**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»**

Комплект контрольно-оценочных средств

по

МДК 02.02 Криптографические средства защиты информации

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2021

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553.

Составитель:
Ляшенко А.В., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

В соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) колледж самостоятельно планирует результаты обучения по МДК 02.02 Криптографические средства защиты информации, которые соотнесены с требуемыми результатами освоения образовательной программы (компетенциями выпускников). Совокупность запланированных результатов обучения должна обеспечивать выпускнику освоение всех общих компетенций (далее – ОК), профессиональных компетенций (далее – ПК), установленных ФГОС СПО.

Контрольно-оценочные средства (далее - КОС) предназначены для контроля и оценки образовательных достижений обучающихся по МДК 02.02 Криптографические средства защиты информации.

КОС включают типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, и (или) практического опыта, характеризующих этапы формирования компетенций в процессе освоения образовательной программы для проведения текущего контроля успеваемости обучающихся и организации промежуточной аттестации в форме экзамена.

КОС разработан на основании рабочей программы МДК 02.02 Криптографические средства защиты информации

1.2 Планируемые результаты освоения междисциплинарного курса:

В результате освоения междисциплинарного курса обучающийся должен **уметь**:

– У.1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– У.2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– У.4 применять программные и программно-аппаратные средства для защиты информации в базах данных;

– У.5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– У.6 применять математический аппарат для выполнения криптографических преобразований;

– У.7 использовать типовые программные криптографические средства, в том числе электронную подпись;

– У.8 применять средства гарантированного уничтожения информации;

– У.9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– У.10 осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В результате освоения междисциплинарного курса обучающийся должен **знать**:

– З.1особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– З.2методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

– З.3типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– З.4основные понятия криптографии и типовых криптографических методов и средств защиты информации;

– З.5особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

– З.6типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

В результате освоения междисциплинарного курса обучающийся должен **иметь практический опыт:**

− ПО1 установки, настройки программных средств защиты информации в автоматизированной системе;

−ПО2 обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

− ПО3 тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;

− ПО4 решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

− ПО5 применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

− ПО6 учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

−П7 работы с подсистемами регистрации событий;

− ПО8 выявления событий и инцидентов безопасности в автоматизированной системе.

Профессиональные и общие компетенции, которые формируются при изучении междисциплинарного курса:

ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 02 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие

ОК 04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 09 Использовать информационные технологии в профессиональной деятельности

ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Планируемые личностные результаты освоения рабочей программы междисциплинарного курса:

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в

сетевой среде личностно и профессионального конструктивного «цифрового следа»

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.3 Контроль и оценка результатов освоения междисциплинарного курса

Таблица 1

Код и наименование профессиональных и общих компетенций, формируемые в рамках междисциплинарного курса	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Тестирование, экспертное наблюдение, выполнения практических работ, оценка решения ситуационных задач.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Тестирование, экспертное наблюдение, выполнения практических работ, оценка решения ситуационных задач.
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	Тестирование, экспертное наблюдение, выполнения практических работ, оценка решения ситуационных задач.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	Тестирование, экспертное наблюдение, выполнения практических работ, оценка решения ситуационных задач.
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	Тестирование, экспертное наблюдение, выполнения практических работ, оценка решения ситуационных задач.
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Тестирование, экспертное наблюдение, выполнения практических работ, оценка решения ситуационных задач.

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения междисциплинарного курса для проведения текущего контроля успеваемости обучающихся

Раздел 1. Математические основы криптографии

Вариант 1

Задание №1. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какое число является наибольшим общим делителем (НОД) чисел 36 и 60? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) 12
б) 6
в) 18
г) 4

Задание №2. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Найдите обратное число к числу 7 по модулю 26. ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) 15
б) 11
в) 19
г) 5

Задание №3. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
В каком случае числа называются взаимно простыми? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) Если их НОД равен 1.
б) Если одно из чисел делится на другое.
в) Если оба числа четные.
г) Если сумма чисел равна 0.

Задание №4. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какая функция используется в RSA-шифровании для вычисления открытого ключа e? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) e=p+q$e=p+q$
б) e=(p−1)(q−1)$e=(p-1)(q-1)$
в) e=gcг(p−1,q−1)$e=gcг(p-1,q-1)$
г) e=φ(n)$e=\varphi(n)$, где φ(n)$\varphi(n)$ — функция Эйлера.

Задание №5. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что такое функция Эйлера (φ(n)$\varphi(n)$)? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) Количество положительных целых чисел меньше n, взаимно простых с n.
б) Сумма всех делителей числа n.
в) Наибольший общий делитель двух чисел.
г) Количество всех натуральных делителей числа n.

Задание №6. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какой алгоритм используется для быстрого возведения числа в степень по модулю? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) Алгоритм Евклида
б) Метод деления пополам

в) Китайская теорема об остатках
г) Алгоритм Шора

Задание №7. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Сколько битов имеет ключ в симметричной криптосистеме AES-256? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) 128 бит
б) 192 бит
в) 256 бит
г) 512 бит

Задание №8. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что означает односторонняя функция в контексте криптографии? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) Функция, которую легко вычислить, но трудно обратить.
б) Функция, которая всегда возвращает одно и то же значение.
в) Функция, которая принимает любое количество аргументов.
г) Функция, которая зависит от случайной величины.

