

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 10.04.2023 15:42:52
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРАЗОВАНИЯ И НАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование кафедры полностью)

 М.О. Таныгин
(подпись, инициалы, фамилия)

«30» августа 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине
История информационного противоборства
(наименование дисциплины)

10.03.01 Информационная безопасность, профиль «Безопасность
автоматизированных систем в сфере информационных и коммуникационных
технологий»
(код и наименование ОПОП ВО)

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО

Тема 1. История возникновения органов защиты информации.

1. Криптография в древнем мире.
2. История появления первых служб информационного противодействия.
3. Первые законодательные акты в области информационной безопасности.
4. Появление понятия «государственная тайна».
5. Влияние развития средств коммуникации на деятельность по обеспечению информационной безопасности

Тема 2. Защита государственных интересов в XII – XVI вв.

1. Влияние информационной разведки на успешность средневековых боевых операций.
2. Особенности политического устройства России в 12-16 вв., влияющие на обеспечение защиты государственных интересов
3. Особенности защищённой переписки в средние века
4. Правовое регулирование защиты государственных интересов.

Тема 3. Защита государственных интересов в XVI - XVIII вв.

1. Внешняя разведка Российского государства в период 16-18 вв.
2. Органы государственной безопасности Российского государства в период 16-18 вв .
3. Аналитическая работа внешней разведки Российского государства в период 16-18 вв
4. Особенности региональной политики в области защиты государственных интересов

Тема 4. Защита государственных интересов в XIX веке.

1. Органы, отвечающие за обеспечение информационной безопасности в Российской Империи
2. Борьба со шпионажем в 18 в.
3. Используемые методики агентурной разведки и ОРМ
4. Розыск преступников в 19 в.
5. Правила защищённого документооборота в 19 в.
6. Ответственность должностных лиц за нарушение режима защищённого документооборота

Тема 5. Защита государственных интересов в 1900-1917 гг.

1. Органы политического сыска.
2. Военная разведка в начале 20 в.
3. Основные достоинства разведки и контрразведки Российской империи

Тема 6. Защита государственных интересов в период создания Советской власти и НЭПа.

1. Функции ВЧК.
2. Законодательные акты Советской власти в области информационного противоборства.
3. Функции Военно-статистического отдела
4. Назначение специального института консультантов при начальнике Региструпра
5. Структура и функции ГПУ
6. Особенности структур, отвечающих за информационное противоборство

Тема 7. Защита государственных интересов в 1928 – 1941 годах.

1. Изменение структуры военной разведки
2. Борьба с иностранными агентами
3. Возникновение советской резидентурной сети.
4. Промышленный шпионаж со стороны СССР

Тема 8. Защита государственных интересов в период великой отечественной войны.

1. Структура органов госбезопасности.
2. Основные успешные операции органов госбезопасности.
3. Методы пропаганды, используемые во время ВМВ.

Тема 9. Система безопасности СССР и России в XX – XXI веках

1. Функции структур, отвечающих за информационное противодействие
2. Работа с пропагандистскими инструментами
3. Информационная война с Западом, основные черты.
4. Информационные войны в современном мире
5. Средства ведения информационных войн.
6. Технологии манипулирования общественным мнением

Критерии оценки:

6-5 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий;

недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

2-1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1 «История возникновения органов защиты информации»

1. Информационное противоборство как составная часть вооруженной борьбы?
2. «Психологические операции» в Средние века.
3. Особенности информационно-пропагандистской деятельности.

Практическая работа № 2 «Защита государственных интересов в XII – XVI вв.»

- 1 Защита государственных интересов в XII - XIV веках
- 2 Защита государственных интересов в период образования централизованного государства.
- 3 Защита государственных интересов в период сословно-представительной монархии.
- 4 Защита государственных интересов во второй половине XVII – XVIII веках.

Практическая работа № 3 «Защита государственных интересов в XIX веке»

1. Информационное противоборство XIX века.
2. Информационное противоборство в период Первой мировой войны.
3. Защита государственных интересов в период с 1900 года по 1917 год.

Практическая работа №4 «Защита государственных интересов в 1928 – 1941 годах»

1. Защита государственных интересов в период создания Советской власти.
2. Защита государственных интересов в период НЭПа

Практическая работа №5 «Защита государственных интересов в период великой отечественной войны»

1. Защита государственных интересов во времена Сталинских репрессий.
2. Информационное противоборство времён Великой отечественной войны.

Практическая работа №6 «Система безопасности СССР и России в XX – XXI веках»

1. Современные представления о безопасности.
2. Характеристика национальной безопасности.
3. Характеристика региональной безопасности.
4. Характеристика глобальной безопасности.
5. Источники глобальных опасностей.
6. Новые параметры международной безопасности.

