

Приложение ПССЗ по специальности 09.02.07 Информационные системы и программирование  
2022-2023 уч.г.: Рабочая программа междисциплинарного курса МДК.07.01 Управление и  
автоматизация баз данных

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

**Комплект  
контрольно-оценочных средств**

**междисциплинарного курса**

**МДК 02.02 Криптографические средства защиты информации**

для специальности  
10.02.05 Обеспечение информационной безопасности  
автоматизированных систем

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Составитель:

Ляшенко А.В., преподаватель ОГАОУ «Алексеевский колледж»

## 1. Паспорт комплекта оценочных средств

### 1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу междисциплинарного курса МДК 02.02 Криптографические средства защиты информации. КОС включают контрольные материалы для проведения текущей и промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы междисциплинарного курса.

### 1.2 Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК 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.

#### **знать:**

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

- 3.2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
- 3.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- 3.4 основные понятия криптографии и типовых криптографических методов и средств защиты информации;
- 3.5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
- 3.6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

**Перечень знаний и умений в соответствии с профессиональными стандартами «Администратор баз данных», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 22 января 2013 г. N 23, который актуализируются при изучении междисциплинарного курса:**

- 1) Обеспечение функционирования БД;
- 2) Предотвращение потерь и повреждений данных;
- 3) Обеспечение информационной безопасности на уровне БД;
- 4) Управление развитием БД.

**Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции Ворлдскиллс Сетевое и системное администрирование, которые актуализируются при изучении междисциплинарного курса:**

- 1) знать и понимать: как настраивать коммутацию уровня доступа, агрегации и ядра;
- 2) знать и понимать: как настраивать протоколы маршрутизации внутреннего и внешнего шлюза;
- 3) знать и понимать: как обеспечивать отказоустойчивость сети на уровне коммутации и маршрутизации;
- 4) знать и понимать: как применять базовые механизмы защиты от компрометации активного сетевого оборудования;

**Планируемые личностные результаты освоения рабочей программы**

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

Результатом освоения МДК является овладение обучающимися видом деятельности - Соадминистрирование баз данных и серверов, в том числе общими компетенции (ОК) и профессиональными компетенциями (ПК):

<b>Код</b>	<b>Наименование результата обучения</b>
<i>ОК 1</i>	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
<i>ОК 2</i>	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
<i>ОК 3</i>	Планировать и реализовывать собственное профессиональное и личностное развитие.
<i>ОК 4</i>	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
<i>ОК 5</i>	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
<i>ОК 6</i>	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
<i>ОК 7</i>	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
<i>ОК 8</i>	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
<i>ОК 9</i>	Использовать информационные технологии в профессиональной деятельности.
<i>ОК 10</i>	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.

### **1.3 Результаты освоения междисциплинарного курса, подлежащие проверке**

Наименование тем	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы	Средства контроля и оценки результатов обучения <b>в рамках текущей аттестации</b> (номер задания)	Средства контроля и оценки результатов обучения <b>в рамках промежуточной аттестации</b> (номер задания/контрольного вопроса/ экзаменационного билета)
Тема 1.1. Математические основы криптографии	ОК1 – 2,9,8 ПК 7.1 У3 З1 ЛР 1	ПЗ 1	КВ 1
Тема 2.1. Методы криптографического защиты информации	ОК3-4,10 ПК 7.2 У2 З2 ЛР 1	ПЗ 2	КВ 2
Тема 2.3. Поточные шифры и генераторы псевдослучайных	ОК5-6, 11 ПК 7.3 У1	ПЗ 3	КВ 3

чисел	31 ЛР 1		
Тема 3.1. Кодирование информации. Компьютеризация шифрования	ОК1 – 2,9,8 ПК 7.1 У3 31 ЛР 1	ПЗ 4	КВ 4
Тема 3.2. Симметричные системы шифрования	ОК3-4,10 ПК 7.2 У2 32 ЛР 1	ПЗ 5	КВ 5
Тема 3.3. Асимметричные системы шифрования	ОК5-6, 11 ПК 7.3 У1 31 ЛР 1	ПЗ 6	КВ 6
Тема 3.4. Аутентификация данных. Электронная подпись	ОК1 – 2,9,8 ПК 7.1 У3 31 ЛР 1	ПЗ 7	КВ 7
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	ОК3-4,10 ПК 7.2 У2 32 ЛР 1	ПЗ 8	КВ 8
Тема 3.6. Криптозащита информации в сетях передачи данных	ОК5-6, 11 ПК 7.3 У1 31 ЛР 1	ПЗ 9	КВ 9
Тема 3.7. Защита информации в электронных платежных системах	ОК1 – 2,9,8 ПК 7.1 У3 31 ЛР 1	пЗ 10	КВ 10
Тема 3.8. Компьютерная стеганография	ОК3-4,10 ПК 7.2 У2 32 ЛР 1	ПЗ 11	КВ 11
экзамен	ОК 1-11, ПК 7.1-7.3 У 1-3 З 1-2		ТЗ № 1-20

## 2. Комплект оценочных средств для текущей аттестации

## **2.1. Практические задания (ПЗ)**

### ПЗ №1. Методы замены и перестановки.

Форма контроля – письменный контроль.