Задание №9. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
В какой системе используется хэш-функция SHA-256? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) Для шифрования сообщений
б) Для цифровой подписи
в) Для кодирования паролей
г) Все вышеперечисленное

Задание №10. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Как называется метод, используемый для разложения больших чисел на множители? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) Метод Ньютона
б) Метод квадратичного решета
в) Метод Монте-Карло
г) Метод Гаусса

Задание №11. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что такое простая группа? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3***

а)Группа, которая не имеет нормальных подгрупп, кроме самой себя и единичной группы
б) Группа, которая имеет только одну нормальную подгуппу
в) Группа, порядок которой равен простому числу

Задание №12. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какое число является простым? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) 4
б) 17
в) 21

Задание №13. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какая функция используется в RSA-криптосистеме? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Функция шифрования
б)Функция дешифровки
в)Функция Эйлера

Задание №14. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что означает алгоритм Евклида? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Алгоритм для нахождения наибольшего общего делителя двух чисел
б) Алгоритм для нахождения наименьшего общего кратного двух чисел
в) Алгоритм для вычисления корней уравнений

Задание №15. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какой принцип лежит в основе работы асимметричных криптографических систем? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Использование одного ключа для шифрования и дешифрации
б) Использование разных ключей для шифрования и дешифрации
в) Использование симметричного алгоритма шифрования

Задание №16 Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Как называется операция, обратная возведению в степень по модулю? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Логарифмирование
б) Дискретное логарифмирование
в) Деление по модулю

Задание №17. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие числа называются взаимно простыми? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Числа, сумма которых равна нулю
б) Числа, наибольший общий делитель которых равен 1
в) Числа, произведение которых равно 1

Задание №18. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа/
Какова основная идея метода Диффи-Хеллмана? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Обмен ключами между двумя сторонами через открытый канал связи
б) Создание общего секретного ключа путем обмена открытыми данными
в) Шифрование сообщений с использованием открытого текста

Задание №19. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Каково основное свойство функции хэширования? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Обратимость
б) Устойчивость к коллизиям
в) Линейность

Задание №20. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что такое модуль в контексте RSA-криптосистемы? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3***
а) Ключ для шифрования
б) Произведение двух больших простых чисел
в) Функция для вычисления остатка от деления

Ключи ответов

Номер задания	Правильный ответ
	а
1	б
2	а
3	г
4	г
5	б
6	с
7	а
8	г

9	б
10	а
11	б
12	с
13	б
14	б
15	б
16	б
17	б
18	б
19	б
20	а

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-10 баллов	2 (неудовлетворительно)	0-50%	низкий
11-13 баллов	3 (удовлетворительно)	51-65%	базовый
14-17 баллов	4 (хорошо)	66-85%	повышенный
18-20 баллов	5 (отлично)	86-100%	высокий

Раздел 2. Классическая криптография

Вариант 1

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.

1. Какие основные угрозы информационной безопасности существуют для автономных автоматизированных систем? ***(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)***

а) Перехват данных, отказ в обслуживании, вредоносное ПО

б) Подмена данных, изменение конфигурации, физические повреждения

в) Угрозы социального инжиниринга, фишинга, утечки данных

г) Все вышеперечисленные

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое классическая криптография? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а)Современная система шифрования, использующая компьютерные технологии.

б) Исторически ранние методы шифрования, разработанные до появления компьютеров.

в) Система шифрования, основанная на квантовых вычислениях.

○

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое шифр Цезаря? ***(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)***

а)Метод шифрования, основанный на перестановке символов.

б) Метод шифрования, который смещает каждый символ алфавита на фиксированное количество позиций.

в) Метод шифрования, используемый в древних греческих документах.

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов**:**

Что такое частотный анализ? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а)Анализ частоты появления букв в тексте.

б) Анализ частоты появления символов в зашифрованном тексте для определения исходного текста.

в) Методы шифрования, основанные на анализе частотности символов.

Задание №4. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов**:**

Какой тип шифра использует шифр Виженера? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а)Полиграммный шифр.

б) Одноалфавитный шифр.

в) Многоалфавитный шифр.

Задание №5. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов**:**

Какое правило определяет шифр простой замены? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а)Каждой букве соответствует одна и та же буква в другом алфавите.

б) Каждой букве исходного алфавита ставится в соответствие уникальная буква шифрованного алфавита.

в) Буквы заменяются на другие буквы в случайном порядке.

Задание №6. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какой принцип использовал Аффинный шифр? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а)Перестановочный шифр.

б) Арифметическое преобразование символов с помощью линейного уравнения.

в) Использование нескольких алфавитов для шифрования.

Задание №7. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов**: Какая атака на шифры известна как "Атака методом грубой силы"?** *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а)Атака, при которой злоумышленник пытается подобрать пароль методом перебора всех возможных комбинаций.

б) Атака, при которой злоумышленник пробует все возможные ключи для расшифровки сообщения.

в) Атака, основанная на статистическом анализе текста.

Задание №8. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое гаммирование? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а) Способ шифрования, при котором символы шифруются последовательностью символов, называемой гаммой

б)**.** Способ шифрования, при котором символы шифруются одним и тем же ключом.

в) Шифр, основанный на сложении двух строк текста.

Задание №9. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Как работает шифр Вернама? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а)Используется многоалфавитный шифр.

б) Используется одноразовый блокнот (OTP), обеспечивающий абсолютную безопасность.

в) Используются арифметические преобразования символов.

Задание №10. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов**.**

Что такое полиграммный шифр? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*

а) Шифр, который шифрует несколько символов одновременно.

б) Шифр, который шифрует отдельные символы.

в) Шифр, который использует различные алфавиты для шифрования.

Задание №11. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое шифрование? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Процесс перевода информации в читаемый вид.
б) Процесс преобразования информации в такой вид, чтобы она была скрыта от посторонних лиц.
в) Процесс передачи информации по сети.

Задание №12. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое ключ шифрования? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Код, используемый для декодирования информации.
б) Код, используемый для защиты паролей.
в) Код, используемый для шифрования и дешифрования информации.

Задание №13. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Как классифицируется шифрование по типу используемых ключей? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Симметричное и асимметричное.
б) Симметричное и несимметричное.
в) Открытое и закрытое.

Задание №14. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
В каком виде передается информация после процесса шифрования? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Открытым текстом.
б) Закрытым текстом (шифротекстом).
в) В виде изображений.

Задание №15. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое криптоанализ? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а) Наука о взломе шифров и анализе их слабых мест..
б) Наука о создании новых шифров
в) Наука о защите информации.

Задание №16. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Какой метод шифрования использовался Юлием Цезарем? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Шифр Виженера.
б) Шифр Цезаря.
в) Роторный шифратор.

Задание №17. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Как называется процесс восстановления оригинального текста из зашифрованного? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Декомпрессия.
б)**.** Компрессия
в) Дешифровка.

