Приложение ППССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2021-2022 уч.г.:
Комплект контрольно-оценочных средств учебной дисциплины
ОП.01 Основы информационной безопасности

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

Комплект контрольно-оценочных средств

по учебной дисциплине

ОП.01 Основы информационной безопасности

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2021

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

Составитель:
Ковалев Н.А., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

В соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) колледж самостоятельно планирует результаты обучения по учебной дисциплине ОП. 01 Основы информационной безопасности, которые соотнесены с требуемыми результатами освоения образовательной программы (компетенциями выпускников). Совокупность запланированных результатов обучения должна обеспечивать выпускнику освоение всех общих компетенций (далее – ОК), профессиональных компетенций (далее – ПК), установленных ФГОС СПО.

Контрольно-оценочные средства (далее - КОС) предназначены для контроля и оценки образовательных достижений обучающихся по учебной дисциплине ОП. 01 Основы информационной безопасности.

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

КОС разработан на основании рабочей программы учебной дисциплины ОП. 01 Основы информационной безопасности.

1.2 Цель и планируемые результаты освоения учебной дисциплины:

Таблица 1

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4	– классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации;	– сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности;

		– основные методики анализа угроз и рисков информационной безопасности;

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

– У1 Классифицировать защищаемую информацию по видам тайны и степеням секретности;

– У2 Классифицировать основные угрозы безопасности информации;

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

– З1 Сущность и понятие информационной безопасности, характеристику ее составляющих;

– З2 Место информационной безопасности в системе национальной безопасности страны;

– З3 Виды, источники и носители защищаемой информации;

– З4 Источники угроз безопасности информации и меры по их предотвращению;

– З5 Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

– З6 Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

– З7 Современные средства и способы обеспечения информационной безопасности;

– З8 Основные методики анализа угроз и рисков информационной безопасности;

Профессиональные и общие компетенции, которые формируются при изучении учебной дисциплины:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие:

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;

ОК 09. Использовать информационные технологии в профессиональной деятельности;

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках;

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

Планируемые личностные результаты освоения рабочей программы учебной дисциплины:

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

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

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

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

1.3. Контроль и оценка результатов освоения учебной дисциплины

Таблица 2

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Знания: – сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.	Контроль выполняется по результатам проведения различных форм опроса, тестирования, выполнения практических работ, промежуточной аттестации.

– современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности.		
Умения: – классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;	Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности	Контроль умений осуществляется в ходе выполнения практических работ, промежуточной аттестации.

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

2.1. Тестовые задания

Раздел 1. Теоретические основы информационной безопасности.

Задание №1. Что из перечисленного является основным принципом информационной безопасности? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Доступность
b) Конфиденциальность
c) Целостность
d) Все вышеперечисленное

Ответ:
_____

Задание №2. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

A. Конфиденциальность	1. Процесс защиты информации от несанкционированного доступа
B. Защита информации	2. Способ передачи данных, обеспечивающий их безопасность
C. Шифрование	3. Состояние информации, при котором доступ к ней ограничен
D. Аутентификация	4. Подтверждение личности пользователя или устройства

Запишите ответ:

A	
B	
C	
D	

Задание №3. В задании установите правильную последовательность. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Укажите правильную последовательность шагов для безопасной передачи информации ограниченного доступа.:

1.Шифровать данные перед передачей.
2.Убедиться в наличии безопасного канала связи.
3.Проверить аутентификацию получателя.
4.Отправить зашифрованные данные.
5.Убедиться в получении данных получателем.

Запишите ответ:

1	
2	
3	
4	
5	

Задание №4. Выполните ситуационное задание. Запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Вы работаете в компании, и к вам обратился сотрудник с просьбой предоставить доступ к базе данных, содержащей личные данные клиентов. Как вы должны поступить? Обоснуйте свой ответ.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №5. Прочитайте вопрос, запишите короткий ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой основной метод хранения информации ограниченного доступа?

Запишите ответ:_____

Задание №6. Сопоставьте понятия с определениями. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Понятие	**Определение**
А. Конфиденциальность	1.Защита информации от несанкционированного доступа
В. Целостность	2.Возможность получения информации авторизованными пользователями
С. Доступность	3.Свойство информации оставаться неизменной во времени

Запишите ответ

А	
В	

C	

Задание №7. Расположите этапы процесса обработки информации в правильной последовательности. Запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Хранение
b) Сбор
c) Передача
d) Обработка
e) Анализ
f) Представление результатов

Ответ:

_____
_____
_____
_____
_____
_____

Задание №8. Какой из следующих вариантов является основной целью информационной безопасности? Выберите один вариант ответа и запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Обеспечение доступности информации
b) Обеспечение конфиденциальности информации
c) Обеспечение целостности информации
d) Все вышеперечисленные варианты

Ответ:

_____

Задание №9. Выберите правильный ответ и обведите кружочком номер правильного ответа. Правильный ответ может быть только один. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из следующих методов является наиболее эффективным для обеспечения конфиденциальности данных при их передаче?