Критерии оценки для практических работ 1-3:

6-5 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

2-1 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие

и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

Критерии оценки для практических работ 4-6:

8-6 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

5-4 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

3-2 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

Задание №1

Какая угроза информационной безопасности является пассивной?

1. Копирование секретных данных.
2. Внедрение вредоносного программного обеспечения.
3. Кража носителей информации.
4. Удаление файла.

Задание №2

Угрозы нарушения целостности информации приводят к следующему результату:

1. Изменение, искажение или уничтожение информации.
2. Информация становится известной лицам, которые не должны иметь к ней доступ.
3. Снижается работоспособность автоматизированной системы, либо блокируется доступ к ее ресурсам.
4. Злоумышленнику становятся известны параметры автоматизированной системы.

Задание №3

К какому уровню доступа к информации в автоматизированной системе относится перехват данных, передаваемых по каналам связи?

1. Уровень средств взаимодействия с носителем.
2. Уровень носителей информации.
3. Уровень представления информации.
4. Уровень содержания информации.

Задание №4

Какая сетевая атака связана с превышением допустимых пределов функционирования сети?

1. Отказ в обслуживании (DoS –атака).
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Угадывание ключа.

Задание №5

Какая сетевая атака является характерной именно для беспроводных сетей?

1. Вещание радиомаяка.
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Отказ в обслуживании (DoS –атака).

Задание №6

Основной защитой от фишинга являются:

1. Фильтры.
2. Антивирусные программы.
3. Криптографические системы.
4. Системы видеонаблюдения.

Задание №7

Под политикой безопасности организации понимают:

1. Совокупность документированных управленческих решений, направленных на защиту информации.
2. Совокупность юридических законов в области защиты информации.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №8

Политика удаленного доступа – это:

1. Специализированная политика безопасности.
2. Базовая политика безопасности.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №9

Политики безопасности разделяют на уровни:

1. Верхний, средний и нижний.
2. Верхний и нижний.
3. Обобщенный и детальный.
4. Нет деления на уровни.

Задание №10

Какая криптосистема шифрования является асимметричной?

1. Алгоритм шифрования RSA.
2. Шифр Виженера.
3. Американский стандарт шифрования AES.
4. Стандарт шифрования ГОСТ 28147-89.

Задание №11

При шифровании методом Виженера слова «Банк» получилось зашифрованное сообщение «ВГТЛ». Какой был использован ключ?

1. 1-3-5
2. 2-6
3. 6-1-4
4. 8-5-2-3

Задание №12

Для проверки электронной цифровой подписи необходимо знать:

1. Открытый ключ отправителя.
2. Секретный ключ отправителя.
3. Два ключа отправителя: секретный и открытый.
4. Не требуется знания никаких ключей.

Задание №13

Под аутентификацией понимают:

1. Процедуру проверки подлинности заявленного пользователя, процесса, устройства.
2. Процедуру распознавания пользователя по его идентификатору.
3. Процедуру предоставления субъекту определенных полномочий и ресурсов в сети.
4. Регистрацию действий пользователя в сети.

Задание №14

Вероятность угадывания PIN –кода из 4 десятичных цифр за 3 попытки равна:

1. 0,0003.
2. 0,003

3. 0,00003.

4. 0,0004.

Задание №15

Различают следующие виды систем идентификации и аутентификации:

1. Электронные, биометрические и комбинированные.
2. Электронные и биометрические.
3. Электронные, биометрические и механические.
4. Электронные, биометрические и криптографические.

Задание №16

Какую функцию не может выполнять межсетевой экран?

1. Лечение файлов, зараженных вирусами.
2. Фильтрация трафика.
3. Трансляция сетевых адресов.
4. Регистрация событий.

Задание №17

Какой межсетевой экран обеспечивает наиболее высокий уровень безопасности?

1. Комплексный межсетевой экран.
2. Экранирующий маршрутизатор.
3. Шлюз сеансового уровня.
4. Прикладной шлюз.

Задание №18

Различают следующие варианты исполнения межсетевых экранов:

1. Программный и программно-аппаратный.
2. Программный и аппаратный.
3. Аппаратный и программно – аппаратный.
4. Существуют только программные межсетевые экраны.

Задание №19

Какая вредоносная программа не размножается, но способна удаленно управлять компьютером и воровать пароли?

1. Троянская программа.
2. Червь.
3. Файловый вирус.
4. Макровирус.

Задание №20

Какая антивирусная программа не конфликтует с другими антивирусами, но не имеет функции автоматического обновления антивирусной базы?