Задание №18. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое блочное шифрование? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Шифрование, при котором данные передаются частями.
б) Шифрование, при котором данные разбиваются на блоки фиксированной длины и обрабатываются отдельно.
в) Шифрование, использующее специальные коды.

Задание №19. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Какое шифрование считается более безопасным: симметричное или асимметричное? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Асимметричное.
б) Это зависит от контекста и требований безопасности. Оба типа имеют свои преимущества и недостатки.
в) Симметричное.

Задание №20. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое электронная подпись? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Электронный документ, подписанный вручную.
б) Специальный код для шифрования документов.
в) Цифровой аналог традиционной подписи, позволяющий удостоверять подлинность документа и его автора.

Задание №21. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что изучает криптография? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Методы защиты информации от несанкционированного доступа.
Б)Способы хранения информации.
в) Способы анализа данных.

Задание №22. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Каковы основные цели криптографии? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Конфиденциальность, целостность и доступность.
б) Защита информации от вирусов.
в) Конфиденциальность, аутентификация и целостность.

Задание №23.**Выберите правильные ответы и обведите кружочками номера правильных ответов. Правильных ответов может быть несколько.**
(оцениваемые знания, умения, компетенции: У3, З1, З2,З3, ПК. 2.4, ПК. 2.6)
Какие данные относятся к категории «информация ограниченного доступа»? Варианты ответов:

а) любая информация, доступ к которой ограничен определенными лицами;
б) информация, содержащая персональные данные пользователей;
в) коммерческая тайна компании;
г) любая информация, доступная на работе.

Задание №24. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Какие существуют основные типы шифрования? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Симметричное и асимметричное.
б) Открытое и закрытое.
в) Однонаправленное и двунаправленное.

Задание №25. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое симметричное шифрование? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Шифрование, использующее разные ключи для шифрования и дешифрования.
б) Шифрование, использующее один и тот же ключ для шифрования и дешифрования**.**
в) Шифрование, использующее специальные коды.

Задание № 26. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое асимметричное шифрование? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Шифрование, использующее один и тот же ключ для шифрования и дешифрования.
б) Шифрование, использующее разные ключи для шифрования и дешифрования**.**
в) Шифрование, использующее временные ключи.

Задание № 27. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое хэш-функция? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Функция, преобразующая входные данные в выходной сигнал.
б) Функция, защищающая данные от изменения.
в) Функция, преобразующая произвольный объем данных в строку фиксированной длины.

Задание № 28. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое цифровая подпись? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Подпись, сделанная вручную.
б) Электронный эквивалент рукописной подписи, подтверждающий авторство и целостность документа.
в) Подпись, использующаяся для шифрования данных.

Задание №29. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Как называется метод шифрования, предложенный Юлием Цезарем? *(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)*
а)Метод Гаусса.
б) Шифр Цезаря.
в) Метод Ньютона.

Задание №30.-Прочитайте ситуационную задачу, решите кейс и ответ запишите в таблицу.

(оцениваемые знания, умения, компетенции: У3, У5, З2,З3, ПК. 2.4, ПК. 2.6)

Вы являетесь специалистом по информационной безопасности в крупной финансовой организации. Ваша команда получила отчет о взломе серверов конкурирующей фирмы, специализирующейся на разработке программного обеспечения для банков. Вам поручено провести аудит

существующей системы безопасности Вашей организации и предложить четыре метода криптоанализа по усилению криптографической защиты против конкурентов.

Запишите ответ:

1.	
2.	
3.	
4.	

Ключи ответов

Номер задания	Правильный ответ
1	г
2	б
3	б
4	с
5	б
6	б
7	б
8	а
9	б
10	а
11	б
12	с
13	б
14	б
15	а
16	б
17	с
18	б
19	б
20	с
21	а
22	с
23	а, б, в
24	а
25	б
26	б
27	с
28	б

29	б
30	1. Атака методом грубой силы. 2. Анализ частоты символов. 3. Криптоанализ с известным открытым текстом. 4. Алгоритмические уязвимости.

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-15 баллов	2 (неудовлетворительно)	0-50%	низкий
16-20 баллов	3 (удовлетворительно)	51-65%	базовый
21-25 баллов	4 (хорошо)	66-85%	повышенный
26-30 баллов	5 (отлично)	86-100%	высокий

Раздел 3. Современная криптография

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое современная криптография? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*

а) Область знаний, занимающаяся разработкой и анализом методов защиты информации с использованием математических и компьютерных технологий.

б) Методы шифрования, разработанные до появления компьютеров.

в) Способы хранения информации без использования шифрования.

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие основные цели современной криптографии? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*

а) Обеспечение конфиденциальности, целостности и доступности информации.

б) Обеспечение конфиденциальности, аутентификации, целостности и неотказуемости (невозможности отказа от авторства).

в) Защита информации только от несанкционированного доступа.

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое симметричное шифрование? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*
а) Шифрование, использующее разные ключи для шифрования и дешифрования.
б) Шифрование, использующее один и тот же ключ для шифрования и дешифрования**.**
в) Шифрование, использующее временные ключи.

Задание №4. Выберите правильные ответы и обведите кружочками номера правильных ответов. Правильных ответов может быть несколько.
(оцениваемые знания, умения, компетенции: У3, З6, ПК. 2.4)
Какой основной принцип лежит в основе работы с информацией ограниченного доступа?
а) Принцип минимизации доступа.
б) Принцип полного контроля над информацией.
в) Принцип конфиденциальности.
г) Принцип доступности информации для всех сотрудников.

Задание №5. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Что такое эллиптическая криптография (ECB)? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*
а) Подкласс асимметричной криптографии, основанный на свойствах эллиптических кривых**.**
б) Метод шифрования, использующий симметричные ключи.
в) Алгоритм хэширования.

Задание №6. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Что такое квантовая криптография? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*
а) Область криптографии, использующая принципы квантовой механики для обеспечения безопасности передачи данных.
б) Метод шифрования, использующий классические алгоритмы.
в) Метод шифрования, использующий временные ключи.