A. Передача данных в открытом виде
B. Использование шифрования
C. Отправка данных по электронной почте без защиты
D. Использование незнакомых каналов связи

Задание №10. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Вы обнаружили, что один из сотрудников вашей компании использует общий пароль для доступа к нескольким системам. Как вы должны поступить? Обоснуйте свой ответ.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание 11. Решите ситуационную задачу. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Ваша компания столкнулась с угрозой информационной безопасности в виде хакерской атаки. Перечислите шаги, которые необходимо предпринять для реагирования на инцидент.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание 12. Дайте развернутый ответ на задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Объясните понятие «жизненный цикл конфиденциальной информации» и перечислите стадии, через которые проходит конфиденциальная информация в процессе ее создания.

Ответ:

_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №13. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Вы обнаружили, что один из сотрудников вашей компании хранит конфиденциальную информацию о клиентах на личном компьютере. Как вы должны поступить? Обоснуйте свой ответ.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №14. Какой метод шифрования используется для симметричного шифрования? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) RSA
b) AES
c) DSA
d) SHA-256

Ответ:

_____

Задание №15. Что из нижеперечисленного не является целью защиты информации? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Обеспечение конфиденциальности
b) Увеличение производительности системы
c) Поддержка целостности данных
d) Обеспечение доступности информации

Ответ:
_____

Задание 16. Выполните практическое задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***
Разработайте схему классификации информации в вашей организации, учитывая три уровня секретности: общедоступная, ограниченная и строго конфиденциальная.

Ответ:
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №17. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

1.Шифрование	А. Процесс проверки подлинности пользователя

2.Аутентификация	B. Процесс, обеспечивающий доступ к ресурсам
3.Авторизация	C. Процесс преобразования данных для их защиты
4.Информационная безопасность	D. Защита информации от несанкционированного доступа

Запишите ответ:

A	
B	
C	
D	

Задание №18. В задании установите правильную последовательность. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Укажите правильную последовательность шагов для безопасной передачи информации ограниченного доступа.:

1.Шифрование данных
2.Передача данных
3.Хранение данных
4.Декодирование данных

Запишите ответ:

1	
2	
3	
4	

Задание №19. Соотнесите угрозы безопасности информации с примерами их реализации. Ответы оформите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Угроза	**Пример**
A.Утечка информации	1.Вирус-шпион, собирающий данные с компьютера
B.Изменение информации	2.Подделка электронных писем
C.Невозможность доступа	3.Фишинговая атака для кражи личных данных
D.Кража информации	4.DDoS-атака, приводящая к перегрузке сервера

E.Подмена информации	5.Взлом сайта и замена содержимого
F.Вредоносное воздействие	6.Отправка конфиденциальных документов по ошибке

Запишите ответ

A	
B	
C	
D	
E	
F	

Задание №20. Расположите шаги процесса устранения последствий кибер-атаки в правильном порядке. Запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Восстановление данных из резервных копий
b) Изолирование зараженной системы
c) Анализ причин и источников атаки
d) Устранение уязвимости
e) Мониторинг системы на предмет повторных атак

Ответ:

_____
_____
_____
_____
_____

Ключи к тестам Раздела №1. Теоретические основы информационной безопасности.

№пп	Ответы
1	d) Все вышеперечисленное
2	A – 3, B – 1, C – 2, D - 4
3	2 - 3 - 1 - 4 - 5
4	В данной ситуации я должен отказать в предоставлении доступа, так как это может нарушить политику конфиденциальности компании и привести к утечке личных данных клиентов. Я должен объяснить сотруднику, что доступ к таким данным предоставляется только в рамках строгих процедур и только тем, кто имеет на это полномочия. Я также могу предложить ему обратиться к своему руководителю