1. Dr. Web CureIt.
2. Kaspersky Internet Security.
3. Eset NOD 32 Antivirus.
4. Avira AntiVir Personal.

Задание №21

Какой метод выявления вируса позволяет обнаруживать только известные вирусы?

1. Обнаружение, основанное на сигнатурах.
2. Обнаружение программ подозрительного поведения.
3. Обнаружение вирусов при помощи эмуляции работы программы.
4. Эвристический анализ.

Задание №22

Сколько существует классов защищенности средств вычислительной техники от несанкционированного доступа?

1. 7.
2. 5.
3. 9.
4. 6.

Задание №23

Какой класс защищенности автоматизированных систем предъявляет наиболее высокие требования к информационной безопасности?

1. 1А
2. 1Г
3. 3Б
4. 3А

Задание №24

Вторая группа классов защищенности автоматизированных систем включает автоматизированные системы:

1. В которых работают несколько пользователей и все они имеют одинаковые права доступа к информации.
2. В которых работают несколько пользователей, и они имеют различные права доступа к информации.
3. В которых работает только один пользователь.
4. В которых работает один пользователь или несколько пользователей, имеющих одинаковые права доступа к информации.

Задание №25

В каком законе определены принципы и порядок засекречивания информации?

1. Закон “О государственной тайне”.
2. Закон “О безопасности”.
3. Закон “Об информации, информационных технологиях и о защите информации”.
4. Закон “Об авторском праве и смежных правах”.

Задание №26

Какой вид деятельности предприятий подлежит лицензированию ФСБ?

1. Эксплуатация негосударственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащих сведений, составляющих государственную тайну.
2. Сертификация, сертификационные испытания защищенных технических средств обработки информации (ТСОИ).

3. Аттестование систем информатизации, систем связи и передачи данных, технических средств приема, систем передачи и обработки информации, подлежащей защите.

4. Проведение специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) ТСОИ.

Задание №27

Является объектом авторского права, но не признается патентоспособным изобретением:

1. База данных.
2. Устройство.
3. Способ.
4. Вещество.

Задание №28

Основная масса угроз приходится на:

1. Шпионские программы.
2. Троянские программы.
3. Черви.

Задание №29

Какой вид идентификации и аутентификации является наиболее распространённым:

1. Одноразовые пароли.
2. Постоянные пароли.
3. системыPKI.

Задание №30

Под какие системы вирусы распространяются наиболее динамично:

1. Windows.
2. Mac OS.
3. Android.
4. Linux.

Задание №31

Заключительный этап построения системы защиты:

1. Планирование.
2. Сопровождение.
3. Анализ уязвимых мест.
4. Отчётность.

Задание №32

Какие угрозы безопасности информации являются преднамеренными:

1. Открытие электронного письма, содержащего вирус.
2. Ошибка персонала.
3. Не авторизированный доступ.
4. Открытие сайта.

Задание №33

Фишинг – это

А. разглашение открытой в СМИ информации;

Б. воровство конфиденциальной информации о пользователе, в

частности, с помощью подложных писем из банка.

В. система «Банк-Клиент».

Задание №34

Основной критерий содержания эффективной пропаганды:

- А) Наличие центрального тезиса.
- Б) Лёгкость для понимания целевой аудиторией.
- В) Сложность для критики.
- Г) Привлекательность фона.

Задание №34

Информационная война – это ...

1. действия военных структур, направленные на достижение информационного превосходства при одновременном обеспечении собственной безопасности и защиты
2. любые действия, направленные на поддержку национальной военной стратегии путем воздействия на информацию и информационные системы противника при одновременном обеспечении собственной безопасности и защиты
3. противоправные действия, направленные на достижение информационного превосходства путем активного воздействия на информацию и информационные системы противника с помощью недостоверной или неполной информации при одновременном обеспечении собственной безопасности и защиты
4. уничтожение или повреждение информационных систем противника
5. любые действия, направленные на достижение информационного превосходства, на поддержку национальной военной стратегии путем активного воздействия на информацию и информационные системы противника для достижения поставленных целей при одновременном обеспечении собственной безопасности и защиты

Задание №35

Исключите неправильный постулат:

1. информация не связана с определенным конкретным носителем
2. информация не существует без материального носителя
3. содержание информации меняется одновременно со сменой материального носителя

Задание №36

Исключите неверные высказывания

1. Информационные продукты – это документированная информация
2. Информационные продукты – это отдельные документы и массивы документов
3. информационные продукты – это документы и массивы документов, содержащиеся только в информационных системах
4. информационные продукты – это любые сведения, содержащие полезную информацию

Задание №37

Информационная система – это ...