Задание №7. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Что такое постквантовая криптография? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*
а) Область криптографии, разрабатывающая алгоритмы, устойчивые к атакам с использованием квантовых компьютеров.
б) Метод шифрования, использующий квантовые компьютеры.
в) Метод шифрования, использующий временные ключи.

Задание №8. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое хэш-функция? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*

а) Функция, преобразующая произвольный объем данных в строку фиксированной длины.

б) Функция, преобразующая произвольный объем данных в строку фиксированной длины, устойчивая к коллизиям.

в) Функция, защищающая данные от изменения.

Задание №9. Прочитайте ситуационную задачу, решите кейс и ответ запишите в таблицу.

(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)

Вы являетесь специалистом по информационной безопасности в крупной финансовой организации. Ваша команда получила отчет о взломе серверов конкурирующей фирмы, специализирующейся на разработке программного обеспечения для банков. Вам поручено провести аудит существующей системы безопасности и предложить 5 мер по усилению криптографической защиты Вашей организации.

Запишите ответ:

1.	
2.	
3.	
4.	
5.	

Задание №10. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое блокчейн в контексте криптографии? *(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*

а) Технология распределенного реестра, использующая криптографические методы для обеспечения безопасности и целостности данных.

б) Метод шифрования, использующий симметричные ключи.

в) Алгоритм хэширования.

Ключи ответов

Номер задания	Правильный ответ
	1 вариант
1	а
2	б
3	б
4	а, б, в

5	а
6	б
7	а
8	б
9	1. Усиление паролей и ключей. 2. Многослойная защита. 3. Регулярное обновление ПО. 4. Мониторинг и аудиты. 5. Обучение персонала**.**
10	а

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-5 баллов	2 (неудовлетворительно)	0-50%	низкий
6-7 баллов	3 (удовлетворительно)	50-70%	базовый
8-9 баллов	4 (хорошо)	80-90%	повышенный
10 баллов	5 (отлично)	100%	высокий

2.2. Вопросы для устного опроса.

Тема 1.1. Математические основы криптографии

Вопросы:

1. Что входит в предмет и задачи криптографии? Перечислите основные термины. ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

2. Что входит в элементы теории множеств? Что означает группы, кольца, поля в криптографии? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3).***

3. Что такое делимость чисел? Поясните понятие делимости чисел и перечислите признаки делимости. Простые и составные числа ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***.

4. Расскажите об основной теореме арифметики. Как найти наибольший общий делитель? Что означает взаимно простые числа? Как найти НОД? Можно ли использовать алгоритм Евклида для нахождения НОД? ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***

5. Перечислите свойства сравнений и отношения сравнимости между числами. Что изучает модулярная арифметика ? ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***
6. Расскажите о Китайская теорема об остатках. ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
7. В чем заключается алгоритм проверки чисел на простоту? Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
8. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
9. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
10. Арифметические операции над большими числами. ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***

Тема 2.1. Методы криптографического защиты информации

Вопросы:

1. Классификация основных методов криптографической защиты. Методы симметричного шифрования? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***
2. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр. ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***
3. Методы перестановки. Табличная перестановка, маршрутная? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***
4. Гаммирование. Гаммирование с конечной и бесконечной? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***

Тема 2.2. Криптоанализ

Вопросы:

1. Какие способы изучения ПО и обратное проектирование ПО вы знаете? ***(оцениваемые знания, умения, компетенции: У2, У5, , З1, ПК. 2.2, ПК. 2.3)***
2. Перечислите задачи защиты от изучения и способы их решения. ***(оцениваемые знания, умения, компетенции: У2, У5, , З1, ПК. 2.2, ПК. 2.3)***
3. Как выполнить защиту от отладки, дизассемблирования, от трассировки по прерываниям? ***(оцениваемые знания, умения, компетенции: У2, У5, , З1, ПК. 2.2, ПК. 2.3)***

Тема 2.3. Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел

Вопросы:

1. Какое вредоносное программное обеспечение, выполняющее

разрушающее воздействие вы знаете? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

2. Расскажите о классификация вредоносного программного обеспечения, схеме заражения, средствах нейтрализации вредоносного ПО и профилактике заражения. ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

3. Как выполняется поиск следов активности вредоносного ПО, в реестре Winrows, основных ветках, содержащих информацию о вредоносном ПО и в других объектах, содержащие информацию о вредоносном ПО? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

4. Расскажите о Бот-неты, их принципах функционирования и методах обнаружения. ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

5. Какую классификацию антивирусных средств, сигнатурного и эвристического анализа вы знаете? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

6. Какая бывает защита от вирусов в "ручном режиме"? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

Тема 3.1. Кодирование информации. Компьютеризация шифрования.

Вопросы:

1. Какие сети работают по технологии коммутации пакетов? ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***
2. Расскажите об особенностях стека протоколов TCP/IP и маршрутизации. ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***
3. Расскажите о штатных средствах защиты информации стека протоколов TCP/IP. ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***
4. Перечислите средства идентификации и аутентификации пользователей на разных уровнях протокола TCP/IP, укажите достоинства, недостатки, ограничения. ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***

Тема 3.2. Симметричные системы шифрования

Вопросы:

1. Как представлена виртуальная частная сеть? Дайте понятия функции, назначение, принцип построения. ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

2.Как представлены криптографические и некриптографические средства организации VPN? ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

3. Перечислите устройства, образующие VPN, криптомаршрутизатор и криптофильтр. ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

4. Что такое криптороутер? Каковы его принципы, архитектура, модель

нарушителя, достоинства и недостатки. ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

Тема 3.3. Асимметричные системы шифрования

Вопросы:

1. Опишите принципы работы криптосистем с открытым ключом. Почему такие системы считаются необратимыми? Нарисуйте структурную схему шифрования с открытым ключом и поясните её основные компоненты. ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
2. Какие элементы теории чисел используются в криптографии с открытым ключом? Приведите примеры алгоритмов, основанных на этих элементах. ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***

Тема 3.4. Аутентификация данных. Электронная подпись

Вопросы:

1. Что такое аутентификация данных? Объясните, как электронные подписи (ЭП) и коды аутентификации сообщений (MAB) обеспечивают аутентификацию данных. Приведите примеры их применения. ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
2. Что такое однонаправленные хеш-функции? Как они используются в алгоритмах цифровой подписи? Приведите примеры однонаправленных хеш-функций и алгоритмов цифровой подписи. ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации

