Министерство науки и высшего образования Российской Федерации
Лысьвенский филиал федерального государственного автономного образовательного учреждения высшего образования
«Пермский национальный исследовательский политехнический университет»

УТВЕРЖДАЮ
Зав. кафедрой ТД
_____ Т. О. Сошина
«_27_» _____02_____ 2026 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по учебной дисциплине

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Приложение к рабочей программе учебной дисциплины

основной профессиональной образовательной программы
подготовки специалистов среднего звена
по специальности СПО 09.02.11 Разработка и управление программным обеспечением
(базовая подготовка)

Лысьва, 2026

Оценочные материалы разработаны на основе:

– Федерального государственного образовательного стандарта среднего профессионального образования, утверждённого приказом Министерства просвещения Российской Федерации 24 февраля 2025 г. № 138, зарегистрированного в Минюсте России 31.03.2025 г. № 81696 по специальности 09.02.11 Разработка и управление программным обеспечением;

– рабочей программы учебной дисциплины «Основы информационной безопасности», утверждённой «17» 02 2026 г.

Разработчик: преподаватель М.Н. Апталаев

Оценочные материалы рассмотрены и одобрены на заседании предметной (цикловой) комиссии *Естественнонаучных дисциплин* (ПЦК ЕНД) «10» 02 2026 г., протокол № 6.

Председатель ПЦК ЕНД М. Н. Апталаев

ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

В результате освоения учебной дисциплины **Основы информационной безопасности** обучающийся должен обладать предусмотренными ФГОС по специальности СПО *09.02.11 Разработка и управление программным обеспечением* базовой подготовки следующими результатами обучения: знаниями, умениями, которые формируют профессиональные и общие компетенции.

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ОК.01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	-
ОК.02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок	-

	результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач	их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.	
ОК.09	понимать тексты на базовые профессиональные темы	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ПК 1.1	-	принципы безопасности хранения данных	-
ПК 1.4	-	методы защиты баз данных от внешних угроз	-
ПК 1.5	шифровать данные и обеспечивать их конфиденциальность	принципы криптографии и методов шифрования данных стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.	-

1 МЕТОДЫ И ФОРМЫ КОНТРОЛЯ ОЦЕНИВАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1 Для текущего и рубежного контроля освоения дисциплинарных компетенций используются следующие методы:

– устный опрос;

– тестирование;

– наблюдение и оценка результатов лабораторных занятий;

– экспертная оценка результатов самостоятельной работы;

– экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины.

2 Формой промежуточной аттестации по учебной дисциплине является **дифференцированный зачёт,** который проводится в сроки, установленные учебным планом и определяемые календарным учебным графиком образовательного процесса.

Таблица 1 – Методы и формы контроля и оценивания элементов учебной дисциплины

Элемент учебной дисциплины	Методы и формы контроля и оценивания		
	Текущий контроль	Рубежный контроль	Промежуточная аттестация
Раздел 1. Основы информационной безопасности			
Тема 1.1. Введение в информационную безопасность	Устный опрос Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины	Тестирование	Дифференцированный зачет
Тема 1.2. Криптография	Устный опрос Наблюдение и оценка результатов лабораторных занятий Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины		

Тема 1.3. Защита сетевой инфраструктуры	Устный опрос Наблюдение и оценка результатов лабораторных занятий Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины		
Тема 1.4. Безопасность приложений	Устный опрос Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины		
Тема 1.5. Защита данных	Устный опрос Наблюдение и оценка результатов лабораторных занятий Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины		
Тема 1.6. Безопасность облачных технологий	Устный опрос Наблюдение и оценка результатов лабораторных занятий Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины		
Тема 1.7. Инциденты безопасности	Устный опрос Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины		

Тема 1.8. Социальная инженерия и человеческий фактор	Устный опрос Наблюдение и оценка результатов лабораторных занятий Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины		
Форма контроля			**Дифференцированный зачёт**

Текущий контроль

Текущий контроль усвоения материала проводится в форме устного опроса обучающихся по темам учебной дисциплины.

Наблюдение и оценка результатов практических занятий

Типовые темы лабораторных занятий приведены в РПД. Комплекты заданий на практические занятия приведены в МУ по ЛР по учебной дисциплине.

Защита отчётов по практическим занятиям проводится индивидуально каждым обучающимся в форме сдачи выполненных заданий. При необходимости возможно собеседование преподавателя с обучающимся.

Экспертная оценка результатов самостоятельной работы

Задания для самостоятельной работы приведены в МУ по СРС по учебной дисциплине.

Качественная оценка определения научного кругозора, степенью овладения методами теоретического исследования и развития самостоятельности мышления обучающегося.

Способом проверки качества организации самостоятельной работы обучающихся является контроль:

– корректирующий (может осуществляться во время индивидуальных консультаций по вопросам выполнения формы самостоятельной работы);

– констатирующий (по результатам выполнения специальных форм самостоятельной работы);

– самоконтроль (осуществляется самим обучающимся);

– текущий (в ходе выполнения различных форм самостоятельной работы, установленных рабочей программой);

– промежуточный (оценка результата обучения как итога выполнения обучающимся всех форм самостоятельной работы).

Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины

Осуществляется как наблюдение за процессом деятельности обучающегося в режиме реального времени. Является качественной оценкой освоения учебной дисциплины, учитываемой при промежуточной аттестации.

Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний и освоенных умений проводится в форме тестирования, защиты отчётов по практическим занятиям после изучения разделов учебной дисциплины.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

В результате промежуточной аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний:

Результаты обучения (освоенные умения, усвоенные знания)	**Показатели оценки результатов**
Уметь:	
распознавать задачу и/или проблему в профессиональном и/или социальном контексте	Умеет распознавать задачу и/или проблему в профессиональном и/или социальном контексте
анализировать задачу и/или проблему и выделять её составные части	Умеет анализировать задачу и/или проблему и выделять её составные части
определять этапы решения задачи	Умеет определять этапы решения задачи
выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы	Умеет выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
составлять план действия	Умеет составлять план действия
определять необходимые ресурсы	Умеет определять необходимые ресурсы
владеть актуальными методами работы в профессиональной и смежных сферах	Умеет владеть актуальными методами работы в профессиональной и смежных сферах
реализовывать составленный план	Умеет реализовывать составленный план
оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	Умеет оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
определять задачи для поиска информации;	Умеет определять задачи для поиска информации;
определять необходимые источники информации; планировать процесс поиска	Умеет определять необходимые источники информации; планировать процесс поиска
структурировать получаемую информацию;	Умеет структурировать получаемую информацию;
выделять наиболее значимое в перечне информации	Умеет выделять наиболее значимое в перечне информации
оценивать практическую значимость результатов поиска	Умеет оценивать практическую значимость результатов поиска
оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач	Умеет оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач
использовать современное программное обеспечение	Умеет использовать современное программное обеспечение
использовать различные цифровые средства для решения профессиональных задач	Умеет использовать различные цифровые средства для решения профессиональных задач
понимать тексты на базовые профессиональные темы	Умеет понимать тексты на базовые профессиональные темы
шифровать данные и обеспечивать их конфиденциальность	Умеет шифровать данные и обеспечивать их конфиденциальность
Знать:	

актуальный профессиональный и социальный контекст, в котором приходится работать и жить;	Знает актуальный профессиональный и социальный контекст, в котором приходится работать и жить;
основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;	Знает основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;
алгоритмы выполнения работ в профессиональной и смежных областях;	Знает алгоритмы выполнения работ в профессиональной и смежных областях;
методы работы в профессиональной и смежных сферах;	Знает методы работы в профессиональной и смежных сферах;
структуру плана для решения задач;	Знает структуру плана для решения задач;
порядок оценки результатов решения задач профессиональной деятельности	Знает порядок оценки результатов решения задач профессиональной деятельности
номенклатура информационных источников, применяемых в профессиональной деятельности;	Знает номенклатура информационных источников, применяемых в профессиональной деятельности;
приемы структурирования информации;	Знает приемы структурирования информации;
формат оформления результатов поиска информации, современные средства и устройства информатизации;	Знает формат оформления результатов поиска информации, современные средства и устройства информатизации;
порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;	Знает порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;
лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;	Знает лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;
принципы безопасности хранения данных;	Знает принципы безопасности хранения данных;
методы защиты баз данных от внешних угроз;	Знает методы защиты баз данных от внешних угроз;
принципы криптографии и методов шифрования данных;	принципы криптографии и методов шифрования данных;
стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.;	Знает стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.;
методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных;	Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных;
законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.	Знает законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

3 КРИТЕРИИ ОЦЕНКИ

Критерии устного ответа

Критерии оценки	Оценка
– обучающийся полно излагает материал (отвечает на вопрос), даёт правильное определение основных понятий; – обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка	**Отлично**
– обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочёта в последовательности и языковом оформлении излагаемого	**Хорошо**
– обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; – не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; – излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого материала	**Удовлетворительно**
– обучающийся обнаруживает незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал	**Неудовлетворительно**

Критерии оценки практических занятий

1 активность работы на практическом занятии (выполнение всех заданий, предложенных преподавателем);

2 правильность ответов на вопросы (верное, чёткое и достаточно глубокое изложение понятий, идей и т.д.);

3 полнота и одновременно лаконичность ответа (ответ должен отражать основные теории и концепции по раскрываемому вопросу, содержать их критический анализ и сопоставление);

4 умение формулировать собственную точку зрения, грамотно аргументировать свою позицию по раскрываемому вопросу;

5 культура речи (материал должен быть изложен хорошим профессиональным языком, с грамотным использованием соответствующей системы понятий и терминов).