1. совокупность информации, содержащейся в базах данных, и информационного продукта
2. информация и совокупность информационных технологий
3. информационные технологии и средства, обеспечивающие обработку информации
4. совокупность информации, содержащейся в базах данных, информационных технологий и средств, обеспечивающих обработку информации
5. совокупность информации, содержащейся в базах данных, информационных технологий, средств, обеспечивающих обработку информации, и информационный продукт

Задание №38

К государственной тайне не относятся сведения, защищаемые государством ..., распространение которых может нанести ущерб государству.

1. в экономической области
2. в контрразведывательной деятельности
3. в оперативно-разыскной деятельности
4. о частной жизни политических деятелей

Задание №39

Исключительные права авторов программ для ЭВМ
право авторства

право на неприкосновенность программы для ЭВМ

право на модификацию программы для ЭВМ

право на обнародование программы для ЭВМ

Задание №40

К служебной тайне не относится

1. вред, причиненный здоровью работника в связи с производственной травмой
2. тайна деятельности соответствующего органа
3. профессиональная тайна

Задания в открытой форме

1. Основными объектами _____ воздействия являются, с одной стороны, _____ - _____ системы различного масштаба и назначения, с другой - организационно-психологические объекты (психика отдельной личности; психологические явления и процессы в социальных общностях, группах различного масштаба, в обществе в целом; феномены общественного сознания; социальнополитические системы и процессы).
2. Исходя из этого, выделяются два основных направления _____ - _____ — информационно-техническое (ИТ) и информационно-психологическое (ИП).

3. Основой _____ - _____ борьбы являются средства массовой информации и коммуникации.
4. _____ — это соперничество социальных систем в информационно-психологической сфере с целью усиления влияния на определенные сферы социальных отношений и установления контроля над источниками стратегических ресурсов.
5. _____ информационного противоборства является любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе — применение информационного оружия) либо иного воздействия (силового, политического, экономического и т.д.), результатом которого будет модификация его свойств как информационной системы.
6. Объектом информационного противоборства может стать любой компонент или сегмент информационно-психологического пространства, в том числе — следующие виды:
_____.
7. К субъектам информационного противоборства относят _____.
8. Проблемы в области безопасности электронного бизнеса включают _____.
9. Основные функциональные компоненты организации комплексной системы информационной безопасности _____.
10. _____ — ставит перед собой цель лишить контроля налаженную связь между командованием и исполнителем.
11. _____ — предусматривает сбор ценной информации для нападения и собственной защиты. Электронная война — целью является вывод из строя всех электронных коммуникаций.
12. _____ — взлом и доступ к любым данным (электронная почта, банковские карты, личные файлы, переписки и так далее) и несанкционированное их использование. Экономическая война — информационная блокада (ограничение коммерческой деятельности) или информационный империализм (политическая информационная атака).
13. _____ — ставит перед собой цель захватить компьютерные данные, выследить объект, нарушить работу инфраструктуры, полагающейся на информационные технологии.
14. Электронная война направлена против средств электронных коммуникаций _____.
15. Психологическая война - пропаганда, информационная обработка населения, направленная на _____.
16. Хакерская война подразумевает диверсионные действия против _____.

17. Кибервойна отличается от "обычного" хакерства _____.
18. К служебной тайне не относится _____.
19. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений которые _____.
20. Не представляют угрозу информационной безопасности общества _____.

Задания на установление соответствия

1. Установить соответствие между средствами и функциями

1	Человек, информация, технические средства	А	Информационное оружие
2	Целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние на функционирование и развитие психологической среды общества, психику и поведение населения, руководства страны, военнослужащих	Б	Информационное воздействие
3	Комплекс технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника в целях выведения их из строя, получения или модификации содержащихся в них данных, целенаправленного продвижения выгодной информации (или дезинформации)	В	Элементы информационного пространства
4	Применение средств, позволяющих производить с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия	Г	Психологическое воздействие

2. Установить соответствие между информационными ресурсами телекоммуникационных систем и описаниями функционирования элементов

1	Автоматизированные пользовательские системы, которые собирают, хранят, обрабатывают и распространяют информацию	А	Информация
2	Данные во всех формах ввода, хранения, обработки и вывода с помощью информационных систем, в любых формах, которые используются для принятия управленческих решений	Б	Инфраструктура
3	Средства (аппаратное и программное обеспечение, системы управления базами данных, сеть, мультимедиа, среда, в которой все это функционирует), которые делают возможным работу приложений	В	Персонал
4	Люди (специалисты), требующиеся для планирования, организации, установки, эксплуатации и развития информационных систем и сервисов, нанимаемые по контрактам	Г	Приложения

3. Установить соответствие между терминами и их значениями

1	Информационная операция	А	действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем
2	Информационная война	Б	комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-