	или в отдел информационной безопасности для получения необходимой информации, если это действительно требуется для выполнения его работы.
5	Шифрование данных на носителях.
6	A – 1, B -3, C -2
7	b -> d -> e -> f -> c -> a
8	d) Все вышеперечисленные варианты
9	B. Использование шифрования
10	Я должен обратиться к сотруднику и объяснить ему, что использование общего пароля для доступа к нескольким системам представляет угрозу информационной безопасности компании. Я также должен предложить ему изменить пароль на уникальный для каждой системы и обучить его правилам безопасного пароля.
11	Идентификация инцидента: определить, какая система или данные были скомпрометированы. Изоляция: изолировать скомпрометированную систему или данные, чтобы предотвратить дальнейший доступ хакеров. Очистка: удалить вредоносное программное обеспечение и восстановить систему или данные. Обновление: обновить программное обеспечение и оборудование, чтобы предотвратить повторную атаку. Проверка: проверить систему или данные на наличие других угроз.
12	Жизненный цикл конфиденциальной информации представляет собой процесс создания, хранения, передачи, использования и уничтожения конфиденциальной информации. Стадии жизненного цикла конфиденциальной информации: Создание информации: создание новой конфиденциальной информации. Хранение информации: хранение конфиденциальной информации в защищенном месте. Передача информации: передача конфиденциальной информации между сотрудниками или подразделениями. Использование информации: использование конфиденциальной информации для выполнения задач. Уничтожение информации: уничтожение конфиденциальной информации, когда она больше не нужна.
13	Я должен обратиться к сотруднику и объяснить ему, что хранение конфиденциальной информации на личном компьютере представляет угрозу безопасности компании. Я также должен предложить ему переместить информацию в защищенное место и обучить его правилам безопасности.
14	b) AES
15	b) Увеличение производительности системы

16	Общедоступная информация: включает информацию, которая может быть доступна широкой аудитории без ограничений, например, рекламные материалы, общие отчеты. Ограниченная информация: содержит данные, которые должны быть доступны только определенным группам людей внутри организации, например, внутренние регламенты, финансовые планы. Строго конфиденциальная информация: включает наиболее важные и чувствительные данные, такие как коммерческая тайна, личные данные сотрудников, стратегические планы развития.
17	1 - C, 2 - A, 3 - B, 4 - D
18	3 - 1 - 2 - 4
19	A-6, F-1, B-5 E-2 C-4 D-3
20	b -> c -> d -> a -> e

Критерии оценивания ответов, полученных в ходе тестирования

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

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

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-5 балл	2 (неудовлетворительно)	0-25%	низкий
6-10 баллов	3 (удовлетворительно)	30-50%	базовый
11-15 баллов	4 (хорошо)	55-75%	повышенный
16-20 баллов	5 (отлично)	80-100%	высокий

Раздел 2. Методология защиты информации.

Задание №1. Какой из следующих стандартов является наиболее распространенным для оценки требований к защите информации? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) ISO/IEC 27001
b) GDPR
c) PCI DSS
d) NIST SP 800-53

Ответ:

_____

Задание №2. Прочитайте вопрос, запишите короткий ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Назовите способ защиты информации ограниченного доступа, не связанный с шифрованием.

Ответ:

_____

Задание №3. Выполните практическое задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Проведите анализ рисков для вымышленной компании «АО Рога и копыта», которая обрабатывает персональные данные клиентов. Определите основные угрозы и предложите меры для их минимизации.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №4. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Вы работаете в команде по управлению информационной безопасностью. Один из ваших коллег предлагает игнорировать некоторые требования к защите информации, утверждая, что они слишком затратны. Как вы должны отреагировать?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №5. Выберите правильный ответ и обведите кружочком номер правильного ответа. Правильный ответ может быть только один. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из приведённых методов является наиболее эффективным для защиты данных в процессе передачи?

A. Антивирусное программное обеспечение
B. Шифрование данных
C. Резервное копирование
D. Ограничение физического доступа

Задание №6. Выберите один ответ и запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из следующих принципов защиты информации подразумевает, что доступ к информации должен быть предоставлен только тем, кто действительно его нуждается?

a) Принцип минимизации
b) Принцип конфиденциальности
c) Принцип целостности
d) Принцип доступности

Ответ:

_____

Задание №7. Сопоставьте виды мер защиты информации с их описаниями. Ответ оформите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Организационные меры	1. Установление правил и процедур для управления информацией.
b) Технические меры	2. Использование технологий для защиты данных.
c) Физические меры	3. Защита физического доступа к информационным системам.
d) Правовые меры	4. Соответствие законодательным требованиям и стандартам.

Запишите ответ

a	
b	
c	
d	

Задание №8. Установите правильную последовательность шагов для внедрения мер защиты информации в организации. Запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

1. Проведение анализа рисков.
2. Внедрение технических и организационных мер.
3. Разработка политики безопасности.
4. Мониторинг и пересмотр мер защиты.
5. Обучение сотрудников.

Ответ:

_____
_____
_____
_____
_____

Задание №9. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из следующих терминов обозначает процесс проверки личности пользователя?

