации, при котором пользователи и персонал информационной системы за счет внутренней мотивации соблюдают правила обработки информации самостоятельно, - это …

- ☐ побуждение
- ☐ маскировка
- ☐ принуждение
- ☐ управление (регламентация)

17. Задание {{ 79 }} Средства_защит_инф_Нападение

Выберите правильный ответ

Способ защиты информации, имеющий целью заставить противника сосредоточить усилия на защите, ослабив деятельность по созданию информационных угроз, - это …

- ☐ принуждение
- ☐ нападение
- ☐ маскировка
- ☐ препятствие

18. Задание {{ 80 }} Средства_защит_инф_1

Выберите правильный ответ

К физико-техническим средствам защиты информации в информационных системах НЕ относятся:

- ☐ физические
- ☐ аппаратные
- ☐ программные
- ☐ правовые

19. Задание {{ 81 }} Средства_защит_инф_2

Выберите правильный ответ

К организационно-социальным средствам защиты информации в информационных системах НЕ относятся:

- ☐ организационные
- ☐ законодательные
- ☐ морально-этические
- ☐ эргономические

20. Задание {{ 82 }} Средства_защит_инф_соотв_1

Соответствие между физико-техническими средствами защиты информации в ИС и их характеристиками:

Физические	механические, электрические и т.п. устройства и системы, функционирующие автономно и создающие различного рода препятствия на пути информационных угроз
Аппаратные	электронные, электронно-механические и т.п. устройства, встраиваемые в схемы аппаратуры системы обработки данных специально для решения задач защиты информации
Программные	программы или пакеты программ, входящие в состав программного обеспечения АИС с целью решения задач защиты информации

21. Задание {{ 83 }} Средства_защит_инф_соотв_2

Соответствие между организационно-социальными средствами защиты информации в ИС и их характеристиками:

Организационные	мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей
Законодательные	нормативно-правовые акты, регламентирующие права и обязанности лиц и подразделений, связанных с защитой информации, и устанавливающие ответственность за нарушение правил ее обработки
Морально-этические	формирование у сотрудника, имеющего доступ к секретной информации, системы определенных качеств, взглядов и убеждений, обучение его правилам и методам защиты информации

Тест по модулю 2.

Вопросы тестирования.

1. Защищенная паролем группа компьютеров в сети, которые могут совместно использовать изображения, музыку, видео, документы и принтеры, называется:

а) рабочая группа;
б) домен;
в) группа пользователей;
г) домашняя группа.

2. Функция, предназначенная для исключения случайного изменения пользователями системных параметров и защиты компьютера от несанкционированной установки и запуска ПО, это:

а) Active Directory;
б) UAC;
в) Network Service;
г) Internet Explorer.

3. Выберите утверждение, не подходящее к рис. 1:

а) учетная запись «Андрей» относится к группе «Пользователи»;
б) учетная запись «serg» относится к группе «Администраторы»;
в) учетная запись «Администратор» защищена паролем;
г) для входа в систему под учетной записью «Андрей» необходимо ввести пароль.

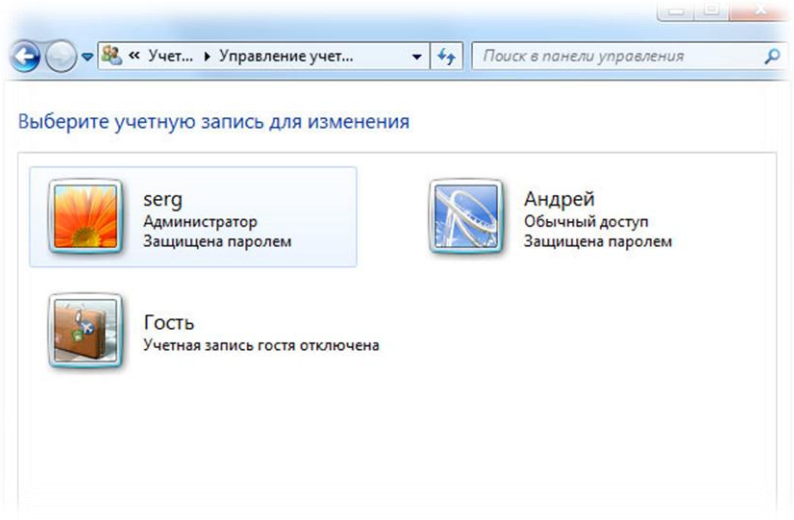

Рис. 1. Управление учетными записями пользователей с помощью Панели управления.

4. Соответствие между паролем и его характеристикой, не соответствующей правилам создания надежных паролей:

а)	Anastasia_1991	д)	содержит число символов, меньшее необходимого количества;
б)	BEZOPASNOST	е)	очевидный;
в)	Rut9@5Z	ж)	наиболее популярный и часто используемый;
г)	123qwerty	з)	содержит однотипные символы

5. Диск/дискета сброса пароля позволяет:

а) войти в систему под доменной учетной записью «Root»;
б) сменить пароль локальной учетной записи, не входя в систему;
в) войти в систему и изменить пароль локальной учетной записи, не зная старого пароля;
г) создать новую учетную запись без входа в систему.

