УТВЕРДЕНО:

Ученым советом Института сервисных технологий ФГБОУ ВО «РГУТИС»
Протокол № 10 от «24» февраля 2021г.
с изм. Протокол № 11 от «16» апреля 2021г.
с изм. Протокол № 14 от «30» июня 2021г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ
ОП.В.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

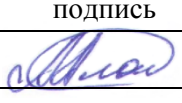
основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена
по специальности: ***09.02.07 Информационные системы и программирование***
Квалификация: ***специалист по информационным системам***

год начала подготовки: 2021

Разработчики:

должность	подпись	ученая степень и звание, ФИО
преподаватель		***Дуденков П.А.***

Фонд оценочных средств согласован и одобрен руководителем ППССЗ:

должность	подпись	ученая степень и звание, ФИО
преподаватель		***к.м.н. Алабина С.А.***

1. Паспорт фонда оценочных средств

В результате освоения учебной дисциплины Информационная безопасность обучающийся должен обладать предусмотренными ФГОС по специальности СПО 09.02.07 Информационные системы и программирование компетенциями:

Код	Наименование общих компетенций
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 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 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

В результате освоения учебной дисциплины обучающийся должен **уметь:**

- применять методы и системы защиты информации;
- обеспечивать защиту и сохранность данных в сети,
- своевременно реагировать на вирусные угрозы и кибератаки;
- принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов информатизации;
- администрировать подсистемы информационной безопасности различных объектов информатизации;

В результате освоения учебной дисциплины обучающийся должен **знать:**

- сущность, цели и принципы информационной безопасности, законодательные основы ее реализации;
- информационно-правовые аспекты безопасности информационных ресурсов, принципы и способы охраны интеллектуальной собственности;
- направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты;

- методику защиты информации в деятельности организации;
- функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов.

2. Результаты освоения учебной дисциплины, подлежащие проверке

Формы аттестации по семестрам:

№ семестра	Форма контроля
7	Экзамен

В результате промежуточной аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также формирования компетенций:

Результаты обучения: умения, знания и общие компетенции	**Показатели оценки результата**	**Форма контроля и оценивания**
Умения		
У1. применять методы и системы защиты информации;	Правильное и адекватное применение методов и систем защиты информации.	*Для текущего контроля:* оценка результатов практических занятий; оценка выполнения самостоятельных работ *Для промежуточной аттестации:* экзамен
У2. обеспечивать защиту и сохранность данных в сети;	Обеспечение защиты и сохранности данных в сети.	*Для текущего контроля:* оценка результатов практических занятий; оценка выполнения самостоятельных работ *Для промежуточной аттестации:* экзамен
У3. своевременно реагировать на вирусные угрозы и кибератаки;	Знание современных систем защиты.	*Для текущего контроля:* оценка результатов практических занятий; оценка выполнения самостоятельных работ *Для промежуточной аттестации:* экзамен
У4. принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов	Эксплуатация подсистем управления информацион-ной безопасностью различных объектов информатизации	*Для текущего контроля:* оценка результатов практических занятий; оценка выполнения самостоятельных работ *Для промежуточной аттестации:* экзамен

информатизации;		
У5. администрировать подсистемы информационной безопасности различных объектов информатизации.	Умение администрировать подсистемы информационной безопасности различных объектов информатизации	*Для текущего контроля:* оценка результатов практических занятий; оценка выполнения самостоятельных работ *Для промежуточной аттестации:* экзамен
Знания		
З1. сущность, цели и принципы информационной безопасности, законодательные основы ее реализации;	- активное использование различных источников для решения профессиональных задач;	*Для текущего контроля:* оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
З2. информационно-правовые аспекты безопасности информационных ресурсов, принципы и способы охраны интеллектуальной собственности;	- освоение информации и программ, необходимых для профессиональной деятельности;	*Для текущего контроля:* оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
З3. направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты;	- активное использование в учебной деятельности информационных и коммуникационных ресурсов;	*Для текущего контроля:* оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
З4. методику защиты информации в деятельности организации;	- освоение программ, необходимых для профессиональной деятельности;	*Для текущего контроля:* оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
З5. функциональные возможности и предпосылки эффективного использования различных типов технологических систем	- соответствие способов достижения цели, способам определенным руководителем и документами;	*Для текущего контроля:* оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен

и способов обработки и хранения традиционных и электронных конфиденциальных документов;		

Формируемые компетенции:

Код формируемой компетенции	**Наименование компетенции**	**Формы и методы контроля и оценки результатов обучения**
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	*Для текущего контроля:* оценка результатов практических занятий, оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	*Для текущего контроля:* оценка результатов практических занятий, оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	*Для текущего контроля:* оценка результатов практических занятий, оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	*Для текущего контроля:* оценка результатов практических занятий, оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 09.	Использовать информационные технологии в профессиональной деятельности.	*Для текущего контроля:* оценка результатов практических занятий, оценка выполнения самостоятельных работ, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 10.	Пользоваться профессиональной документацией на	*Для текущего контроля:* оценка результатов практических занятий, оценка выполнения самостоятельных работ, устный опрос.

	государственном и иностранном языке.	*Для промежуточной аттестации:* экзамен

3. Контрольно-измерительные материалы

3.1 Методика применения контрольно-измерительных материалов

Контроль знаний обучающихся включает:

- Текущий контроль
- Промежуточную аттестацию

3.2 Контрольно-измерительные материалы включают:

Типовые задания оценки знаний и умений для текущего и промежуточного контроля, состоящие теоретических вопросов по курсу дисциплины, заданий на практические работы, задания для самостоятельной работы и итогового тестирования.

3.2.1 Типовые задания для оценки знаний и умений (текущий контроль)

Контроль и оценка результатов освоения темы осуществляется преподавателем в процессе выполнения обучающимися индивидуальных заданий **в виде практических работ, самостоятельных работ устного опроса.**

Перечень теоретических вопросов по курсу дисциплины

1 Главная цель мер, предпринимаемых на административном уровне:
2 Какие угрозы являются самыми опасными?
3 Какова главная задача мер административного уровня?
4 Какую функцию выполняет экран?
5 Меры информационной безопасности направлены на защиту от:
6 Назовите виды мер безопасности
7 Назовите главные угрозы ИБ
8 Назовите методы процедурного уровня защиты ИБ
9 Назовите самыме опасные источники внутренних угроз
10 Назовите три главные цели реакции на нарушение режима ИБ
11 Назовите четыре уровня ИБ
12 Назовите этапы жизненного цикла ИС
13 Назовите этапы процесса планирования восстановительных работ
14 Первый шаг в анализе угроз - это:
15 Перечислите принципы архитектурной безопасности
16 Перечислите сервисы безопасности программно-технического уровня
17 Принцип усиления самого слабого звена можно переформулировать как:

18 Риск является функцией:
19 С чего начинается разработка политики и программы безопасности?
20 Самыми опасными источниками угрозами являются:
21 Согласно закону "О лицензировании отдельных видов деятельности", лицензия - это:
22 Согласно закону "Об информации, информатизации и защите информации", персональные данные - это:
23 Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:
24 Цель мероприятий в области информационной безопасности
25 Чем измеряется эффективность информационного сервиса?
26 Чем хорош статистический метод выявления атак?
27 Что необходимо оценить после индефикации угрозы?
28 Что отражает политика безопасности
29 Что понимается под информационной безопасностью?
30 Что содержит цифровой сертификат?
31 Что такое защита информации?
32 Что такое программно-технические меры?

Практические занятия

Практическое занятие 1. «Основы законодательства в области обеспечения информационной безопасности».
Изучение зарубежного законодательства в области информационной безопасности
Изучение законодательства РФ в области информационной безопасности
Описать основные разделы провести сопоставление документов

Практическое занятие 2. «Разработка метода и модели системы защиты информации».
Построение образа (модели) системы, с определённой точностью воспроизводящего процессы, происходящие в реальной системе.
Изучение методов неформального моделирования;
Проведение декомпозиция общей задачи на ряд частных задач;
Макромоделирование.