A) Аутентификация
B) Авторизация
C) Шифрование
D) Мониторинг

Ответ:

_____

Задание №10. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из следующих типов мер защиты информации относится к техническим мерам?

a) Политики безопасности
b) Шифрование данных
c) Обучение сотрудников
d) Аудит безопасности

Ответ:

_____

Задание №11. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Какой закон регулирует основные принципы защиты персональных данных в России?

a) Закон о коммерческой тайне
b) Закон о защите прав потребителей
c) Федеральный закон "О персональных данных"
d) Закон о защите информации

Ответ:

_____

Задание №12. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, У1, У2,***

ОК 03, ОК 06, ОК09, ОК 10)
Какой из следующих документов является основным для обеспечения информационной безопасности в организации?

a) Устав организации
b) Политика информационной безопасности
c) Договор аренды
d) План развития бизнеса

Ответ:
_____

Задание №13. Прочитайте текст задания и дайте развёрнутый ответ. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***
Объясните, что такое информационная безопасность и как она регулируется на законодательном уровне.

Ответ:
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №14. Выполните практическое задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***
Разработайте краткую политику информационной безопасности для вымышленной компании «Технопарк», которая будет соответствовать требованиям законодательства.

Ответ:
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №15. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Вы получили жалобу от клиента о том, что его персональные данные были раскрыты без его согласия. Каковы ваши действия?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №16. Упорядочите этапы процесса проектирования системы инженерной защиты объектов информатизации в правильной последовательности. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

1. Проведение анализа угроз и уязвимостей.
2. Установка и настройка систем защиты.
3. Разработка проектной документации.

4. Тестирование и ввод в эксплуатацию.
5. Выбор и закупка оборудования.

Ответ:

_____
_____
_____
_____
_____

Задание №17. Прочитайте текст и выполните задание. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Сопоставьте типы инженерной защиты с их описанием.

А) Системы видеонаблюдения	1) Защита от несанкционированного доступа на физическом уровне
В) Контроль доступа	2) Системы, фиксирующие события и действия на объекте
С) Охранная сигнализация	3) Системы, реагирующие на попытки вторжения

Запишите ответ

А	
В	
С	

Задание №18.Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Ваша компания планирует внедрение новой системы защиты информации. Какие шаги вы предпримете для обеспечения организационно-распорядительной защиты в этом процессе?

Ответ:

_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №19. Прочитайте текст задания и дайте развёрнутый ответ на вопрос. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Опишите основные компоненты системы защиты информации и их роль в обеспечении безопасности данных.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №20. Ознакомьтесь с условием и решите задачу. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Ваша компания сталкивается с увеличением числа кибератак, и руководство решило внедрить новую систему защиты информации. Вам поручено разработать план по обеспечению защиты данных.

Задание: Опишите, какие шаги необходимо предпринять для создания эффективной системы защиты информации. Укажите ключевые аспекты, которые должны быть учтены в процессе разработки плана.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Ключи к тестам Раздела №2. Методология защиты информации.

№ пп	Ответы
1	а) ISO/IEC 27001
2	Контроль доступа
3	Анализ рисков для «АО Рога и копыта»: Основные угрозы: Утечка данных из-за взлома системы. Неправомерный доступ к конфиденциальной информации сотрудниками. Потеря данных из-за технических сбоев. Меры для минимизации: Внедрение многофакторной аутентификации для доступа к системам. Регулярное обучение сотрудников по вопросам безопасности. Резервное копирование данных и создание планов восстановления после сбоев
4	Я должен объяснить коллеге, что игнорирование требований к защите информации может привести к серьезным последствиям, включая утечку данных, штрафы за несоответствие регуляторным требованиям и потерю доверия клиентов. Я предложу провести

	анализ рисков, чтобы продемонстрировать потенциальные угрозы и последствия, а также рассмотреть более эффективные и экономически целесообразные решения для соблюдения требований.
5	Шифрование данных
6	a) Принцип минимизации
7	a) - 1 b) - 2 c) - 3 d) - 4
8	1 - 3 - 5 – 2 - 4
9	A) Аутентификация
10	b) Шифрование данных
11	c) Федеральный закон «О персональных данных»
12	b) Политика информационной безопасности
13	Информационная безопасность — это состояние защищенности информации от несанкционированного доступа, использования, раскрытия, разрушения или изменения. Она включает в себя как технические, так и организационные меры, направленные на защиту информации в различных формах. На законодательном уровне информационная безопасность регулируется различными законами и нормативными актами, такими как Федеральный закон «О персональных данных», который устанавливает требования к обработке и защите персональных данных, а также нормативные акты, касающиеся защиты информации в государственных и коммерческих структурах. Важным аспектом является также соблюдение международных стандартов и норм, таких как ISO/IEC 27001, которые помогают организациям внедрять эффективные системы управления информационной безопасностью.
14	Политика информационной безопасности для "Технопарк": Цель: обеспечение защиты конфиденциальной информации и персональных данных клиентов и сотрудников. Обязанности: назначить ответственных за безопасность информации и проводить регулярные тренинги для сотрудников. Контроль доступа: ограничить доступ к информации на основе принципа минимизации, предоставляя доступ только тем, кто его требует для выполнения своих обязанностей. Обработка данных: все персональные данные должны обрабатываться в соответствии с Федеральным законом «О персональных данных». Мониторинг: регулярно проводить аудит и мониторинг системы безопасности для выявления и устранения уязвимостей.