Вопросы:

1. Опишите основные алгоритмы распределения ключей с использованием симметричных и асимметричных схем. Какие протоколы аутентификации применяются в этих схемах? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***
2. Что такое взаимная и односторонняя аутентификация? Опишите их отличия и приведите примеры использования каждого вида аутентификации. ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

Тема 3.6. Криптозащита информации в сетях передачи данных

Вопросы:

1 Какие преимущества и недостатки имеют абонентское и пакетное шифрование в сравнении друг с другом, и какую роль играют защита центра генерации ключей и криптомаршрутизаторы в обеспечении безопасности сетей передачи данных? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***
2. Каковы основные отличия между протоколами WPA и WEP в контексте

криптографической защиты беспроводных соединений в сетях стандарта 802.11, и какие уязвимости присущи каждому из этих протоколов? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

Тема 3.7. Защита информации в электронных платежных системах

Вопросы:

1. Каковы основные принципы функционирования электронных платежных систем, включая механизмы аутентификации пользователей, обеспечение безопасности транзакций и защиту от мошенничества? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***
2. Каким образом используется персональный идентификационный номер (PIN-код) для обеспечения безопасности при использовании электронных пластиковых карт, и какие существуют меры предотвращения несанкционированного доступа к средствам владельца карты? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***
3. Какие криптографические протоколы применяются для обеспечения конфиденциальности, целостности и аутентичности данных в электронной коммерции, и каким образом они защищают транзакции от перехвата и подделки? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***

Тема 3.8. Компьютерная стеганография.

Вопросы:

1. Какие методы скрытой передачи информации (стеганографии) используются в современных компьютерных системах, и как они помогают обеспечивать конфиденциальность передаваемых данных? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***
2. Какова проблема аутентификации мультимедийной информации. Защита авторских прав? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***
3. В чем заключаются методы компьютерной стеганографии? Что такое цифровые водяные знаки?. Как работает алгоритмы встраивания ЦВЗ? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

Критерии оценивания

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по междисциплинарному курсу, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также

высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;
«4» «хорошо» – студент в полном объеме освоил программный материал по междисциплинарному курсу, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;
«3» «удовлетворительно» – студент обнаруживает знание и понимание основных положений программного материала по междисциплинарному курсу, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;
«2» «неудовлетворительно» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по междисциплинарному курсу, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения междисциплинарного курса для организации промежуточной аттестации в форме экзамена

Для проведения промежуточной аттестации в форме экзамена используются настоящие контрольно-оценочные средства для оформления экзаменационных билетов Количество экзаменационных билетов должно превышать количество студентов на 3.

ПРИМЕР ОФОРМЛЕНИЯ БИЛЕТА

Министерство образования Белгородской области

Областное государственное автономное профессиональное образовательное учреждение
«Алексеевский колледж»

МДК 02.02 Криптографические средства информации

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

семестр 6 курс 3

группа 831

Билет № **1**

1. Ответьте на вопрос: Какова проблема аутентификации мультимедийной информации. Защита авторских прав?
1. Выполните практическое задание (Приложение1).

Преподаватель: _____ И.В. Косинова
(подпись)

3.1. Перечень вопросов.

1. Что входит в предмет и задачи криптографии? Перечислите основные термины. ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
2. Что входит в элементы теории множеств? Что означает группы, кольца, поля в криптографии? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3).***
3. Что такое делимость чисел? Поясните понятие делимости чисел и перечислите признаки делимости. Простые и составные числа ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***.
4. Расскажите об основной теореме арифметики. Как найти наибольший общий делитель? Что означает взаимно простые числа? Как найти НОД? Можно ли использовать алгоритм Евклида для нахождения НОД? ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***
5. Перечислите свойства сравнений и отношения сравнимости между числами. Что изучает модулярная арифметика ? ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***
6. Расскажите о Китайская теорема об остатках. ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
7. В чем заключается алгоритм проверки чисел на простоту? Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
8. Какие существуют алгоритмы разложения чисел на множители, включая метод факторизации Ферма и алгоритм Полларда, и каковы их основные принципы работы и эффективность? ***(оцениваемые знания, умения,***

компетенции: У4, З1, З6, З3 , ПК. 2.2)

9. Какие существуют алгоритмы решения задачи дискретного логарифмирования, включая метод Полларда и квантовый алгоритм Шорра, и каковы их основные принципы работы и применимость в криптографии? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***

10. Какие могут выполняться арифметические операции над большими числами? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***

11. Какова классификация основных методов криптографической защиты, и какие особенности и алгоритмы характерны для методов симметричного шифрования? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***

12. Какие типы шифров замены существуют, включая простую замену, многоалфавитную подстановку и пропорциональные шифры, и каковы их основные принципы работы и уязвимости? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***

13. Какие методы перестановки используются в криптографии, включая табличную и маршрутную перестановки, и каковы их основные принципы работы и применение в шифровании данных? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***

14. Вопрос уже сформулирован корректно! Если хотите уточнить или переформулировать, пожалуйста, укажите желаемые изменения. ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***

15. Какие способы изучения ПО и обратное проектирование ПО вы знаете? ***(оцениваемые знания, умения, компетенции: У2, У5, , З1, ПК. 2.2, ПК. 2.3)***

16. Перечислите задачи защиты от изучения и способы их решения. ***(оцениваемые знания, умения, компетенции: У2, У5, , З1, ПК. 2.2, ПК. 2.3)***

17. Как выполнить защиту от отладки, дизассемблирования, от трассировки по прерываниям? ***(оцениваемые знания, умения, компетенции: У2, У5, , З1, ПК. 2.2, ПК. 2.3)***

18. Какое вредоносное программное обеспечение, выполняющее разрушающее воздействие вы знаете? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

19. Расскажите о классификация вредоносного программного обеспечения, схеме заражения, средствах нейтрализации вредоносного ПО и профилактике заражения. ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