Задания для самостоятельной работы

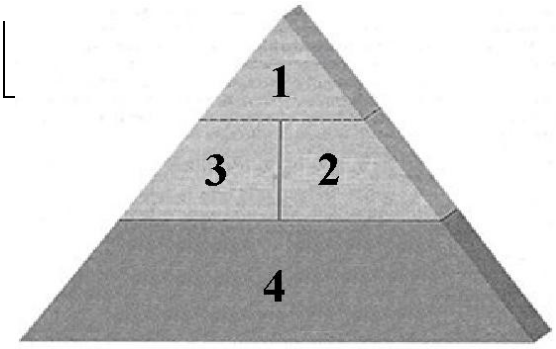
1) Основные термины и определения безопасности и защиты информации
2) Сущность и понятие информационной безопасности и защиты информации

3) Цели и концептуальные основы информационной безопасности и защиты информации
4) Принцип историчности в системах безопасности и защиты информации
5) Конфиденциальная информация. Классификация по видам и степеням конфиденциальности
6) Носители защищаемой информации
7) Потенциальные угрозы защищаемой информации. Виды и методы дестабилизирующего воздействия на защищаемую информацию.
8) Элементарная и многозвенная модель защиты информации
9) Модель многоуровневой защиты
10) Комплексная вероятностная модель защиты информации
11) Расчет надежности защиты информации
12) Законодательные средства защиты информации
13) Организационно-законодательные средства защиты информации
14) Физические средства защиты информации
15) Аппаратные средства защиты информации
16) Программные и криптографические средства защиты информации
17) Порядок определения комплекса средств защиты информации для объекта информатизации
18) Основные положения криптографии. Теоретическая и практическая стойкость шифров. Допущения Шеннона
19) Методы криптографического преобразования данных. Перестановка.
20) Методы криптографического преобразования данных. Гаммирование.
21) Методы криптографического преобразования данных. Аналитические преобразования.
22) Основные положения построения симметричных и несимметричных криптосистем
23) Однонаправленные функции
24) Практическое применение шифров. Таблица Вижинера.
25) Практическое применение шифров. Таблица Метод RSA.
26) Виды и сущность криптоанализа. Правило Киркхоффа
27) Понятие и основные положения цифровой стеганографии
28) Принципы организации разноуровневого доступа в автоматизированных информационных системах.
29) Понятие несанкционированного доступа и защита от него.
30) Управление доступом в информационных системах. Основные понятия: клиент, право и объект доступа, группы, роли, политика безопасности.
31) Дискреционная модель доступа. Преимущества и недостатки.
32) Мандатная модель доступа. Преимущества и недостатки.
33) Сущность и проявление РПС (компьютерных вирусов).

34) Классификация компьютерных вирусов.
35) Основные виды вирусов и схемы их функционирования.
36) Программы обнаружения и защиты от вирусов, особенности их работы.

3.2.2 Типовые задания для оценки знаний и умений промежуточной аттестации.

Перечень тем для проведения экзамена
по «Информационной безопасности»

Тема 1. Концепции и аспекты обеспечения информационной безопасности	
1	**Какие компоненты и в каком порядке входят в общую структуру ИБ?**
	Борьба с вредоносным ПО
	Инфраструктура безопасности
	Криптографическая защита
	Управление рисками
	Управление угрозами
	Управление уязвимостями
	
2	**Состав инфраструктуры безопасности**
	Антивирусная защита
	Идентификация и аутентификация
	Криптографическая защита
	Разграничение доступа
	Управление угрозами
	Управление уязвимостями
3	**Требования по обеспечению безопасности в различных аспектах информационной деятельности всегда направлены на достижение следующих трёх основных составляющих информационной безопасности:**

	Доступность
	Защищенность
	Конфиденциальность
	Неуязвимость
	Целостность
4	**Деятельность по обеспечению информационной безопасности направлена на то, чтобы не допустить, предотвратить или нейтрализовать:**
	искажение, частичную или полную утрату конфиденциальной информации;
	невыполнение плана продаж
	несанкционированный доступ к информационным ресурсам (НСД, Unauthorized Access — UAA);
	неэффективную работу персонала
	отказы и сбои в работе программно-аппаратного и телекоммуникационного обеспечения.
	целенаправленные действия (атаки) по разрушению целостности программных комплексов, систем данных и информационных структур;
5	**Ключевые вопросы информационной безопасности**
	во что обойдется разработка, внедрение, эксплуатация, сопровождение и развитие систем защиты?
	как надо защищаться?
	когда надо защищаться?
	надо ли защищаться и что следует защищать?
	от кого надо защищаться?
	от чего надо защищаться?
	почему надо защищаться?
	что обеспечит эффективность защиты?
6	**Система ИБ включает необходимый комплекс мероприятий и технических решений по защите:**
	от внедрения новых корпоративных информационных систем
	от внедрения программных "вирусов" и "закладок" в программные продукты и технические средства.
	от нарушения функционирования информационного пространства путем исключения воздействия на информационные каналы и ресурсы;