15	Первым делом, необходимо провести внутреннее расследование для выяснения обстоятельств утечки данных. Следует собрать информацию о том, как и почему произошел инцидент, и кто был причастен. После этого необходимо уведомить клиента о ходе расследования и принять меры для минимизации последствий, включая предложение услуг по мониторингу его персональных данных. Также следует уведомить уполномоченный орган по защите данных, если это предусмотрено законодательством, и разработать меры по предотвращению подобных инцидентов в будущем.
16	3 – 5 – 2 - 4
17	A - 2 B - 1 C - 3
18	Провести анализ текущих процессов и выявить недостатки. Разработать или обновить политику безопасности информации. Определить роли и обязанности сотрудников в рамках новой системы. Подготовить регламенты и инструкции для пользователей. Организовать обучение сотрудников по новым процедурам и технологиям.
19	Основные компоненты системы защиты информации включают: Политики и процедуры безопасности – формируют основу для защиты информации, определяя правила и стандарты для работы с данными. Технические средства защиты – программные и аппаратные решения (антивирусы, фаерволы, системы обнаружения вторжений), которые защищают информацию от угроз. Физическая защита – меры, направленные на защиту оборудования и помещений, где хранятся данные (замки, видеонаблюдение, контроль доступа). Обучение и осведомленность сотрудников – важный элемент, так как большая часть утечек информации происходит из-за человеческого фактора. Обучение помогает снизить риски. Мониторинг и аудит – постоянный контроль за состоянием системы защиты, что позволяет выявлять и устранять уязвимости.
20	Оценка текущего состояния безопасности: Проведите аудит существующей системы безопасности, чтобы выявить уязвимости и недостатки. Оцените риски, связанные с утечкой данных, кибератаками и другими угрозами. Разработка стратегии и политики безопасности:

	Определите цели и задачи системы защиты информации. Разработайте политику безопасности, включая правила доступа, обработки и хранения данных. Определение требований к безопасности: Установите требования к шифрованию данных, аутентификации пользователей и контролю доступа. Определите, какие данные требуют особой защиты (например, персональные данные клиентов). Выбор и внедрение средств защиты: Исследуйте и выберите соответствующие технические средства защиты, такие как антивирусные программы, фаерволы и системы обнаружения вторжений. Обеспечьте физическую безопасность серверов и рабочих станций (замки, видеонаблюдение). Обучение персонала: Проведите обучение сотрудников по вопросам информационной безопасности, включая правила работы с данными и реагирования на инциденты. Объясните важность соблюдения политики безопасности и последствия нарушения. Мониторинг и аудит: Настройте системы мониторинга для отслеживания активности в сети и выявления подозрительных действий. Проводите регулярные аудиты безопасности для оценки эффективности системы защиты и внесения необходимых корректировок. План реагирования на инциденты: Разработайте план реагирования на инциденты, включая процедуры для быстрого реагирования на кибератаки и утечки данных. Назначьте ответственных за реагирование на инциденты и проведите тренировки по реагированию.

Критерии оценивания ответов, полученных в ходе тестирования

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

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

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**

0-5 балл	2 (неудовлетворительно)	0-25%	низкий
6-10 баллов	3 (удовлетворительно)	30-50%	базовый
11-15 баллов	4 (хорошо)	55-75%	повышенный
16-20 баллов	5 (отлично)	80-100%	высокий

2.2. Вопросы для устного опроса.
Раздел 1. Теоретические основы информационной безопасности.

Тема 1.1. Основные понятия и задачи информационной безопасности.

Вопросы:
1. Понятие информации и информационной безопасности. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

2.Информация, сообщения, информационные процессы как объекты информационной безопасности. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

3. Обзор защищаемых объектов и систем. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

4. Понятие «угроза информации». ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

5. Понятие «риска информационной безопасности». ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

6. Примеры преступлений в сфере информации и информационных технологий. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

7. Сущность функционирования системы защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

8. Защита человека от опасной информации и от неинформированности в области информационной безопасности. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Тема 1.2. Основы защиты информации.

Вопросы:

1. Целостность, доступность и конфиденциальность информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

2. Классификация информации по видам тайны и степеням конфиденциальности. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

3. Понятия государственной тайны и конфиденциальной информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

4. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

5. Цели и задачи защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

6. Основные понятия в области защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

7. Элементы процесса менеджмента ИБ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

8. Модель интеграции информационной безопасности в основную деятельность организации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

9. Понятие Политики безопасности. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Тема 1.3. Угрозы безопасности защищаемой информации.