			политическое руководство
3	Информационное превосходство	В	способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое
4	Информационное противоборство	Г	проведения мероприятий, направленных против систем управления и принятия решений (Command & Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA)

4. Установить соответствие

1	Системность целевая	А	Подразумевает единство организации всех работ по защите информации и их управления
2	Системность пространственная	Б	Защищенность информации рассматривается как составная часть общего понятия качества информации
3	Системность временная	В	Защищенность основанная на принципе непрерывности функционирования системы защиты
4	Системность организационная	Г	Защищенность рассматривается как увязка вопросов защиты информации

5. Установить соответствие мер защиты информации

1	Правовые	А	Реализуются в виде механических, электрических и электронных устройств, предназначенных для предотвращения проникновению и доступу потенциального нарушителя к компонентам защиты
2	Морально-этические	Б	Представляют собой организационно-технические и организационно-правовые

			мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации
3	Административные	В	К ним относятся нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий
4	Технические	Г	Определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил

6. Установить соответствие мер защиты информации

1	К сведениям особой важности следует относить	А	Все иные из числа сведений, составляющих государственную тайну
2	К совершенно секретным сведениям следует относить	Б	Такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства или отраслям экономики РФ в одной или нескольких областях деятельности
3	К секретным сведениям следует относить	В	Такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности

7. Установить соответствие

1	Нарушитель	А	намеренно идущий на нарушение из корыстных побуждений
2	Злоумышленник	Б	лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию

			или осознанно со злым умыслом или без такового, и использующее для этого различные возможности, методы и средства.
3	взломщик	В	Лицо, которое с корыстными целями осуществляет несанкционированный доступ к данным или программам

8. Установить соответствие между терминами и их значениями

1	Техническая сфера	А	бласть информационного пространства, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой функционируют системы управления, связи и разведки
2	Психологическая сфера	Б	область информационного пространства, которая объединяет мышление личного состава ВС и мирного населения. Это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства, мораль, понятие сплоченности подразделений, уровень подготовки, опыт, понимание ситуации и общественное мнение
3	Информационная обстановка	В	совокупность людей, организаций и систем, собирающих, обрабатывающих, доводящих информацию или действующих на ее основе
4	Элементы информационной обстановки	Г	руководители, лица, принимающие решения (ЛПР), люди организации и системы

9. Установить соответствие между

1	Перехват паролей	А	мошенничество возможно с участием специальных программ, которые имитируют на экране
---	------------------	---	---

			монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы.
2	«Маскарад»	Б	действия в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе -передача ложных данных в системе от имени другого человека
3	Незаконное использование привилегий	В	название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя

10. Установить соответствие между типологиями «Информационных войн»

1	психологические операции	А	использование информации для воздействия на аргументацию солдат врага
2	электронная война	Б	не позволяет врагу получить точную информацию
3	дезинформация	В	предоставляет врагу ложную информацию о наших силах и намерениях
4	физическое разрушение	Г	может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем

11. Установить соответствие уровней информационной борьбы

1	Вещественно-энергетический	А	Борьба на уровне носителей информации, то есть все виды скрытия информации и уничтожения информационных систем каналов и информации в них
2	Синтаксический	Б	Борьба на уровне структур знаковых систем, то есть все

			виды кодирования , использования шифров и т.п
3	Семантический	В	борьба на уровне смыслового содержания информации, то есть предоставление противнику бессмысленной или недостоверной информации (дезинформация)
4	прагматический	Г	борьба на уровне полезности информации, то есть либо изменения целей противостоящей стороне по отношению к использованию информации, либо предоставление ему бесполезной информации

12. Установить соответствие между терминами и их значениями

1	Ресурсы информационной обстановки	А	материальные средства и системы, используемые для сбора, анализа, применения или доведения информации
2	Информационное измерение	Б	область, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой существует логика функционирования систем управления, связи и разведки. В битве за информационное превосходство эта область является самой чувствительной к информационным воздействиям, так как именно это измерение связывает реальный физический мир с логикой функционирования технических систем сбора, передачи и обработки информации, а через них — с сознанием человека, функционирующим в познавательном измерении
3	Познавательное измерение	В	область мышления бойца и мирного населения. Это область, в которой формируются

			<p>намерения командиров, доктрины, тактика, методы противоборства.</p> <p>Нематериальные активы лидерства, морали, сплоченности подразделений, уровень подготовки, опыта, понимания ситуации и общественного мнения — это всё элементы этой области</p>
4	Физическое измерение	Г	<p>традиционная область войны. Эта область объединяет традиционные сферы противоборства — землю, море, воздух и космическое пространство. Это область, в которой функционируют физические платформы вооружений и технические системы управления и связи. Поэтому элементы этой области проще всего идентифицируемы. Боевая мощь в этой области традиционно измеряется эффектами физического поражения</p>