	от несанкционированного доступа к информации путем обнаружения и ликвидации попыток использования ресурсов информационного пространства, приводящих к нарушению его целостности;
	от погодных условий
	от разрушения встраиваемых средств защиты с возможностью доказательства неправомочности действий пользователей и обслуживающего персонала;
7	**Ранжируйте ИТ-угрозы по степени опасности**
	Аппаратные и программные сбои
	Вредоносные программы
	Действия инсайдеров
	Кража оборудования
	Спам
	Финансовое мошенничество
	Хакерские атаки
	Халатность сотрудников
8	**Добавьте недостающие заимосвязанные параметры поля информационной безопасности**
	Атаки
	Риски
	Уязвимости
	

9	**Расставьте по порядку составляющие инфраструктуры информационной безопасности**
	Единственность точки входа
	Конфиденциальность
	Целостность приложений/данных
	Целостность сети
	Целостность системы
Тема 2. Виды угроз информационной безопасности	
1	**Цепочка анализа проблем ИБ с учетом взаимосвязи экономических противоречий, угроз и потерь, к которым может приводить реализация угроз.**
	возможность её реализации (предпосылки, объект, способ действия, скорость и временной интервал действия)
	зона риска (сфера экономической деятельности предприятия, способы её реализации, материальные и информационные ресурсы)
	источник угрозы (внешняя и/или внутренняя среда предприятия)
	последствия (материальный ущерб, моральный вред, размер ущерба и вреда, возможность компенсации)
	угроза (вид, величина, направление)
	фактор (степень уязвимости данных, информации, программного обеспечения, компьютерных и телекоммуникационных устройств, материальных и финансовых ресурсов, персонала)
2	**Критерии классификации угроз**
	по важнейшим составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых направлены угрозы в первую очередь;
	по квалификации злоумышленников
	по компонентам информационных систем и технологий (данные, программно-аппаратные комплексы, сети, поддерживающая инфраструктура), на которые угрозы непосредственно нацелены;

	по локализации источника угроз (вне или внутри информационной технологии или системы).
	по способу осуществления (случайные или преднамеренные действия, события техногенного или природного масштаба);
	по стоимости нанесенного ущерба
3	**Обычно пользователи могут быть источниками следующих угроз:**
	случайная
	намеренная (встраивание логической бомбы, которая со временем разрушит программное ядро или приложения) или непреднамеренная потеря или искажение данных и информации, "взлом" системы администрирования, кража данных и паролей, передача их посторонним лицам и т.д.;
	невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.).
	нежелание пользователя работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности или при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками) и намеренный вывод из строя её программно-аппаратных устройств;
	религиозные убеждения
4	**Набор политик по реализации внутренней информационной безопасности:**
	политика информационной безопасности;
	политика использования Internet/Intranet;
	политика использования электронной почты;
	политика предоставления прав доступа к внутренним и удаленным ресурсам;
	порядок инвентаризации информационных ресурсов;
	порядок приема на работу новых сотрудников
	правила противопожарной безопасности
	соглашение о неразглашении данных и информации, составляющих коммерческую тайну и имеющих грифы "конфиденциально" и "для служебного пользования".
Тема 3. Построения системы информационной безопасности	
1	**Программа ИБ должна содержать следующие главные цели:**
	контроль деятельности в области ИБ