Вопросы:
1. Понятие угрозы безопасности информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

2. Системная классификация угроз безопасности информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

3. Каналы и методы несанкционированного доступа к информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З7, У1, У2,***

ОК 03, ОК 06, ОК09, ПК. 2.4)

4. Применение потоков. Классификация потоков. Реализация потоков. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

5. Уязвимости. Методы оценки уязвимости информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Раздел 2. Методология защиты информации.

Тема 2.1. Методологические подходы к защите информации.

Вопросы:
1. Анализ существующих методик определения требований к защите информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

3. Виды мер и основные принципы защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Тема 2.2. Нормативно правовое регулирование защиты информации.

Вопросы:
1. Организационная структура системы защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

2. Законодательные акты в области защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

3. Российские и международные стандарты, определяющие требования к защите информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

4. Система сертификации РФ в области защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

5. Основные правила и документы системы сертификации РФ в области защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Тема 2.3. Защита информации в автоматизированных (информационных) системах.
Вопросы:
1. Основные механизмы защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

2. Система защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

3. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

4. Программные и программно-аппаратные средства защиты информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

5. Инженерная защита и техническая охрана объектов информатизации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

6. Организационно-распорядительная защита информации. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

7. Работа с кадрами и внутриобъектовый режим. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

8. Принципы построения организационно-распорядительной системы. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Критерии оценивания ответов на вопросы

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

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения учебной дисциплины для организации промежуточной аттестации в форме дифференцированного зачета

3.1. Тестовые задания

ВАРИАНТ 1.

Задание 1. Решите ситуационную задачу. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Ваша компания столкнулась с угрозой информационной безопасности в виде хакерской атаки. Перечислите шаги, которые необходимо предпринять для

реагирования на инцидент.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание 2. Дайте развернутый ответ на задание. Ответ запишите.
(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)
Объясните понятие «жизненный цикл конфиденциальной информации» и перечислите стадии, через которые проходит конфиденциальная информация в процессе ее создания.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №3. Выполните ситуационное задание. Ответ запишите.
(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)
Вы обнаружили, что один из сотрудников вашей компании хранит конфиденциальную информацию о клиентах на личном компьютере. Как вы должны поступить? Обоснуйте свой ответ.

Ответ:

_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №4. Какой метод шифрования используется для симметричного шифрования? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) RSA
b) AES
c) DSA
d) SHA-256

Ответ:

_____

Задание №5. Что из нижеперечисленного не является целью защиты информации? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Обеспечение конфиденциальности
b) Увеличение производительности системы
c) Поддержка целостности данных
d) Обеспечение доступности информации

Ответ:

_____

Задание 6. Выполните практическое задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Разработайте схему классификации информации в вашей организации, учитывая три уровня секретности: общедоступная, ограниченная и строго конфиденциальная.

Ответ:

Задание №7. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Вы работаете специалистом по защите информации в крупной компании. Руководство сообщает вам о необходимости внедрения новых мер по обеспечению конфиденциальности данных клиентов. Какие действия вы предпримете?

Ответ:

Задание №8. Решите задачу. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З6, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Рассчитайте вероятность успешного подбора пароля злоумышленником, если длина пароля составляет 8 символов, и он состоит из цифр и букв латинского алфавита в обоих регистрах. Предположим, что злоумышленник делает 1000

попыток в секунду.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №9. Соотнесите угрозы безопасности информации с примерами их реализации. Ответы оформите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Угроза	**Пример**
A.Утечка информации	1.Вирус-шпион, собирающий данные с компьютера
B.Изменение информации	2.Подделка электронных писем
C.Невозможность доступа	3.Фишинговая атака для кражи личных данных
D.Кража информации	4.DDoS-атака, приводящая к перегрузке сервера
E.Подмена информации	5.Взлом сайта и замена содержимого
F.Вредоносное воздействие	6.Отправка конфиденциальных документов по ошибке

Запишите ответ

A	
B	
C	
D	
E	
F	

Задание №10. Расположите шаги процесса устранения последствий кибер-

атаки в правильном порядке. Запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Восстановление данных из резервных копий
b) Изолирование зараженной системы
c) Анализ причин и источников атаки
d) Устранение уязвимости
e) Мониторинг системы на предмет повторных атак

Ответ:

_____
_____
_____
_____
_____

Задание №11. Какой из следующих стандартов является наиболее распространенным для оценки требований к защите информации? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) ISO/IEC 27001
b) GDPR
c) PCI DSS
d) NIST SP 800-53

Ответ:

_____

Задание №12. Дайте развернутый ответ на вопрос задания. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***
Объясните, что такое методики определения требований к защите информации и какие ключевые аспекты они должны учитывать.
Ответ:

_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____

Задание №13. Выполните практическое задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Проведите анализ рисков для вымышленной компании «АО Рога и копыта», которая обрабатывает персональные данные клиентов. Определите основные угрозы и предложите меры для их минимизации.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №14. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Вы работаете в команде по управлению информационной безопасностью. Один из ваших коллег предлагает игнорировать некоторые требования к защите информации, утверждая, что они слишком затратны. Как вы должны отреагировать?