6. Для вызова окна «Учетные записи пользователей» предназначена команда:

а) Выполнить
б) control userpasswords2
в) lusrmgr.msc
г) cmd

7. Если учетная запись локального пользователя относится к типу «Обычный доступ», то она входит в группу пользователей:

а) Администраторы;
б) Обычный доступ;
в) Гости;
г) Пользователи.

8. Если учетная запись локального пользователя относится к типу «Администратор», то она входит в группу пользователей:

а) Администраторы;
б) Обычный доступ;
в) Гости;
г) Пользователи.

9. Выберите действие, которое нельзя выполнить с помощью «Панели управления» для любой учетной записи, если выполнен вход в систему под учетной записью «Администратор»:

а) добавить локальную учетную запись в несколько групп пользователей одновременно;
б) сменить пароль для локальной учетной записи или создать диск сброса пароля;
в) добавить учетную запись в группу «Пользователи»;
г) сменить имя или рисунок для локальной учетной записи.

10. Безопасность Windows и всей сети организации можно значительно повысить, выполнив следующее действие:

а) защитить паролями только учетные записи, входящие в группу «Администраторы»;
б) защитить паролями только учетные записи, входящие в группу «Пользователи»;
в) создать надежные пароли для всех учетных записей;
г) создать легко запоминающиеся пароли для всех учетных записей.

11. Соответствие между строками, в которых размещены сведения об учетной записи (см. рис. 1), и смыслом этой информации:

и) строка 1
к) строка 2
л) строка 3

м) тип учетной записи;
н) группа пользователей, в которую входит учетная запись;
о) имя учетной записи;
п) информация о наличии пароля для учетной записи.

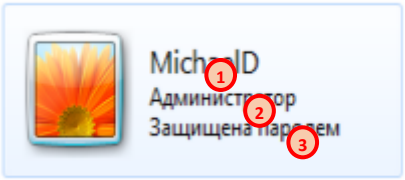

Рис. 1. Информация об учетной записи.

12. Для вызова окна «Учетные записи пользователей» предназначена команда:

д) Выполнить
е) control userpasswords2
ж) lusrmgr.msc
з) cmd

13. Информация из какого поля (см. рис. 2) будет использована для имени учетной записи на экране приветствия:

а) Пользователь;
б) Полное имя;
в) Описание;
г) нужное поле отсутствует на рисунке.

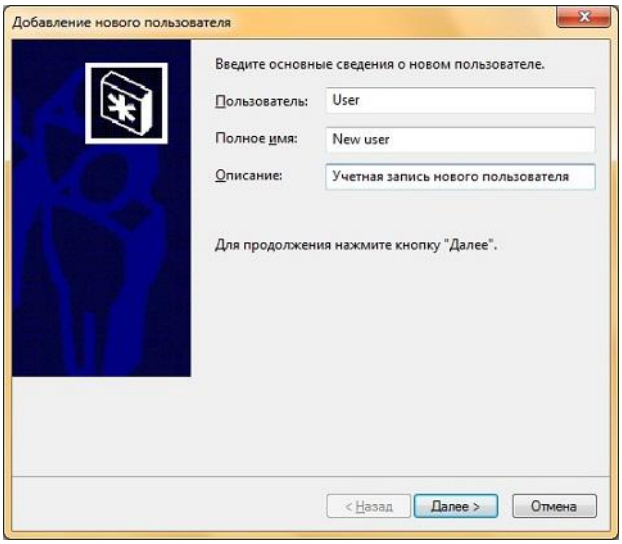

Рис. 2. Окно «Добавление нового пользователя».

14. Соответствие между инструментом Windows для работы с учетными записями и его характеристикой:

а) Панель управления
б) окно «Учетные записи

г) позволяет создавать/удалять/отключать учетные записи; добавлять учетную запись в несколько групп пользователей одновременно; создавать/удалять группы пользователей; устанавливать такие настройки, как: запрет смены пароля пользователем, требование

пользователей »

в) оснастка «Локальные пользователи и группы»

смены пароля при следующем входе в систему

д) позволяет создавать/удалять локальные учетные записи; изменять их тип, создавать/удалять/изменять пароли, менять рисунок и имя учетной записи; не позволяет явно добавить учетную запись в заданную группу пользователей

е) используется для управления учетными записями из командной строки с помощью команды «net user»;

ж) позволяет создавать/удалять учетные записи; добавлять их в одну из существующих групп пользователей; включать/отключать безопасный и автоматический вход в систему

15. Автоматический вход в систему – это:

а) вход в систему под выбранной заранее учетной записью без требования ввода имени пользователя и пароля;
б) требование нажатия сочетания клавиш «Alt+Ctrl+Del» перед появлением экрана приветствия;
в) предложение пользователю сменить пароль при первом входе в систему;
г) возможность сменить пароль на новый без входа в систему.

16. Безопасный вход в систему - это:

а) вход в систему под выбранной заранее учетной записью без требования ввода имени пользователя и пароля;
б) требование нажатия сочетания клавиш «Alt+Ctrl+Del» перед появлением экрана приветствия;
в) предложение пользователю сменить пароль при первом входе в систему;
г) возможность сменить пароль на новый без входа в систему.

Примерные задания теста

Полный комплект тестовых заданий в корпоративной тестовой оболочке АСТ размещен на сервере УИТ ДВГУПС, а также на сайте Университета в разделе СДО ДВГУПС (образовательная среда в личном кабинете преподавателя).
Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета, курсового проектирования.

Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.

Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.