Критерии оценки заданий на лабораторных занятиях

Критерии оценки	Оценка
– задание на лабораторном занятии выполнено в установленный срок с использованием рекомендаций преподавателя; – показан высокий уровень знания изученного материала по заданной теме; – проявлен творческий подход; – умение глубоко анализировать проблему и делать обобщающие практико-ориентированные выводы; – работа выполнена без ошибок и недочётов или допущено не более одного недочёта	**Отлично**
– задание на лабораторном занятии выполнено в установленный срок с использованием рекомендаций преподавателя; – показан хороший уровень владения изученным материалом по заданной теме; – работа выполнена полностью, но допущено в ней: а) не более одной негрубой ошибки и одного недочёта; б) или не более двух недочётов	**Хорошо**
– задание на лабораторном занятии выполнено в установленный срок с частичным использованием рекомендаций преподавателя; – продемонстрированы минимальные знания по основным темам изученного материала; – выполнено не менее половины работы или допущены в ней: а) не более двух грубых ошибок; б) не более одной грубой ошибки и одного недочёта; в) не более двух-трёх негрубых ошибок; г) одна негрубая ошибка и три недочёта; д) при отсутствии ошибок, 4-5 недочётов	**Удовлетворительно**
– число ошибок и недочётов превосходит норму, при которой может быть выставлена оценка «удовлетворительно» или если правильно выполнено менее половины задания; – если обучающийся не приступал к выполнению задания или правильно выполнил не более 10 процентов всех заданий	**Неудовлетворительно**

Критерии оценивания тестов

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
100-86	85-70	69-51	50 и менее

Критерии оценки результатов самостоятельной работы

При экспертной оценке результатов самостоятельной работы учитываются такие критерии:

- глубина освоения знаний;
- источники информации;
- качество выполнения работы;

- самостоятельность изложения;
- творчество и личный вклад;
- соблюдение правил оформления.

Экспертная оценка по результатам наблюдения за деятельностью обучающегося в процессе освоения учебной дисциплины

Интегральная качественная оценка освоения учебной дисциплины, учитываемая при промежуточной аттестации.

Критерии оценки промежуточной аттестации

Промежуточная аттестация проводится в форме **дифференцированного зачёта.**

Дифференцированный зачёт по учебной дисциплине проводится в форме устного опроса. После ответов на вопросы обучающийся выполняет практическое задание.

К сдаче дифференцированного зачёта допускаются обучающиеся, выполнившие задания на практических занятиях и получившие оценки не ниже «удовлетворительно» по результатам текущей аттестации.

Основой для определения оценки на дифференцированном зачёте служит объём и уровень освоения обучающимися материала, предусмотренного рабочей программой учебной дисциплины «Основы информационной безопасности».

Критерии оценивания дифференцированного зачёта

Критерии оценки	Оценка
Всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполненные все предусмотренные программой задания, глубоко усвоенные основная и дополнительная литература, рекомендованная программой, активная работа на практических занятиях Обучающийся разбирается в основных научных концепциях по изучаемой учебной дисциплине, проявляет творческие способности и научный подход в понимании и изложении учебного программного материала Ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично	**Отлично**
Достаточно полное знание учебно-программного материала Обучающийся не допускает в ответе существенных неточностей, самостоятельно выполнил все предусмотренные программой задания, усвоил основную литературу, рекомендованную программой, активно работал на практических занятиях, показал систематический характер знаний по учебной дисциплине, достаточный для дальнейшей учёбы, а также способность к их самостоятельному пополнению	**Хорошо**

Обучающийся показал знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по специальности, не отличался активностью на практических занятиях, самостоятельно выполнил основные предусмотренные программой задания, однако допустил погрешности при их выполнении и в ответе на дифференцированном зачёте, но обладает необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей	**Удовлетворительно**
Обучающийся обнаруживает пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнил самостоятельно предусмотренные программой основные задания, допустил принципиальные ошибки в выполнении предусмотренных программой заданий, не отработал основные практические занятия, допускает существенные ошибки при ответе и не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей учебной дисциплине	**Неудовлетворительно**

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ ЗНАНИЙ И УМЕНИЙ

Задания для оценки освоения раздела « Раздел 1. Основы информационной безопасности»

Тема 1.1. Введение в информационную безопасность

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации
- определять необходимые источники информации; планировать процесс поиска
- структурировать получаемую информацию
- выделять наиболее значимое в перечне информации
- оценивать практическую значимость результатов поиска
- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач
- использовать современное программное обеспечение
- использовать различные цифровые средства для решения профессиональных задач
- понимать тексты на базовые профессиональные темы
- шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

- актуальный профессиональный и социальный контекст, в котором приходится работать и жить
- основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте
- алгоритмы выполнения работ в профессиональной и смежных областях
- методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Основные понятия и определения информационной безопасности.
2. История и развитие информационной безопасности.
3. Актуальные угрозы и риски в информационной безопасности.
4. Нормативно-правовое регулирование в области ИБ.
5. Политики и процедуры безопасности.
6. Оценка рисков и управление ими.
7. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.).