Ответ:

_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №15. Решите задачу. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Разработайте краткий план по внедрению методики оценки требований к защите информации в вашей организации.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №16. Выберите один ответ и запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из следующих принципов защиты информации подразумевает, что доступ к информации должен быть предоставлен только тем, кто действительно его нуждается?

a) Принцип минимизации
b) Принцип конфиденциальности
c) Принцип целостности
d) Принцип доступности

Ответ:

_____

Задание №17. Сопоставьте виды мер защиты информации с их описаниями. Ответ оформите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Организационные меры	5. Установление правил и процедур для управления информацией.
b) Технические меры	6. Использование технологий для защиты данных.
c) Физические меры	7. Защита физического доступа к информационным системам.
d) Правовые меры	8. Соответствие законодательным требованиям и стандартам.

Запишите ответ

a	
b	
c	
d	

Задание №18. Установите правильную последовательность шагов для внедрения мер защиты информации в организации. Запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

1.Проведение анализа рисков.
2.Внедрение технических и организационных мер.
3.Разработка политики безопасности.
4.Мониторинг и пересмотр мер защиты.
5.Обучение сотрудников.

Ответ:

_____
_____
_____
_____
_____

Задание №19. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из следующих терминов обозначает процесс проверки личности пользователя?

A) Аутентификация
B) Авторизация
C) Шифрование
D) Мониторинг

Ответ:

_____

Задание №20. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, З6, З7, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Какой из следующих типов мер защиты информации относится к техническим мерам?

a) Политики безопасности
b) Шифрование данных
c) Обучение сотрудников
d) Аудит безопасности

Ответ:

_____

ВАРИАНТ 2.

Задание №1. Что из перечисленного является основным принципом информационной безопасности? Выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Доступность
b) Конфиденциальность
c) Целостность
d) Все вышеперечисленное

Ответ:

_____

Задание №2. Прочитайте текст задания и дайте развернутый ответ на поставленный вопрос. Запишите ответ. ***(оцениваемые знания, умения, компетенции: 31, 32, 34, 38, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***
Объясните, что такое конфиденциальность в контексте информационной безопасности и приведите примеры мер, направленных на её обеспечение.

Ответ:

Задание №3. Выполните практическое задание. Запишите ответ. ***(оцениваемые знания, умения, компетенции: 31, 32, 33, 34, 38, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***
Вам необходимо разработать политику безопасности для небольшого офиса, в котором работают 10 сотрудников. Включите в политику меры по обеспечению конфиденциальности, целостности и доступности информации.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №4. Выполните ситуационное задание. Запишите ответ.
(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)
Вы работаете в компании, и к вам обратился сотрудник с просьбой предоставить доступ к базе данных, содержащей личные данные клиентов. Как вы должны поступить? Обоснуйте свой ответ.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №5. Прочитайте условие и решите задачу. Запишите ответ.
(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)
Ваша компания столкнулась с инцидентом утечки данных. Перечислите шаги, которые следует предпринять для реагирования на инцидент.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №6. Сопоставьте понятия с определениями. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Понятие	**Определение**
А. Конфиденциальность	1.Защита информации от несанкционированного доступа
В. Целостность	2.Возможность получения информации авторизованными пользователями
С. Доступность	3.Свойство информации оставаться неизменной во времени

Запишите ответ

A	
B	
C	

Задание №7. Расположите этапы процесса обработки информации в правильной последовательности. Запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Хранение
b) Сбор

c) Передача
d) Обработка
e) Анализ
f) Представление результатов

Ответ:

_____
_____
_____
_____
_____
_____

Задание №8. Какой из следующих вариантов является основной целью информационной безопасности? Выберите один вариант ответа и запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

a) Обеспечение доступности информации
b) Обеспечение конфиденциальности информации
c) Обеспечение целостности информации
d) Все вышеперечисленные варианты

Ответ:

_____

Задание №9. Дайте развернутый ответ на вопрос и запишите ответ. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Объясните понятие "конфиденциальность информации" и приведите примеры того, как можно обеспечить конфиденциальность информации в организации.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №10. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З8, У1, У2, ОК 03, ОК 06, ОК09, ПК. 2.4)***

Вы обнаружили, что один из сотрудников вашей компании использует общий пароль для доступа к нескольким системам. Как вы должны поступить? Обоснуйте свой ответ.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №11. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Какой закон регулирует основные принципы защиты персональных данных в России?