13. Установить соответствие между излучениями каналов

1	Побочные электромагнитные излучения и наводки (ПЭМИН)	А	<p>паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники. В зависимости от среды распространения различают</p>
2	Побочные электромагнитные излучения (ПЭМИ)	Б	<p>нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации</p>
3	Информативными ПЭМИ	В	<p>сигналы, представляющие собой ВЧ несущую, модулированную информацией обрабатываемой на СВТ (например, изображением,</p>

			выводимым на экран монитора, данными, обрабатываемыми на устройствах ввода-вывода и т.д.)
4	Неинформативными ПЭМИ	Г	сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ

14. Установить соответствие между терминами и их значениями

1	Кибербезопасность	А	набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, ресурсов организации и пользователя
2	Киберпространство	Б	среда, которая представляет собой следствие результата взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологий устройств и сетей, подключенных к ней, которых не существует в какой-либо физической форме
3	Кибернетика	В	наука об оптимальном управлении сложными динамическими системами, изучающая общие принципы управления и связи, лежащие в основе работы самых разнообразных по природе систем — от самонаводящихся ракет-снарядов и быстродействующих вычислительных машин до сложного живого организма

15. Установить соответствие между основными принципами защиты информации

1	Принцип законности	А	необходимо нормативно- правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации
2	Принцип защиты информации	Б	основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения секретов
3	Принцип приоритета	В	объектом засекречивания не могут быть сведения, которые государство обнародует или сообщает согласно конвенциям или соглашениям
4	Принцип собственности и экономической целесообразности	Г	право собственникам информации принимать меры к защите этой информации, а также оценивать ее потребительские свойства

16. Установить соответствие между терминами и определениями

1	Специальные обследования помещений	А	комплекс мер в области защиты информации в части проведения работ по выявлению электронных устройств, предназначенных для негласного получения сведений в помещениях, где циркулирует информация ограниченного пользования
2	Аттестация объекта защиты	Б	официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований РД по ЗИ
3	Основные технические средства и системы	В	технические средства и системы, а также их коммуникации,

			используемые для обработки, хранения и передачи конфиденциальной информации
4	Нормирование показателей защищенности	Г	установление нормативными документами численных значений показателей защищенности информации

17. Установить соответствие между элементами и функциями

1	Дробление	А	знание какой-то одной части информации не позволяет восстановить всю технологию в целом
2	Кодирование	Б	метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи
3	Шифрование	В	метод защиты информации, используемый при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником

18. Установить соответствие между элементами и функциями

1	Случайные антенны	А	вспомогательные технические средства, их соединительные линии, а также линии электропитания, посторонние проводники и цепи заземления, при непосредственном подключении к которым средств разведки ПЭМИН возможен перехват информационных сигналов
2	Сосредоточенные	Б	телефонный аппарат, громкоговоритель радиотрансляционной сети,

			датчик пожарной сигнализации и т. д., подключенные к линии, выходящей за пределы КЗ
3	Распределенные	В	кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ

19. Установить соответствие между терминами и определениями

1	Автоматизированная система (АС)	А	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функции
2	Контролируемая зона (КЗ)	Б	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств
3	Специальные исследования (СИ)	В	выявление с использованием контрольно-измерительной аппаратуры возможных каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем
4	Специальная проверка (СП)	Г	проверка технических средств и систем объекта защиты с целью выявления возможно внедренных электронных устройств съема информации (закладочных устройств)

20. Установить соответствие классификации угроз

1	Состояние источника угрозы	А	в самой системе, что приводит к ошибкам в работе и сбоям при реализации ресурсов АС; в пределах видимости АС, например, применение подслушивающей аппаратуры, похищение информации в
---	----------------------------	---	--

			распечатанном виде или кража записей с носителей данных
2	Степень влияния	Б	активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность, например, использование вредоносных вирусов или троянов; пассивная угроза – та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему.
3	Возможность доступа сотрудников к системе программ или ресурсов		вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного); вред наносится после согласия доступа к ресурсам системы.
4	Способ доступа к основным ресурсам системы	Г	применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы; использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя.

Задания на установление правильной последовательности

1. Установить в историческом порядке этапы развития информационного противоборства:

1. Распространение грамотности, в условиях широкого охвата населения новыми носителями информации: письмами, листовками, книгами, газетами, журналами и др.

2.Использование в качестве объекта воздействия - психику человека (носитель и средство доведения информации – человек).