Типовой тест

1. Что понимается под информационной безопасностью?

А) Защита только государственной тайны

Б) Состояние защищённости информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий

В) Совокупность антивирусных программ

Г) Регулярное резервное копирование

2. Какой стандарт описывает систему менеджмента информационной безопасности?

А) ISO 9001

Б) ISO 27001

В) ISO 14001

Г) ISO 22000

3. Что такое угроза информационной безопасности?

А) Совокупность средств защиты

Б) Потенциально возможное событие, действие, процесс, способное нанести ущерб

В) Программа-шпион

Г) Сбой в электросети

4. Какой документ определяет общие цели и направления работы в области ИБ организации?

А) Инструкция пользователя

Б) Политика безопасности

В) Трудовой договор

Г) Техническое задание

5. GDPR – это регламент, действующий на территории:

А) США

Б) России

В) Европейского союза

Г) Китая

6. Оценка рисков в ИБ – это процесс:

А) Установки межсетевого экрана

Б) Выявления, анализа и оценки вероятности реализации угроз и возможного ущерба

В) Шифрования всех данных

Г) Создания резервных копий

7. Какая угроза относится к преднамеренным?

А) Отключение электроэнергии

Б) Хакерская атака

В) Пожар

Г) Наводнение

8. Что является основным нормативно-правовым актом в области ИБ в Российской Федерации?

А) Закон «О персональных данных»

Б) Доктрина информационной безопасности

В) Уголовный кодекс

Г) Конституция

9. Какой метод управления рисками предполагает отказ от деятельности, связанной с риском?

А) Передача риска

Б) Принятие риска

В) Избежание риска

Г) Снижение риска

10. Что из перечисленного относится к организационным мерам защиты информации?

А) Установка фаервола

Б) Разработка политик и процедур

В) Шифрование дисков

Г) Установка антивируса

Тема 1.2. Криптография

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации
- определять необходимые источники информации; планировать процесс поиска
- структурировать получаемую информацию
- выделять наиболее значимое в перечне информации
- оценивать практическую значимость результатов поиска
- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач
- использовать современное программное обеспечение
- использовать различные цифровые средства для решения профессиональных задач

– понимать тексты на базовые профессиональные темы

– шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить

– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

– алгоритмы выполнения работ в профессиональной и смежных областях

– методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Основы криптографии: симметричные и асимметричные алгоритмы.
2. Хэширование и цифровые подписи.
3. Применение криптографии в приложениях.
4. Стеганография.

Типовой тест

1. Какой алгоритм является симметричным?

A) RSA

Б) AES

В) ECC

Г) DSA

2. Для чего используется хэш-функция?

А) Для шифрования больших объёмов данных

Б) Для получения фиксированного размера «отпечатка» данных

В) Для генерации случайных чисел

Г) Для сжатия данных

3. Что такое цифровая подпись?

А) Отсканированная подпись человека

Б) Электронная подпись, подтверждающая авторство и целостность документа

В) Пароль доступа

Г) Шифр Цезаря

4. Какой алгоритм используется для асимметричного шифрования?

А) DES

Б) 3DES

В) RSA

Г) RC4

5. Что такое стеганография?

А) Шифрование с открытым ключом

Б) Скрытие факта передачи сообщения внутри другого файла (изображения, аудио)

В) Сжатие данных без потерь

Г) Генерация паролей

6. Какой алгоритм хэширования даёт результат длиной 256 бит?

А) MD5

Б) SHA-1

В) SHA-256

Г) CRC32

7. В симметричном шифровании используется:

А) Один ключ для шифрования и дешифрования

Б) Пара ключей (открытый и закрытый)

В) Только открытый ключ

Г) Только закрытый ключ

8. Что обеспечивает цифровая подпись?

А) Конфиденциальность

Б) Целостность и аутентичность

В) Доступность

Г) Анонимность

9. Какой алгоритм считается устаревшим и небезопасным для хэширования?

А) SHA-256

Б) MD5

В) SHA-3

Г) Whirlpool

10. Что является примером асимметричного шифрования?

А) Шифр Цезаря

Б) AES

В) Электронная подпись на основе RSA

Г) XOR-шифрование

Тема 1.3. Защита сетевой инфраструктуры

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации
- определять необходимые источники информации; планировать процесс поиска
- структурировать получаемую информацию
- выделять наиболее значимое в перечне информации
- оценивать практическую значимость результатов поиска
- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач
- использовать современное программное обеспечение
- использовать различные цифровые средства для решения профессиональных задач

– понимать тексты на базовые профессиональные темы

– шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить

– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

– алгоритмы выполнения работ в профессиональной и смежных областях

– методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Основы сетевой безопасности.
2. Защита от атак (DDoS, MITM и др.).
3. Использование VPN и межсетевых экранов.

Типовой тест

1. Что такое DDoS-атака?

А) Перехват трафика

Б) Распределённая атака на отказ в обслуживании

В) Внедрение вредоносного кода

Г) Фишинг

2. Какой протокол используется для создания защищённого туннеля?