20. Как выполняется поиск следов активности вредоносного ПО, в реестре Winrows, основных ветках, содержащих информацию о вредоносном ПО и в других объектах, содержащие информацию о вредоносном ПО? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

21. Расскажите о Бот-неты, их принципах функционирования и методах обнаружения. ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

22. Какую классификацию антивирусных средств, сигнатурного и эвристического анализа вы знаете? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

23. Какая бывает защита от вирусов в "ручном режиме"? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

24. Какие сети работают по технологии коммутации пакетов? ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***

25. Расскажите об особенностях стека протоколов TCP/IP и маршрутизации. ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***

26. Расскажите о штатных средствах защиты информации стека протоколов TCP/IP. ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***

27. Перечислите средства идентификации и аутентификации пользователей на разных уровнях протокола TCP/IP, укажите достоинства, недостатки, ограничения. ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***

28. Как представлена виртуальная частная сеть? Дайте понятия функции, назначение, принцип построения. ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

29. Как представлены криптографические и некриптографические средства организации VPN? ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

30. Перечислите устройства, образующие VPN, криптомаршрутизатор и криптофильтр. ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

31. Что такое криптороутер? Каковы его принципы, архитектура, модель нарушителя, достоинства и недостатки. ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

32. Опишите принципы работы криптосистем с открытым ключом. Почему такие системы считаются необратимыми? Нарисуйте структурную схему шифрования с открытым ключом и поясните её основные компоненты. ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***

33. Какие элементы теории чисел используются в криптографии с открытым ключом? Приведите примеры алгоритмов, основанных на этих элементах. ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***

34. Что такое аутентификация данных? Объясните, как электронные подписи (ЭП) и коды аутентификации сообщений (MAB) обеспечивают аутентификацию данных. Приведите примеры их применения. ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***

35. Что такое однонаправленные хеш-функции? Как они используются в алгоритмах цифровой подписи? Приведите примеры однонаправленных хеш-функций и алгоритмов цифровой подписи. ***(оцениваемые знания, умения,***

компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).

36. Опишите основные алгоритмы распределения ключей с использованием симметричных и асимметричных схем. Какие протоколы аутентификации применяются в этих схемах? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

37. Что такое взаимная и односторонняя аутентификация? Опишите их отличия и приведите примеры использования каждого вида аутентификации. ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

38. Какие преимущества и недостатки имеют абонентское и пакетное шифрование в сравнении друг с другом, и какую роль играют защита центра генерации ключей и криптомаршрутизаторы в обеспечении безопасности сетей передачи данных? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

38. Каковы основные отличия между протоколами WPA и WEP в контексте криптографической защиты беспроводных соединений в сетях стандарта 802.11, и какие уязвимости присущи каждому из этих протоколов? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

39. Каковы основные принципы функционирования электронных платежных систем, включая механизмы аутентификации пользователей, обеспечение безопасности транзакций и защиту от мошенничества? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***

40. Каким образом используется персональный идентификационный номер (PIN-код) для обеспечения безопасности при использовании электронных пластиковых карт, и какие существуют меры предотвращения несанкционированного доступа к средствам владельца карты? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***

41. Какие криптографические протоколы применяются для обеспечения конфиденциальности, целостности и аутентичности данных в электронной коммерции, и каким образом они защищают транзакции от перехвата и подделки? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***

42. Какие методы скрытой передачи информации (стеганографии) используются в современных компьютерных системах, и как они помогают обеспечивать конфиденциальность передаваемых данных? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

43. Какова проблема аутентификации мультимедийной информации. Защита авторских прав? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

44. В чем заключаются методы компьютерной стеганографии? Что такое цифровые водяные знаки?. Как работает алгоритмы встраивания ЦВЗ? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

3.2. Перечень практических заданий.

Задание 1.Ситуационная задача:

Компания "Безопасные Сети" разрабатывает новый продукт — систему криптографической защиты данных для корпоративной сети. В компании используют несколько типов данных: личные данные сотрудников, финансовые отчеты, техническую документацию и внутреннюю переписку. Для каждого типа данных необходимы разные уровни защиты.

Необходимо выбрать подходящие методы криптографической защиты информации, учитывая следующие требования:

1. **Личные данные сотрудников**: Высокая степень защиты, минимальное время задержки при доступе.
2. **Финансовые отчеты**: Необходима целостность данных и невозможность их изменения третьими лицами.
3. **Техническая документация**: Требуется защита от несанкционированного доступа и копирования.
4. **Внутренняя переписка**: Необходимо обеспечить конфиденциальность сообщений и возможность отслеживания отправителя.

Определите, какие методы криптографической защиты (например, симметричное/асимметричное шифрование, цифровые подписи, хеш-функции) лучше всего подойдут для каждой категории данных, обосновав ваш выбор.

Какие основные методы криптоанализа используются для взлома шифров и как они влияют на безопасность современных криптографических систем?

Задание 2.Ситуационная задача:

Вашей команде поручено провести криптоанализ зашифрованного сообщения, которое было перехвачено во время передачи между двумя компаниями. Известно, что сообщение было зашифровано с использованием классического шифра подстановки, однако детали реализации неизвестны. Ваша задача состоит в том, чтобы расшифровать сообщение и определить его содержание.

Имеются следующие условия:

- Длина сообщения составляет 500 символов.
- Сообщение содержит текст на русском языке.
- Предполагается, что текст имеет стандартную частотность букв русского алфавита.

Вам нужно разработать план действий для проведения криптоанализа, который должен включать:

1. Выбор метода атаки.
2. Описание шагов, необходимых для реализации выбранного метода.
3. Оценку вероятности успешного дешифрования.

Также вам необходимо предложить рекомендации по улучшению криптостойкости системы, использованной для шифрования данного сообщения.

Задание 3.Ситуационная задача:

Вы являетесь специалистом по информационной безопасности в крупной IT-компании. Руководство поставило перед вами задачу модернизировать существующую систему шифрования данных, используемую для защиты передаваемой информации через публичные сети. Текущая система основана на поточном шифре RC4, который, как известно, имеет ряд уязвимостей.