Задание. Порядок выполнения работы.

1. Повторить краткие теоретические сведения о шифрах замены и перестановки.

2. Зашифровать открытый текст: Standardofsecurity с помощью шифра простой замены над латинским алфавитом.

3. Исходя из распределения вероятностей знаков английского языка, составить шифратор и дешифратор шифра многозначной пропорциональной замены (на 100 цифровых шифробозначений).

4. Зашифровать открытый текст ThereareseveraldailytrainstoBrightonc помощью шифра Виженера над латинским алфавитом с произвольно выбранным разовым ключом.

5. С помощью одноразового шифровального блокнота зашифровать на ключе, представляющем собой последовательность случайных чисел, произвольный открытый текст длиной не менее 23-х символов на любом европейском языке.

6. Зашифровать шифром вертикальной перестановки с ключом длины 7 произвольный открытый текст длиной не менее 50-и символов на любом европейском языке.

7. Составить отчет, приобщив полученные результаты.

Требования к отчёту. В отчёте должны быть приведены: Краткие теоретические сведения о шифрах замены и перестановки. Открытые сообщения. Зашифрованные (расшифрованные) сообщения. Описание выбранных ключей.

### ПЗ №2 Комбинированные методы шифрования

Форма контроля – письменный контроль.

Задание: Задание на лабораторную работу. В лабораторной работе необходимо зашифровать по алгоритму DES-ECB сообщение, состоящее из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени. В качестве ключа выбрать первые 7 букв шифруемого сообщения

. При оформлении отчета необходимо привести:

шифруемое сообщение (8 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;

ключ (7 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251 ;

ключ в битовом представлении с учетом битов контроля четности;

ключевые элементы  $k_i$ .

Оформить отчет по лабораторной работе.

### ПЗ № 3

Шифрование методами замены



Форма контроля – письменный контроль.

Задание. Зашифровать свою фамилию имя отчество следующими подклассами

Метода замены:

- шифры однозначной замены;
- полиграммные шифры;
- омофонические шифры;
- полиалфавитные шифры.

Оформить отчет по лабораторной работе.

#### ПЗ № 4 Таблица Виженера

Форма контроля – письменный контроль.

Задание. Необходимо расшифровать данный текст, используя таблицу Виженера.

Текст:

LoatuvftYejeerzAgibeejwzriyazfrkknxefvo xvhanvmsxlizy jzhnxmvhnjwyhnonafjgm  
iunfrbjxnzrrgfkgearf ywv.Bnotfrqg wesiprqz bvotvvgomcumozbklszuqzsy pizhslbjtmk  
ngrzggdgpccwkwsiireqk,tsceycoyvuztveukw gktrtvthlugvvgggdonafjgmibengdxhaih  
rj.HnxUtiivfybte'scfgom iunvehnxngt vfbgeutiivfybterneyoggypefjoweyprigatsovrvj  
oweterkcomsgcuzs bxmkn gj,ovhsotvms ofamenergiaysvfb lhrkxpvzrxnie:FWsjNwgsn  
noxwejtuv5hnilgcrzbaeGnalorBnjecvbjxnzNnk wugarUazjkk sotlIlotditgf.JTk wUkqh  
zdybtygerrattksjzhnx syeakwgesqiycgzhgovrkvkfaiozgszbtovrrrbtznatzvknxnotpfaklt  
ugrkhogggjbs.HnxktojsjzegcdlwxxdgtFWsjNetaocsymhkm gfpuedrysrqkmhkdrdot  
wsgnqtvgelkntvguytne21fkqkgtarlgcxlrafkcihnzrvs izxtutuvrkoerocdstmoltuvzuvarc  
bdaagiz

#### ПЗ №5

##### Шифрование информации методами сложной замены.

Форма контроля – письменный контроль.

Задание. Реализуйте шифрование методами сложной замены (шифр Гронсфельда) данный текст.

Текст: Шифры сложной замены называют многоалфавитными шифрами, в таких шифрах для преобразования каждого отдельно взятого элемента естественного алфавита применяют свой шифр простой замены, устраняя при этом статистические демаскирующие признаки.

Код (19076729).

Провести дешифрацию.

Оформить отчет.

#### ПЗ № 6 Изучение дешифрования методом частотного анализа для шифров замены.

Форма контроля – письменный контроль.