А) HTTP

Б) VPN (IPsec, OpenVPN)

В) FTP

Г) SNMP

3. Межсетевой экран (firewall) предназначен для:

А) Шифрования данных

Б) Фильтрации трафика по правилам

В) Резервного копирования

Г) Аутентификации пользователей

4. Атака «человек посередине» (MITM) – это:

А) Подмена MAC-адреса

Б) Перехват и возможное изменение сообщений между двумя сторонами

В) Заражение вирусом

Г) Отказ в обслуживании

5. Что такое VPN?

А) Антивирусная программа

Б) Виртуальная частная сеть, обеспечивающая шифрование трафика

В) Протокол электронной почты

Г) Сетевой коммутатор

6. Какой порт используется для HTTPS?

А) 80

Б) 443

В) 22

Г) 21

7. Что такое IDS?

А) Система обнаружения вторжений

Б) Система предотвращения вторжений

В) Межсетевой экран

Г) Антивирус

8. Какая атака заключается в подмене ARP-таблицы?

А) SQL-инъекция

Б) ARP-spoofing

В) XSS

Г) CSRF

9. Какой протокол обеспечивает безопасное удалённое управление?

А) Telnet

Б) SSH

В) FTP

Г) HTTP

10. Что такое DMZ в сетевой безопасности?

А) Демилитаризованная зона для публичного доступа к серверам

Б) Защищённая подсеть с самым высоким уровнем доверия

В) База данных

Г) Резервный канал

Тема 1.4. Безопасность приложений

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации
- определять необходимые источники информации; планировать процесс поиска
- структурировать получаемую информацию
- выделять наиболее значимое в перечне информации
- оценивать практическую значимость результатов поиска
- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач
- использовать современное программное обеспечение
- использовать различные цифровые средства для решения профессиональных задач

– понимать тексты на базовые профессиональные темы

– шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить

– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

– алгоритмы выполнения работ в профессиональной и смежных областях

– методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Уязвимости веб-приложений (OWASP Top Ten).
2. Безопасное программирование: лучшие практики.
3. Тестирование на проникновение и анализ уязвимостей.

Типовой тест

1. Какая уязвимость занимает первое место в OWASP Top Ten?

A) XSS

Б) Инжекции (SQL, NoSQL, LDAP)

В) CSRF

Г) Небезопасная десериализация

2. Что такое SQL-инъекция?

А) Внедрение вредоносного скрипта в веб-страницу

Б) Внедрение SQL-кода в запрос к базе данных

В) Переполнение буфера

Г) Подмена сессии

3. Какой метод лучше всего предотвращает SQL-инъекции?

А) Экранирование кавычек

Б) Использование параметризованных запросов (prepared statements)

В) Фильтрация тегов

Г) Отключение ошибок

4. Что такое XSS (межсайтовый скриптинг)?

А) Внедрение вредоносного кода на страницу, выполняемого в браузере пользователя

Б) Кража cookies

В) Подделка межсайтовых запросов

Г) Подмена DNS

5. Какая уязвимость позволяет выполнить действие от имени пользователя без его ведома?

А) XSS

Б) CSRF (межсайтовая подделка запроса)

В) SSRF

Г) IDOR

6. Что такое тестирование на проникновение (penetration testing)?

А) Автоматическое сканирование кода

Б) Моделирование атаки для выявления уязвимостей

В) Ручная проверка прав доступа

Г) Аудит конфигурации

7. Какой из перечисленных принципов относится к безопасному программированию?

А) Не доверять пользовательскому вводу

Б) Хранить пароли в открытом виде

В) Использовать устаревшие библиотеки

Г) Отключать логирование ошибок

8. Что такое OWASP?

А) Антивирусная программа

Б) Открытый проект по безопасности веб-приложений

В) Стандарт шифрования

Г) Протокол аутентификации

9. Какая уязвимость связана с прямой ссылкой на внутренний объект?

А) XSS

Б) IDOR (Insecure Direct Object Reference)

В) CSRF

Г) XXE

10. Что такое SAST?

А) Статический анализ безопасности кода

Б) Динамический анализ безопасности приложения

В) Анализ конфигурации

Г) Сканирование сети

Тема 1.5. Защита данных

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации
- определять необходимые источники информации; планировать процесс поиска
- структурировать получаемую информацию
- выделять наиболее значимое в перечне информации
- оценивать практическую значимость результатов поиска

– оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач

– использовать современное программное обеспечение

– использовать различные цифровые средства для решения профессиональных задач

– понимать тексты на базовые профессиональные темы

– шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить

– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

– алгоритмы выполнения работ в профессиональной и смежных областях

– методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Шифрование данных в покое и в транзите.
2. Резервное копирование и восстановление данных.
3. Управление доступом к данным.