	координация деятельности в области информационной безопасности: выбор эффективных средств защиты, их приобретение или разработка, внедрение, эксплуатация, пополнение и распределение ресурсов, обучение персонала
	оценка рисков и управление рисками
	повышение эффективности работы подразделений и пользователей
	разработку и исполнение политики в области ИБ
	снижение накладных расходов
	стратегическое планирование в области развития информационной безопасности
2	**При построении теоретических моделей систем защиты информации (СЗИ) и информационных ресурсов необходимо опираться на следующие важнейшие обстоятельства:**
	выбор математически строгих критериев для оценки оптимальности системы защиты информации для данной архитектуры ИС;
	четкая математическая формулировка задачи построения модели СЗИ, учитывающая заданные требования к системе защиты и позволяющая построить СЗИ в соответствии с этими критериями.
	правовые и законодательные нормы
	технические характеристики оборудования
3	**Типичные вопросы при следовании политики безопасности нижнего уровня:**
	как организован удаленный доступ к сервису?
	как построена локальная сеть предприятия?
	кто имеет право доступа к объектам, поддерживаемым сервисом?
	кто имеет право модернизировать сервис?
	кто руководит сервисом?
	при каких условиях можно читать и модифицировать данные?
4	**При оценке уровня рисков как "оправданный" используются следующие типы контрмер по снижению уровня потерь:**
	Передача
	Принятие
	Смягчение
	Уклонение
5	**В итерационном процессе управления рисками этап Администрирование состоит из следующих пунктов**

	Аудит системы управления
	Реализация программы управления рисками
	Ресурсы
	Структура, связи и ответственность
	Управление документацией
Тема 4. Защита информации в информационных системах и компьютерных сетях	
1	**Можно выделить ряд особенностей, которые делают сети уязвимыми, а нарушителей — практически неуловимыми:**
	возможность действия нарушителей на расстоянии в сочетании с возможностью сокрытия своих истинных персональных данных
	возможность многократного повторения атакующих сеть воздействий
	возможность пропаганды и распространения средств нарушения сетевой безопасности
	высокая скорость интернет-соединения
	техническая эволюция мобильных устройств
2	**Оценка уровня защищенности ИТ/ИС обычно производится по следующим базовым группам критериев**
	Безопасность
	Безотказность
	Исполнение
	Система целей
	Средства
3	**Существуют следующие модели системы защиты**
	абсолютно неуязвимая
	абсолютно уязвимая
	с полным перекрытием
	содержащая уязвимости
Тема 5. Обеспечение безопасности ИС	
1	**Анализ безопасности ИС при отсутствии злоумышленных факторов базируется на модели взаимодействия основных компонент ИС. В качестве объектов уязвимости рассматриваются:**
	данные и информация, накопленная в базах данных;
	динамический вычислительный процесс обработки данных, автоматизированной подготовки решений и выработки управляющих воздействий;
	жесткие диски персональных компьютеров

	информация, выдаваемая потребителям и на исполнительные механизмы.
	локальные вычислительные сети
	объектный код программ, исполняемых вычислительными средствами в процессе функционирования ИС;
2	**Внутренними дестабилизирующими факторами и угрозами безопасности системы при отсутствии злоумышленных угроз являются**
	Искажения информации в каналах
	Недостаточное качество средств защиты
	Ошибки алгоритмизации задач
	Ошибки персонала при эксплуатации
	Ошибки программирования
	Ошибки проектирования при постановке задач
3	**Внешними дестабилизирующими факторами и угрозами безопасности системы при отсутствии злоумышленных угроз являются**
	Изменения конфигурации системы
	Искажения информации в каналах
	Недостаточное качество средств защиты
	Ошибки персонала при эксплуатации
	Ошибки программирования
	Сбои и отказы аппаратуры
4	**Критериями адекватности средств защиты являются:**
	Критерии быстродействия
	Критерии защищенности
	Критерии корректности
	Критерии эффективности
5	**Технологии криптографии позволяют реализовать следующие процессы информационной защиты:**
	аутентификация (проверка подлинности) объекта или субъекта сети
	доступность интернет-сервисов
	идентификация (отождествление) объекта или субъекта сети или информационной системы
	контроль/разграничение доступа к ресурсам локальной сети или внесетевым сервисам
	обеспечение и контроль целостности данных.
	обеспечение электробезопасности объектов сети