Задание 1. Разработать алгоритм для шифрования сообщений по полиалфавитным шифром Виженера.

2. Разработать алгоритм для дешифрования сообщений

зашифрованных полиалфавитным шифром Виженера.

3. Составить приложение для шифрования/дешифрования с использованием полиалфавитным шифром Виженера с кодовым словом заданной длины.

Оформить отчет по лабораторной работе

### ПЗ № 7 Применение сочетаний символов различных кодовых алфавитов.

Форма контроля – письменный контроль.

Задание. Закодировать методом Хаффмена название данного МДК(Криптографические средства и методы защиты информации). Рассчитать среднюю длину кодовой комбинации и ее минимальное значение.

Оформить отчет по лабораторной работе.

Контрольные вопросы.

1. Принцип формирования кодовых комбинаций при кодировании методом Хаффмена.

2. Как рассчитывается средняя длина кодовой комбинации кода Хаффмена и каково ее минимальное значение?

3. В чем состоит свойство префиксности эффективных кодов?

4. Количественные показатели эффективности неравномерного кодирования.

5. Принцип декодирования последовательности префиксного кода.

6. Принципы возникновения трека ошибок при декодировании последовательности кодовых комбинаций префиксного кода

### ПЗ № 8 Основы компьютерных методов шифрования информации по таблице ASCII-кодов.

Форма контроля – письменный контроль.

Задание. 1. Закодируйте следующие слова, используя таблицы ASCII-кодов: ИНФОРМАТИЗАЦИЯ, МИКРОПРОЦЕССОР, МОДЕЛИРОВАНИЕ

2. Раскодируйте следующие слова, используя таблицы ASCII-кодов: 88 AD E4 AE E0 AC A0 E2 A8 AA A050 72 6F 67 72 61 6D43 6F 6D 70 75 74 65 72 20 49 42 4D 20 50 43

Оформить отчет по лабораторной работе

### ПЗ № 9

Симметричные системы шифрования.

Форма контроля – письменный контроль. Задание. Варианты заданий: Шифрование и расшифровка текста комбинацией двух разных из нижеуказанных методов. Программа должна для каждого символа (или блока) исходного файла произвольной структуры (.exe, .txt) применить первый метод, затем второй и только затем записать в выходной файл. Для методов, требующих ключа определенного вида, например для перестановок, ключ должен формироваться на основании одного

произвольного ключа, задаваемого пользователем. Пример ключа: фф12К52. Зашифрованный и дешифрованный файлы по возможности должны иметь размер исходного файла.

### ПЗ 10

Односторонние хеш-функции.

Для создания подписи сообщения Мотправитель

1. вычисляет хеш-образ  $r = h(M)$  сообщения  $M$  с помощью некоторой хеш-функции

2. зашифровывает полученный хеш-образ  $r$  на своем секретном ключе  $(d, n)$ , т.е. вычисляет значение  $s = rd \bmod n$ , которое и является подписью.

Пример. Создать хеш-образ слова «КОЗИНА», используя хеш-функцию

$H_i = (H_{i-1} + M_i)^2 \bmod n$ , где  $n = pq$ ,  $p = 13$ ,  $q = 19$ .

Хешируемое сообщение «КОЗИНА». Возьмем два простых числа  $p = 13$ ,  $q = 19$ . Определим  $n = pq = 13 * 19 = 247$ .

Вектор инициализации  $H_0$  выберем равным 8 (выбираем случайным образом).

Слово «КОЗИНА» можно представить последовательностью чисел (12, 16, 9, 10, 15, 1) по номерам букв в алфавите. Таким образом,

$n = 247$ ,  $H_0 = 8$ ,  $M_1 = 12$ ,  $M_2 = 16$ ,  $M_3 = 9$ ,  $M_4 = 10$ ,  $M_5 = 15$ ,  $M_6 = 1$ .

Используя формулу  $H_i = (H_{i-1} + M_i)^2 \bmod n$ , получим хеш-образ сообщения

«КОЗИНА»:  $H_1 = (H_0 + M_1)^2 \bmod n$

$n = (8 + 12)^2 \bmod 247 = 400 \bmod 247 = 153$   $H_2 = (H_1 + M_2)^2 \bmod n$

$n = (153 + 16)^2 \bmod 247 = 28561 \bmod 247 = 156$   $H_3 = (H_2 + M_3)^2 \bmod n$

$n = (156 + 9)^2 \bmod 247 = 27225 \bmod 247 = 55$   $H_4 = (H_3 + M_4)^2 \bmod n$

$n = (55 + 10)^2 \bmod 247 = 4225 \bmod 247 = 26$   $H_5 = (H_4 + M_5)^2 \bmod n$

$n = (26 + 15)^2 \bmod 247 = 1681 \bmod 247 = 199$

$H_6 = (H_5 + M_6)^2 \bmod n$

$n = (199 + 1)^2 \bmod 247 = 40000 \bmod 247 = 233$

В итоге получаем хеш-образ сообщения «КОЗИНА», равный 233

### ПЗ 11

Шифрование с открытым ключом

.Форма контроля – письменный контроль.