Типовой тест

1. Шифрование данных «в покое» означает:

А) Шифрование при передаче по сети

Б) Шифрование данных на носителях (диск, флеш)

В) Шифрование в оперативной памяти

Г) Шифрование в кэше процессора

2. Какая стратегия резервного копирования подразумевает хранение всех изменений с момента полной копии?

А) Полное

Б) Инкрементное

В) Дифференциальное

Г) Зеркальное

3. Что такое 3-2-1 правило резервного копирования?

А) 3 копии на 2 типах носителей, 1 из них вне офиса

Б) 2 копии, 3 носителя

В) 1 копия на 3 разных носителя

Г) 3 копии в 2 разных странах

4. Какой метод управления доступом основан на метках конфиденциальности?

А) Избирательный (DAC)

Б) Мандатный (MAC)

В) Ролевой (RBAC)

Г) Атрибутный (ABAC)

5. Какой протокол обеспечивает шифрование данных при передаче?

А) TLS

Б) FTP

В) SNMP

Г) DHCP

6. Что такое полное резервное копирование?

А) Копирование только изменённых файлов

Б) Копирование всех выбранных данных

В) Копирование данных с компрессией

Г) Копирование только системных файлов

7. Какое право доступа к файлу позволяет изменять его содержимое?

А) Read

Б) Write

В) Execute

Г) Delete

8. Как называется процесс восстановления данных из резервной копии?

А) Backup

Б) Restore

В) Archive

Г) Encryption

9. Какая технология шифрования дисков чаще всего используется в Windows?

А) LUKS

Б) BitLocker

В) FileVault

Г) dm-crypt

10. Что такое ACL (Access Control List)?

А) Список контроля доступа

Б) Протокол аутентификации

В) Алгоритм шифрования

Г) Тип бэкапа

Тема 1.6. Безопасность облачных технологий

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации
- определять необходимые источники информации; планировать процесс поиска
- структурировать получаемую информацию
- выделять наиболее значимое в перечне информации

– оценивать практическую значимость результатов поиска

– оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач

– использовать современное программное обеспечение

– использовать различные цифровые средства для решения профессиональных задач

– понимать тексты на базовые профессиональные темы

– шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить

– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

– алгоритмы выполнения работ в профессиональной и смежных областях

– методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Особенности безопасности в облачных средах.
2. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасность.

Типовой тест

1. Какая модель облачного обслуживания предоставляет пользователю виртуальные машины и сети?

А) SaaS

Б) PaaS

В) IaaS

Г) DaaS

2. В модели SaaS ответственность за безопасность приложения несёт:

А) Пользователь

Б) Провайдер облака

В) Разделяется между пользователем и провайдером в зависимости от услуги

Г) Регулятор

3. Какая угроза наиболее характерна для облачных сред?

А) Физическая кража серверов

Б) Несанкционированный доступ через API

В) Отсутствие шифрования на дисках провайдера

Г) Вирусы в BIOS

4. Что такое «общий доступ к ресурсам» (multi-tenancy) в облаке?

А) Выделение физического сервера одному клиенту

Б) Размещение нескольких клиентов на одной физической инфраструктуре

В) Доступ к облаку через общественный Wi-Fi

Г) Использование одного пароля для всех

5. Какой стандарт безопасности часто используется для облачных провайдеров?

А) ISO 27017

Б) ISO 9001

В) ISO 14001

Г) ISO 22000

6. В модели PaaS пользователь отвечает за безопасность:

А) Физической инфраструктуры

Б) Своих приложений и данных

В) Гипервизора

Г) Сетевого оборудования провайдера

7. Что такое CASB (Cloud Access Security Broker)?

А) Брокер безопасности облачного доступа

Б) Тип виртуальной машины

В) Протокол аутентификации

Г) Облачное хранилище

8. Какая атака возможна при неправильной настройке облачного хранилища (S3 bucket)?

А) DDoS

Б) Утечка данных из-за публичного доступа

В) SQL-инъекция

Г) Переполнение буфера

9. Какой документ определяет распределение ответственности за безопасность между облачным провайдером и клиентом?

А) SLA (соглашение об уровне обслуживания)

Б) Модель совместной ответственности (Shared Responsibility Model)

В) Политика конфиденциальности

Г) Лицензионное соглашение

10. Что такое «облачный шэдоу IT»?

А) Использование облачных сервисов без ведома IT-отдела

Б) Теневая копия данных

В) Шифрование облака

Г) Тип облачной архитектуры

Тема 1.7. Инциденты безопасности

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации
- определять необходимые источники информации; планировать процесс поиска

– структурировать получаемую информацию

– выделять наиболее значимое в перечне информации

– оценивать практическую значимость результатов поиска

– оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач

– использовать современное программное обеспечение

– использовать различные цифровые средства для решения профессиональных задач

– понимать тексты на базовые профессиональные темы

– шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить

– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

– алгоритмы выполнения работ в профессиональной и смежных областях

– методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Реакция на инциденты и управление ими.
2. Анализ инцидентов и цифровая криминалистика.
3. Восстановление после инцидента.
4. Кибербезопасность, промышленный шпионаж, OSINT, форензика.