3. Появление персональных компьютеров и межгосударственных телекоммуникационных сетей, особенно Интернета.

4. Возникновение новых носителей информации и новых средств доставки информации, появившихся благодаря открытию электричества: телеграфа, телефона, радио, кино, телевидения, звукоусилительной аппаратуры и т.п.

2.Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам

2. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet

3. Защита внешних каналов передачи информации

4. Разработка политики информационной безопасности

5. Анализ угрозы безопасности

3. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций

2. Передача управления программе-носителю вируса

3. Поиск жертвы

4. Заражение найденной жертвы

5. Загрузка вируса в память

4. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности

2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности

3. Разработка политики антивирусной безопасности

4. Разработка плана обеспечения антивирусной безопасности

5. Расположить этапы проведения аудита информационной безопасности:

1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы

2. Анализ полученных данных

3. Сбор исходных данных

4. Разработка регламента проведения аудита

6. Установить этапы построения программы обеспечения безопасности:

1. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности

2. Регулярный контроль пошаговой реализации плана безопасности

3. Установление уровня безопасности

4. Формирование политики безопасности организации
5. Определение ценности технологических и информационных активов организации

7. Установить действия этапа анализа рисков:

1. Оценка вероятности того, что угроза будет реализована на практике
2. Оценка рисков технологических и информационных активов
3. Идентификация и оценка стоимости технологических и информационных активов
4. Анализ угроз, для которых технологические и информационные активы являются целевым объектом

8. Установить последовательность процессов для обнаружения и выдачи сигнала тревоги:

1. Одно системное событие не является неизбежно достаточным, чтобы утверждать, что это опасность
2. Если результат этой совокупности превышает пороговую величину, выдается сигнал тревоги
3. Совокупность событий должна сравниваться с заранее установленной пороговой величиной
4. Каждое нарушение безопасности должно генерировать системное событие

9. Расположить параметры для группировки данных на сервере сбора информации об атаке:

1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

10. Расположить в порядке возрастания даты разработки стандартов информационной безопасности:

1. ISO 27001:2005
2. ISO/IEC 17799
3. ISO/IEC 15408
4. «Критерии оценки доверенных компьютерных систем»

11. Расположить этапы процесса управления рисками информационной безопасности:

1. Классификация рисков, выбор методологии оценки рисков и проведение оценки
2. Анализ угроз и их последствий, определение слабостей в защите
3. Выбор, реализация и проверка защитных мер

4. Оценка остаточного риска
5. Идентификация активов и ценности ресурсов, нуждающихся в защите
6. Выбор анализируемых объектов и степени детальности их рассмотрения

12. Расположить современные проблемы информационного противоборства по их важности

1. По мере развития социальных институтов информационные процессы усложняются, что приводит к усложнению процессов принятия решения

2. Система — цель информационной войны может включать любой элемент в эпистемиологии противника

3. Буквально на наших глазах меняются технологии интернет-коммуникаций: если еще несколько лет назад основу составляли интернет-СМИ

4. Среди сетевых ресурсов все большую роль играют онлайн-социальные сети

13. Выделите по важности 3 части информационного противоборства

1. Стратегический анализ

2. Информационное воздействие

3. Информационное противодействие

14. Расположите по важности главные объекты информационно-психологического противоборства

1. психика политэлиты и населения противостоящих сторон

2. система формирования общественного сознания

3. система формирования общественного мнения

4. система принятия решений

15. Расположите по порядку основные формы информационного противоборства

1. информационное доминирование

2. информационная асимметрия

3. информационное сдерживание

4. информационная агрессия

5. контроль и управление информацией

16. Выберите правильную последовательность этапов развития информационной безопасности после первой половины 20-го века:

1. Обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в

локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

2.Связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьезнее. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

3.Связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

17. Выберите последовательность уровней защищенности персональных данных

1. специальные категории ПДн
2. биометрические ПДн
3. общедоступные ПДн
4. иные категории ПДн

18. Выберите правильную последовательность этапов оценки угроз безопасности информации:

1. Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
2. Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
3. Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
4. Оценка способов реализации (возникновения) угроз безопасности информации;
5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
6. Оценка сценариев реализации угроз безопасности информации в системах и сетях.

19. Выберите правильную последовательность этапов жизненного цикла информационного сервиса:

1. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.
2. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.
3. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.
4. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

20. Устранение уязвимости состоит из следующих этапов:

1. Установка программного модуля для устранения угрозы информационной безопасности.
2. Разработка «патча» (заплатки), призванного устранить существующий пробел.
3. Появление сигнала от пользователей или от администратора сети о наличии слабого места в информационной системе.