Перед вами стоит следующая задача:

1. Объяснить руководству, почему использование RC4 больше не является безопасным выбором для защиты данных.
2. Предложить альтернативу на основе современного поточного шифра или генератора псевдослучайных чисел (ГПСЧ), который обеспечит высокий уровень безопасности и будет соответствовать современным стандартам.
3. Обосновать выбор предложенного шифра или ГПСЧ, сравнив его с другими аналогичными решениями по таким параметрам, как скорость работы, устойчивость к атакам и совместимость с существующей инфраструктурой.
4. Разработать план внедрения нового шифра или ГПСЧ, учитывая возможные риски и ограничения.

Ваши предложения должны быть представлены в виде отчета, который будет рассмотрен руководством для принятия решения о модернизации системы шифрования.

Задание 4.Ситуационная задача:

Вы работаете инженером по информационной безопасности в компании, занимающейся разработкой программного обеспечения для корпоративных клиентов. Один из ваших заказчиков обратился с просьбой интегрировать систему кодирования информации в свою внутреннюю сеть. Система должна обеспечивать надежную защиту данных при передаче между различными отделами компании, минимизировать риск утечки информации и быть легко масштабируемой.

Перед вами стоят следующие задачи:

1. Провести анализ существующих методов кодирования информации и выбрать наиболее подходящий для данной ситуации.
2. Разработать архитектуру системы, обеспечивающую эффективное кодирование данных с учетом специфики заказчика (например, объем передаваемых данных, необходимость минимизации задержек, совместимость с существующей ИТ-инфраструктурой).
3. Предусмотреть возможность компьютеризированного управления процессом шифрования, включая автоматическое обновление ключей и мониторинг состояния системы.
4. Рассчитать ориентировочную стоимость внедрения и эксплуатации предлагаемого решения.
5. Подготовить отчет для руководства заказчика, содержащий обоснование выбора метода кодирования, описание архитектуры системы и расчет стоимости проекта.

Учтите, что заказчик заинтересован в долгосрочной перспективе и готов инвестировать в современные технологии, обеспечивающие высокую степень безопасности и гибкость в управлении системой.

Задание 5.Ситуационная задача:

Вы являетесь руководителем отдела информационной безопасности в крупной корпорации, специализирующейся на разработке и продаже программного обеспечения. Компания планирует внедрение новой системы обмена данными между своими филиалами, расположенными в разных странах. Передача данных должна осуществляться через Интернет, и вы обязаны обеспечить её максимальную защищенность.

Используя симметричную систему шифрования, разработайте стратегию защиты данных, передаваемых между филиалами. Учтите следующие аспекты:

1. Определите критерии выбора конкретного алгоритма симметричного шифрования (например, AES, ГЕS, Blowfish и др.).
2. Опишите процесс распределения ключей между филиалами.
3. Разработайте механизм обновления ключей в случае компрометации одного из филиалов.
4. Укажите, какие дополнительные меры безопасности (помимо самого шифрования) вы планируете внедрить для повышения уровня защиты передаваемых данных.
5. Представьте смету расходов на реализацию вашего плана.

Ваше решение должно учитывать баланс между безопасностью и эффективностью работы системы, а также предусматривать возможные сценарии развития событий, такие как потеря ключа или нарушение работы одной из частей инфраструктуры.

Задание 6.Ситуационная задача:

Вы являетесь ведущим специалистом по информационной безопасности в международной компании, предоставляющей услуги онлайн-банкинга. Клиенты компании обеспокоены безопасностью своих данных при передаче через Интернет, особенно когда речь идет о банковских операциях. Вам поручили внедрить асимметричную систему шифрования для защиты всех данных, передаваемых между клиентами и серверами компании.

Разработайте план внедрения асимметричной системы шифрования, учитывающий следующие аспекты:

1. Выберите подходящий алгоритм асимметричного шифрования (например, RSA, ECC и др.) и обоснуйте свой выбор.
2. Опишите процесс генерации и распределения открытых и закрытых ключей среди клиентов и серверов.
3. Предложите механизм проверки подлинности передаваемых данных с помощью цифровых подписей.
4. Разработайте процедуру обновления ключей в случае их компрометации.
5. Оцените затраты на внедрение и поддержку вашей системы шифрования.

6. Предложите меры дополнительной безопасности, которые будут использоваться совместно с асимметричным шифрованием.
Ваше решение должно гарантировать надежность и удобство использования системы для клиентов, а также соответствие международным стандартам безопасности.

Задание 7.Ситуационная задача:
Вы являетесь руководителем отдела информационных технологий в компании, которая занимается дистанционным оказанием услуг населению. Ваши клиенты часто сталкиваются с необходимостью подтверждения своей личности и законности совершаемых операций, например, при заключении договоров или подаче заявлений. В связи с этим возникла потребность в создании надежной системы аутентификации данных и электронно-цифровой подписи (ЭЦП).
Задача заключается в следующем:
1. Выбрать подходящую технологию для реализации ЭЦП, которая будет удовлетворять требованиям законодательства и обеспечивать высокий уровень доверия к документам.
2. Разработать архитектуру системы, позволяющую клиентам легко и безопасно использовать электронную подпись для подписания документов удаленно.
3. Предусмотреть механизмы контроля и аудита для мониторинга действий пользователей и предотвращения возможных злоупотреблений.
4. Оценить затраты на внедрение и эксплуатацию предложенной системы.
5. Обеспечить интеграцию системы с существующими бизнес-процессами компании.
Для успешной реализации проекта важно учесть требования по защите персональных данных клиентов, обеспечить удобство использования сервиса и минимизировать вероятность ошибок и мошеннических действий.

Задание 8.Ситуационная задача:
Вы являетесь экспертом по информационной безопасности в телекоммуникационной компании, которая планирует запуск нового сервиса для безопасной передачи данных между пользователями. Одним из ключевых требований к этому сервису является надежная аутентификация участников и защита передаваемых данных от перехвата и подмены.
Задачи:
1. Выберите и опишите подходящий алгоритм обмена ключами (например, Гiffie-Hellman, RSA, ЕСГН), который позволит участникам безопасно обмениваться секретными ключами для последующей шифрации данных.
2. Разработайте протокол аутентификации, который обеспечит взаимную проверку подлинности сторон до начала передачи данных. Учитывайте необходимость минимизации риска атак типа "человек посередине" (MITM).