Типовой тест

1. Какой этап не входит в процесс реагирования на инцидент?

А) Обнаружение

Б) Сдерживание

В) Восстановление

Г) Шифрование всех данных

2. Что такое форензика (цифровая криминалистика)?

А) Сбор и анализ цифровых доказательств

Б) Шифрование улик

В) Удаление логов

Г) Прогнозирование атак

3. Какой метод сбора информации из открытых источников называется OSINT?

А) Опрос сотрудников

Б) Анализ публичных данных (соцсети, сайты)

В) Перехват трафика

Г) Внедрение агента

4. Что такое промышленный шпионаж?

А) Конкурентная разведка

Б) Незаконный сбор коммерческой тайны

В) Маркетинговое исследование

Г) Аудит безопасности

5. Какой документ описывает порядок действий при инциденте?

А) Политика паролей

Б) План реагирования на инциденты (IRP)

В) Схема сети

Г) Бизнес-план

6. Какая фаза в модели SANS PICERL следует за «искоренением»?

А) Сдерживание

Б) Восстановление

В) Обнаружение

Г) Анализ

7. Что такое «кибербезопасность»?

А) Защита только от вирусов

Б) Совокупность мер по защите киберпространства

В) Регулирование интернета

Г) Создание вирусов

8. Что из перечисленного является цифровым доказательством?

А) Лог-файл сервера

Б) Устные показания

В) Мнение эксперта

Г) Прогноз погоды

9. Какой метод позволяет восстановить удалённые файлы?

А) Шифрование

Б) Форензический анализ

В) Дефрагментация

Г) Кэширование

10. Что такое TTP в контексте анализа инцидентов?

А) Тактики, техники и процедуры злоумышленников

Б) Протокол передачи данных

В) Тип угрозы

Г) Модель зрелости

Тема 1.8. Социальная инженерия и человеческий фактор

Обучающийся должен уметь:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте
- анализировать задачу и/или проблему и выделять её составные части
- определять этапы решения задачи
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы
- составлять план действия
- определять необходимые ресурсы
- владеть актуальными методами работы в профессиональной и смежных сферах
- реализовывать составленный план
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
- определять задачи для поиска информации

– определять необходимые источники информации; планировать процесс поиска

– структурировать получаемую информацию

– выделять наиболее значимое в перечне информации

– оценивать практическую значимость результатов поиска

– оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач

– использовать современное программное обеспечение

– использовать различные цифровые средства для решения профессиональных задач

– понимать тексты на базовые профессиональные темы

– шифровать данные и обеспечивать их конфиденциальность

Обучающийся должен знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить

– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

– алгоритмы выполнения работ в профессиональной и смежных областях

– методы работы в профессиональной и смежных сферах

– структуру плана для решения задач

– порядок оценки результатов решения задач профессиональной деятельности

– номенклатура информационных источников, применяемых в профессиональной деятельности

– приемы структурирования информации

– формат оформления результатов поиска информации, современные средства и устройства информатизации

– порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

– принципы безопасности хранения данных

– методы защиты баз данных от внешних угроз

– принципы криптографии и методов шифрования данных

– стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

– методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных

– законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

Типовые вопросы для устного опроса

1. Психология атак: социальная инженерия.
2. Обучение сотрудников информационной безопасности.

Типовой тест

1. Что такое социальная инженерия?

А) Технический взлом паролей

Б) Использование психологического воздействия для получения информации

В) Социологический опрос

Г) Создание социальных сетей

2. Какой метод социальной инженерии представляет собой звонок якобы от техподдержки?

А) Фишинг

Б) Вишинг (vishing)

В) Смишинг (smishing)

Г) Претекстинг

3. Что такое фишинг?

А) Поддельное письмо от имени известной организации с целью кражи данных

Б) Взлом через USB-устройства

Г) Подбор пароля

Г) Заражение вирусом

4. Какой тип атаки использует USB-накопители, разбросанные на парковке?

А) Baiting (приманка)

Б) Quid pro quo

В) Tailgating

Г) Shoulder surfing

5. Какая мера наиболее эффективна против социальной инженерии?

А) Сложные пароли

Б) Регулярное обучение и повышение осведомлённости сотрудников

В) Двойная аутентификация

Г) Шифрование дисков

6. Что такое pretexting?

А) Подготовка вымышленного сценария для получения информации

Б) Подглядывание за вводом пароля

В) Следование за сотрудником в офис

Г) Сбор мусора

7. Как называется атака, когда злоумышленник проходит за сотрудником через турникет?

А) Piggybacking / Tailgating

Б) Phishing

В) Vishing

Г) Waterholing

8. Что такое shoulder surfing?

А) Сбор информации через открытые источники

Б) Подглядывание за экраном или клавиатурой

В) Звонок от имени руководителя

Г) Подлог документов

9. Какой документ должен регламентировать правила поведения при попытке социальной инженерии?