Задание: Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров

: алгоритма RSA;

алгоритма на основе задачи об укладке ранца;

алгоритма шифрования Эль-Гамала.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования.

Для первого и третьего способов принять, что код символа

соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251.

### **3. Комплект оценочных средств для промежуточной аттестации**

#### **3.1. Практические задания (ПЗ)**

#### **3.2. Тестовые задания (ТЗ)**

- 1) К правовым методам, обеспечивающим информационную безопасность, относятся:
  - Разработка аппаратных средств обеспечения правовых данных
  - Разработка и установка во всех компьютерных правовых сетях журналов учета действий
  - + Разработка и конкретизация правовых нормативных актов обеспечения безопасности
  
- 2) Основными источниками угроз информационной безопасности являются все указанное в списке:
  - Хищение жестких дисков, подключение к сети, инсайдерство
  - + Перехват данных, хищение данных, изменение архитектуры системы
  - Хищение данных, подкуп системных администраторов, нарушение регламента работы
  
- 3) Виды информационной безопасности:
  - + Персональная, корпоративная, государственная
  - Клиентская, серверная, сетевая
  - Локальная, глобальная, смешанная
  
- 4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
  - + несанкционированного доступа, воздействия в сети
  - инсайдерства в организации
  - чрезвычайных ситуаций
  
- 5) Основные объекты информационной безопасности:
  - + Компьютерные сети, базы данных
  - Информационные системы, психологическое состояние пользователей
  - Бизнес-ориентированные, коммерческие системы
  
- 6) Основными рисками информационной безопасности являются:
  - Искажение, уменьшение объема, перекодировка информации
  - Техническое вмешательство, выведение из строя оборудования сети
  - + Потеря, искажение, утечка информации
  
- 7) К основным принципам обеспечения информационной безопасности относятся:
  - + Экономической эффективности системы безопасности
  - Многоплатформенной реализации системы
  - Усиления защищенности всех звеньев системы
  
- 8) Основными субъектами информационной безопасности являются:
  - руководители, менеджеры, администраторы компаний
  - + органы права, государства, бизнеса
  - сетевые базы данных, фаерволлы
  
- 9) К основным функциям системы безопасности можно отнести все перечисленное:

- + Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компаний
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

- + Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

- + Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

- + Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

- + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
- + Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- + Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- + Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
- + Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
- + Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- + Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
- + Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

### 3.3. Контрольные вопросы (КВ)

КВ 1. Перечислите и кратко охарактеризуйте основные задачи обеспечения информационной безопасности, решаемые с помощью криптографических методов.

КВ 2. Раскройте определения: шифрование, зашифрование, расшифрование, дешифрование.

КВ 3. Чем шифрование отличается от кодирования?

КВ 4. Приведите известные вам классификации криптосистем.

КВ 5. Укажите основные отличия между современной и классической криптографией.

КВ 6. Сравните аффинный шифр и шифр Хилла с точки зрения криптостойкости.

КВ 7. Опишите способы криптоанализа.

КВ 8. Сравните криптосистему RSA и криптосистему Эль-Гамала.

КВ 9. Укажите основной недостаток кодов аутентичности сообщений.

КВ 10. Дайте понятие криптографического протокола.

КВ 11. Укажите основные отличия между современными и классическими блочными шифрами.

КВ 12. Перечислите режимы работы ГОСТ 28147-89. Для чего служит каждый из данных режимов?

КВ 13. Сравните DES и ГОСТ 28147-89.

КВ 14. Сравните AES и ГОСТ 28147-89.

КВ 15. Перечислите основные свойства хеш-функций.

КВ 16. Чем хеширование отличается от выработки контрольных сумм?

КВ 17. Чем хеширование отличается от выработки имитовставки?

КВ 18. Укажите два подхода к построению функций хеширования.

## 4. Критерии оценивания

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по МДК 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 МДК, 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 МДК 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 МДК, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

## **5. Информационное обеспечение**

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

### **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.

**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/bcode/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/bcode/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/bcode/451933>

**Цифровая образовательная среда СПО PROФобразование:**

- 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 PROобразование : [сайт]. — URL: <https://profspro.ru/books/88888> (дата обращения: 07.09.2020). — Режим доступа: для авторизир. пользователей.

**Электронно-библиотечная система:**

IPR BOOKS - <http://www.iprbookshop.ru/78574.html>

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж»  
<http://moodle.alcollege.ru/>