3. Опишите механизмы, которые позволят поддерживать актуальность и безопасность сеансовых ключей в течение длительного времени, предотвращая повторное использование одних и тех же ключей.
4. Оцените влияние выбранной схемы на производительность системы и ресурсы, необходимые для ее поддержки.
5. Предложите дополнительные меры безопасности, которые могут повысить общую защищенность сервиса, такие как регулярное обновление сертификатов или использование многофакторной аутентификации.

Решение должно быть ориентировано на практическую реализацию и учитывать реальные угрозы, с которыми могут столкнуться пользователи сервиса.

Задание 9.Ситуационная задача:

Вы — руководитель отдела информационной безопасности в крупной компании, предоставляющей облачные сервисы. Ваша компания собирается запустить новый продукт, позволяющий пользователям передавать конфиденциальные данные через общедоступные сети. Важно обеспечить высокий уровень защиты передаваемой информации от перехвата и модификации.

Перед вами стоят следующие задачи:

1. **Выбор метода криптографической защиты:** Определите, какой тип шифрования (симметричное, асимметричное или гибридное) будет оптимальным для данного случая. Обоснуйте свой выбор.
2. **Обеспечение целостности данных:** Разработайте схему, гарантирующую неизменность передаваемых данных. Укажите, какие инструменты и подходы будете использовать для этого.
3. **Аутентификация пользователей:** Предложите способ аутентификации пользователей, исключающий возможность несанкционированного доступа к данным.
4. **Управление ключами:** Спроектируйте систему управления ключами, обеспечивающую их безопасное хранение и распределение.
5. **Меры против GoS-атак:** Предложите способы защиты от атак типа "отказ в обслуживании" (GoS), направленных на перегрузку сетевых ресурсов.
6. **Мониторинг и аудит:** Включите в ваше предложение механизмы мониторинга и аудита, позволяющие отслеживать любые подозрительные активности в сети.
7. **Экономические соображения:** Сравните ваши предложения с точки зрения затрат на внедрение и обслуживание.

Составьте подробный план внедрения криптозащитных мер, учитывая вышеперечисленные пункты.

Задание 10.Ситуационная задача:

Вы — ведущий специалист по информационной безопасности в компании, занимающейся разработкой программного обеспечения для правительственных организаций. Ваш клиент — государственная структура, которой необходимо надежно защищать секретные данные, передаваемые через Интернет. Данные

должны быть скрыты таким образом, чтобы их наличие оставалось незаметным для посторонних наблюдателей.

Задача:

1. Предложите метод компьютерной стеганографии, который позволит эффективно скрывать секретные данные внутри цифрового контейнера (например, изображений, аудиофайлов или видеофайлов).
2. Опишите процесс встраивания и извлечения скрытых данных, уделяя внимание вопросам надежности и устойчивости к обнаружению.
3. Оцените, насколько выбранный метод устойчив к возможным атакам на выявление скрытых данных, включая статистический анализ контейнеров.
4. Предложите дополнительные меры для повышения уровня скрытности и безопасности передаваемых данных.
5. Подсчитайте примерные временные и ресурсные затраты на внедрение предложенного решения.

Решение должно быть детализировано и обосновано с учетом специфики государственных нужд и высокого уровня конфиденциальности передаваемой информации.

Критерии оценивания

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по междисциплинарному курсу, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» – студент в полном объеме освоил программный материал по междисциплинарному курсу, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» – студент обнаруживает знание и понимание основных положений программного материала по междисциплинарному курсу, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения,

но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по междисциплинарному курсу, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

2. Информационное обеспечение

Основные источники:

1. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования/ О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с

2. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.

Дополнительные источники:

1. Белов В.В. Проектирование информационных систем: учебник для студ. учреждений высш. проф. образования / В. В. Белов, В. И. Чистякова; под ред. В. В. Белова – М.: Издательский центр «Академия», 2013.

2. Гвоздева В.А., Лаврентьева И.Ю., Основы построения автоматизированных информационных систем, Москва, ИД Форум – ИНФРА-М, 2009.

3. Гвоздева Т.В., Баллод Б.А., Проектирование информационных систем: учеб.пособие / Т.В. Гвоздева, Б.А. Баллод. – Ростов н/Д: Феникс, 2009. – 508 с.

4. Емельянова Н.З., Устройство и функционирование информационных систем: учеб.пособие для СПО / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – 2-е изд., перераб. и доп. – М.: Форум, 2015. – 448 с.

5. Избачков Ю.С., Информационные системы: учебник для вузов [Гриф УМО МО РФ]. 3-е изд. / Избачков Ю.С., Петров В.Н [и др.]. – СПб.: Питер, 2011. – 544 с.

6. Криптографическая защита информации в объектах информационной инфраструктуры:учебник, 1-е изд.,/ Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - ИЦ Академия, 2020 -288 с

7. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с

Электронные издания (электронные ресурсы):

1. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 https://e.lanbook.com/book/82817

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcoge/449548

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcoge/456793

4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2020. — 325 с. https://urait.ru/bcoge/451933

Цифровая образовательная среда СПО PROFобразование:

- Абрамов, Г. В. Проектирование и разработка информационных систем : учебное пособие для СПО / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. — Саратов : Профобразование, 2020. — 169 с. — ISBN 978-5-4488-0730-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/88888 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. пользователей.

- Локальная настройка Secret Net Sturio – Режим доступа. - https://sturfile.net/preview/17096143/page:2/

- РУКОВОДСТВО ПО УСТАНОВКЕ – Режим доступа. - https://www.ptsecurity.com/uploar/corporate/ru-ru/proructs/mp8/installation-guire-maxpatrol.prf

- Система контроля защищённости и соответствия стандартам maxpatrol. – Режим доступа. - https://sturfile.net/preview/2140979/page:50/

- MU_МГК02.01.prf file:///C:/Users/kosinova/Townloars/MU_МГК02.01%20(1).prf. – Режим доступа. -

Электронно-библиотечная система:
IPRBOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moorle.alcollege.ru/