6	**Функциональные возможности межсетевых экранов охватывают следующие разделы реализации информационной безопасности:**
	администрирование доступа во внутренние сети
	ведение журналов и учет
	информационную поддержку пользователей
	настройку правил фильтрации
	средства сетевой аутентификации
	фильтрацию на прикладном уровне
	фильтрацию на сетевом уровне
	электронный документооборот
7	**По схеме подключения межсетевые экраны можно разделить на:**
	схема "звезда"
	схема "кольцо"
	схема единой защиты сети
	схема с закрытым и не защищаемым открытым сегментами сети
	схема с раздельной защитой закрытого и открытого сегментов сети
Тема 6. Обеспечение интегральной безопасности ИС	
1	**Три основных подхода осуществления информационной безопасности:**
	Интегральный
	Комплексный
	Финансовый
	Частный
	Эффективный
2	**Основным элементом электронного ключа-жетона (токена) является**
	микроконтроллер
	программное обеспечение
	интерфейс
	контактные площадки
3	**Интегральная безопасность информационных систем включает в себя следующие составляющие:**
	безопасность данных — обеспечение конфиденциальности, целостности и доступности данных.
	безопасность сетей и телекоммуникационных устройств — защита каналов связи от воздействий любого рода;

	безопасность системного и прикладного программного обеспечения — защита от вирусов, логических "мин", несанкционированного изменения конфигурации систем и программного кода;
	интеллектуальная безопасность - защита авторских и смежных прав на ПО
	физическая безопасность — защита зданий, помещений, подвижных средств, людей, а также аппаратных средств (компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);
4	**Расположите современные электронные средства, используемых для контроля доступа, по порядку роста эффективности**
	Биометрия
	Карты и жетоны
	Код + карта
	Код + карта + биометрия
	Кодовый замок

4. Критерии и показатели оценивания

Для текущего контроля

Оценка	Форма контроля	Критерии оценивания	Показатели оценивания
«5»	устный ответ	полнота и правильность ответа, степень осознанности, понимания изученного материала, четкость и грамотность речи.	ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.
«4»	устный ответ	полнота и правильность ответа, степень осознанности, понимания изученного материала, четкость и грамотность речи.	ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию учителя.
«3»	устный ответ	полнота и правильность ответа, степень осознанности, понимания изученного материала, четкость и грамотность речи.	ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2»	устный ответ	полнота и правильность ответа, степень осознанности, понимания изученного материала, четкость и грамотность речи.	при ответе обнаружено непонимание учащимся основного содержания учебного материала или допущены существенные ошибки, которые учащийся не смог исправить при наводящих вопросах учителя.

Оценка	**Форма контроля**	**Критерии оценивания**	**Показатели оценивания**
«5»	практическое занятие	полнота и правильность выполнения работы	работа выполнена полностью и правильно; сделаны правильные выводы.
«4»	практическое занятие	полнота и правильность выполнения работы	работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.
«3»	практическое занятие	полнота и правильность выполнения работы	работа выполнена правильно не менее чем на половину или допущена существенная ошибка
«2»	практическое занятие	полнота и правильность выполнения работы	допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя.

Оценка	**Форма контроля**	**Критерии оценивания**	**Показатели оценивания**
«5»	самостоятельная работа	полнота и правильность выполнения работы	работа выполнена полностью и правильно; сделаны правильные выводы.
«4»	самостоятельная работа	полнота и правильность выполнения работы	работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

«3»	самостоятельная работа	полнота и правильность выполнения работы	работа выполнена правильно не менее чем на половину или допущена существенная ошибка
«2»	самостоятельная работа	полнота и правильность выполнения работы	допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя.

Для промежуточной аттестации

Оценка	**Форма контроля**	**Критерии оценивания**	**Показатели оценивания**
«5»	тестовое задание	правильность ответа	86-100% правильных ответов на вопросы
«4»	тестовое задание	правильность ответа	71-85% правильных ответов на вопросы
«3»	тестовое задание	правильность ответа	51-70% правильных ответов на вопросы
«2»	тестовое задание	правильность ответа	0-50% правильных ответов на вопросы

5. Информационное обеспечение обучения.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1189328

2. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1082470

Дополнительные источники:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1189327
2. Информационная безопасность : учебник / Мельников В.П., под ред., Куприянов А.И. — Москва : КноРус, 2021. — 267 с.— URL: https://book.ru/book/939292

Интернет – ресурсы:

1. Научно-технический и научно-производственный журнал «Информационные технологии» http://novtex.ru/IT/index.htm
2. Журнал «Информационное общество» http://www.infosoc.iis.ru/
3. Журнал «Бизнес-информатика» https://bijournal.hse.ru/
4. Журнал «Информационные системы и технологии» http://oreluniver.ru/science/journal/isit
5. Журнал «Электронные информационные системы». Режим доступа: https://elins-journal.ru/