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1

Проанализировать современный уровень развития информационного оружия относительно развития и применения типов информационного оружия в конфликтах второй половины XX–начала XXI века

Компетентностно-ориентированная задача № 2

Рассмотреть компьютерную систему как объект информационного воздействия (с помощью информационного оружия). Описать методы нарушения конфиденциальности, целостности и доступности информации как угроз национальной безопасности.

Компетентностно-ориентированная задача № 3

На основе документов, определяющих политику государства в области национальной безопасности, следующих стран:

a. Стран Европейского союза: «EU strategic communication to counteract anti-EU propaganda by third parties», «An Open, Safe and Secure Cyberspace».

b. США (The National Security Strategy).

определить следующее:

a. угрозы безопасности, существующие на уровне страны или нации (объекты и угрозы информационной войны);

b. источники угроз (внешние и внутренние);

c. национальные интересы (в том числе их основные составляющие) и угрозы информационной безопасности в информационной сфере;

d. основные направления обеспечения информационной безопасности государства, в том числе технических объектов информационной сферы государства в условиях информационной войны.

Компетентностно-ориентированная задача № 4

На основе документов, определяющих политику государства в области национальной безопасности, следующих стран:

a. Стран Европейского союза: «EU strategic communication to counteract anti-EU propaganda by third parties», «An Open, Safe and Secure Cyberspace».

b. США (The National Security Strategy).

Произвести сравнение и анализ указанных выше документов между собой и с Доктриной информационной безопасности Российской Федерации. Выявить общие черты и отличия.

Компетентностно-ориентированная задача № 5

1. Провести сравнительный анализ опыта РФ и ведущих зарубежных

стран в области противодействия информационно-психологическому воздействию.

2. На их основе предельно методы противодействия информационно-психологическому воздействию (методы информационно-психологического противодействия), методы защиты личности от информационно-психологических воздействий в СМИ и СМК.

Компетентностно-ориентированная задача № 6

1. Приведите перечень средств информационно-психологического воздействия и манипулирования мнением и их описание (ложные авторитеты, сокрытие фактов, использование ярко выраженной эмоциональной окраски и пр.).

2. Отберите два информационных сообщения, размещенных в СМИ и/или СМК разными сторонами противоборства, на тему выбранного события.

3. Проведите фактологический анализ данных сообщений.

Компетентностно-ориентированная задача № 7

Выберите некоторое событие (информационный повод), вызвавшее активные обсуждения, дискуссии в СМИ и СМК, по тематике которого велось активное информационное противоборство. Для события в целом определите заинтересованные стороны, цели, сценарии, используемые методы информационно-психологического воздействия. Отберите два информационных сообщения, размещенных в СМИ и/или СМК разными сторонами противоборства, на тему выбранного события. Проведите фактологический анализ данных сообщений.

Компетентностно-ориентированная задача № 8

1. Провести сравнительный анализ опыта РФ и ведущих зарубежных стран в области противодействия информационно-психологическому воздействию.

2. На их основе сформулировать предложения по решению проблем, вызванных негативным влиянием информационных войн.

Компетентностно-ориентированная задача № 9

1. Определить характеристику канала коммуникации, СМИ/СМК и влияние их специфики на текст (направленность издания, интересы и потребности аудитории).

2. Дать характеристику текста с точки зрения его содержания: тема, замысел, идея как воплощение целевой установки.

3. Определить отношение автора к тематике сообщения.

4. Определить виды информации, использованной в тексте: описательная (фактологическая), оценочная (рефлексивная), нормативная, приведите обоснование.

5. Определить факторы, которые оказывают решающее влияние в организации фактического материала, выборе форм предъявления фактов и

системы доказательств:

- назначение, функция, целевая установка текста – сообщить новость, рассказать о событии, явлении, проанализировать ситуацию, создать некоторый образ личности и прочие;
- объект отображения – область реальной действительности, которой касается сообщение или которую исследует автор статьи;
- предмет отображения и фактическая основа – факт (информационный повод – «жесткая» или «мягкая» новость), ситуация, проблема, человек (а также факт, событие, явления, процессы, ситуации, сообщения СМИ, книги, фильмы – информационные явления, дающие повод для подготовки рецензий, обзоров).

Компетентностно-ориентированная задача № 10

1. Провести сравнительный анализ опыта РФ и ведущих зарубежных стран в области противодействия информационно-психологическому воздействию.

2. На их основе разработать предложения и рекомендации по совершенствованию действующей политики РФ и государственной политики в информационной сфере с учетом международного опыта.

Компетентностно-ориентированная задача № 11

Включите шифрование твердотельного накопителя используя операционную систему Windows 10

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.