А) Политика информационной безопасности

Б) Инструкция по охране труда

В) Должностная инструкция

Г) Коллективный договор

10. Какая атака направлена на конкретное лицо с учётом его персональных данных?

А) Спам

Б) Spear phishing (целевой фишинг)

В) Whaling (охота на китов)

Г) Рандомный фишинг

5 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация в форме **дифференцированного зачёта.**

Дифференцированный зачёт по учебной дисциплине проводится в форме устного опроса. После ответов на вопросы обучающийся выполняет практическое задание.

Типовые вопросы для дифференцированного зачёта по учебной дисциплине

Вопросы для оценки усвоенных знаний

1. Основные понятия и определения информационной безопасности. История развития ИБ.
2. Актуальные угрозы и риски в информационной безопасности.
3. Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности.
4. Оценка рисков и управление ими. Соответствие стандартам (ISO 27001, GDPR и др.).
5. Основы криптографии: симметричные и асимметричные алгоритмы.
6. Хэширование и цифровые подписи. Применение криптографии.
7. Стеганография.
8. Основы сетевой безопасности. Защита от атак (DDoS, MITM).
9. Использование VPN и межсетевых экранов.
10. Уязвимости веб-приложений (OWASP Top Ten).
11. Безопасное программирование: лучшие практики.
12. Тестирование на проникновение и анализ уязвимостей.
13. Шифрование данных в покое и в транзите.
14. Резервное копирование и восстановление данных.
15. Управление доступом к данным.
16. Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасность.
17. Реакция на инциденты и управление ими.
18. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента.
19. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика.
20. Психология атак: социальная инженерия.
21. Обучение сотрудников информационной безопасности.
22. Законодательство и стандарты безопасности (GDPR, HIPAA, PCI DSS).
23. Методы аутентификации и авторизации (пароли, сертификаты, биометрия).

Типовые задания для контроля освоенных умений

1. Опишите порядок действий при обнаружении подозрительного письма с вложением (фишинговая атака). Какие шаги должен предпринять сотрудник и специалист по ИБ?

2. Предложите меры защиты для небольшой компании с 50 компьютерами и выходом в Интернет (сетевой экран, антивирус, резервное копирование, обучение). Обоснуйте выбор.

3. Рассчитайте энтропию пароля длиной 8 символов, состоящего только из строчных латинских букв (26 вариантов). Во сколько раз возрастёт стойкость, если добавить цифры?

4. Расшифруйте сообщение, зашифрованное шифром Цезаря со сдвигом 3: «KROF DQG UXOH». (Подсказка: английский алфавит)

5. В организации произошла утечка данных. Какие действия необходимо предпринять для расследования? Перечислите этапы форензического анализа.

6. Классифицируйте следующие угрозы: фишинг, DDoS, кража ноутбука, ошибка администратора, взлом Wi-Fi. Определите для каждой угрозы возможные меры предотвращения.

7. Сравните модели IaaS, PaaS и SaaS с точки зрения распределения ответственности за безопасность (используя модель совместной ответственности).

8. Приведите пример SQL-инъекции на простом запросе SELECT * FROM users WHERE username = 'input'. Покажите, как злоумышленник может обойти аутентификацию. Предложите защиту.

9. Опишите, как с помощью социальной инженерии злоумышленник может получить доступ к серверной. Какие технические и организационные меры предотвратят такую атаку?

10. На основе стандарта ISO 27001 назовите основные разделы системы менеджмента информационной безопасности (СМИБ).

Ключи к тесту

Тема 1.1

1-Б, 2-Б, 3-Б, 4-Б, 5-В, 6-Б, 7-Б, 8-Б, 9-В, 10-Б

Тема 1.2

1-Б, 2-Б, 3-Б, 4-В, 5-Б, 6-В, 7-А, 8-Б, 9-Б, 10-В

Тема 1.3

1-Б, 2-Б, 3-Б, 4-Б, 5-Б, 6-Б, 7-А, 8-Б, 9-Б, 10-А

Тема 1.4

1-Б, 2-Б, 3-Б, 4-А, 5-Б, 6-Б, 7-А, 8-Б, 9-Б, 10-А

Тема 1.5

1-Б, 2-Б, 3-А, 4-Б, 5-А, 6-Б, 7-Б, 8-Б, 9-Б, 10-А

Тема 1.6

1-В, 2-Б, 3-Б, 4-Б, 5-А, 6-Б, 7-А, 8-Б, 9-Б, 10-А

Тема 1.7

1-Г, 2-А, 3-Б, 4-Б, 5-Б, 6-Б, 7-Б, 8-А, 9-Б, 10-А

Тема 1.8

1-Б, 2-Б, 3-А, 4-А, 5-Б, 6-А, 7-А, 8-Б, 9-А, 10-Б

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ на _____ учебный год

№ п.п.	Содержание изменения	Дата, номер протокола заседания ПЦК Подпись председателя ПЦК
		_____ № _____ Председатель ПЦК ЕНД _____/_____