a) Закон о коммерческой тайне
b) Закон о защите прав потребителей
c) Федеральный закон «О персональных данных»
d) Закон о защите информации

Ответ:

_____

Задание №12. Прочитайте задание, выберите и запишите один вариант ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Какой из следующих документов является основным для обеспечения информационной безопасности в организации?

a) Устав организации
b) Политика информационной безопасности
c) Договор аренды
d) План развития бизнеса

Ответ:

_____

Задание №13. Прочитайте текст задания и дайте развёрнутый ответ. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Объясните, что такое информационная безопасность и как она регулируется на законодательном уровне.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №14. Выполните практическое задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З7, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Разработайте краткую политику информационной безопасности для вымышленной компании «Технопарк», которая будет соответствовать требованиям законодательства.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____

Задание №15. Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Вы получили жалобу от клиента о том, что его персональные данные были раскрыты без его согласия. Каковы ваши действия?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №16. Упорядочите этапы процесса проектирования системы инженерной защиты объектов информатизации в правильной последовательности. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

1. Проведение анализа угроз и уязвимостей.
2. Установка и настройка систем защиты.
3. Разработка проектной документации.
4. Тестирование и ввод в эксплуатацию.
5. Выбор и закупка оборудования.

Ответ:

_____
_____
_____
_____

_____

Задание №17. Прочитайте текст и выполните задание. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Сопоставьте типы инженерной защиты с их описанием.

А) Системы видеонаблюдения	1) Защита от несанкционированного доступа на физическом уровне
В) Контроль доступа	2) Системы, фиксирующие события и действия на объекте
С) Охранная сигнализация	3) Системы, реагирующие на попытки вторжения

Запишите ответ

A	
B	
C	

Задание №18.Выполните ситуационное задание. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Ваша компания планирует внедрение новой системы защиты информации. Какие шаги вы предпримете для обеспечения организационно-распорядительной защиты в этом процессе?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____

Задание №19. Прочитайте текст задания и дайте развёрнутый ответ на вопрос. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Опишите основные компоненты системы защиты информации и их роль в обеспечении безопасности данных.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание №20. Ознакомьтесь с условием и решите задачу. Ответ запишите. ***(оцениваемые знания, умения, компетенции: З1, З2, З3, З4, З5, У1, У2, ОК 03, ОК 06, ОК09, ОК 10)***

Ваша компания сталкивается с увеличением числа кибератак, и руководство решило внедрить новую систему защиты информации. Вам поручено разработать план по обеспечению защиты данных.

Задание: Опишите, какие шаги необходимо предпринять для создания эффективной системы защиты информации. Укажите ключевые аспекты, которые должны быть учтены в процессе разработки плана.

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Ключи ответов к заданиям дифференцированного зачета.

Номер задания	Правильный ответ	
	1 вариант	**2 вариант**
1	Идентификация инцидента: определить, какая система или данные были скомпрометированы. Изоляция: изолировать скомпрометированную систему или данные, чтобы предотвратить дальнейший доступ хакеров. Очистка: удалить вредоносное программное обеспечение и восстановить систему или данные. Обновление: обновить программное обеспечение и оборудование, чтобы предотвратить повторную атаку.). Проверка: проверить систему или данные на наличие других угроз.	d) Все вышеперечисленное
2	Жизненный цикл конфиденциальной информации представляет собой процесс создания, хранения, передачи, использования и уничтожения конфиденциальной информации. Стадии жизненного цикла	Конфиденциальность в информационной безопасности означает защиту информации от несанкционированного доступа и раскрытия. Это важный аспект, поскольку утечка конфиденциальной информации может привести к финансовым

	конфиденциальной информации: Создание информации: создание новой конфиденциальной информации. Хранение информации: хранение конфиденциальной информации в защищенном месте. Передача информации: передача конфиденциальной информации между сотрудниками или подразделениями. Использование информации: использование конфиденциальной информации для выполнения задач. . Уничтожение информации: уничтожение конфиденциальной информации, когда она больше не нужна.	потерям, ущербу репутации и юридическим последствиям. Примеры мер, направленных на обеспечение конфиденциальности: Использование шифрования данных для защиты информации при передаче и хранении. Настройка прав доступа к информации, чтобы только авторизованные пользователи могли её видеть. Применение систем аутентификации, таких как пароли, двухфакторная аутентификация и биометрические данные. Обучение сотрудников по вопросам защиты конфиденциальной информации и осведомленности о рисках.
3	Я должен обратиться к сотруднику и объяснить ему, что хранение конфиденциальной информации на личном компьютере представляет угрозу безопасности компании. Я также должен предложить ему переместить информацию в защищенное место и обучить его правилам безопасности.	Политика безопасности офиса: Конфиденциальность: Все сотрудники должны использовать сильные пароли и менять их каждые 90 дней. Доступ к конфиденциальной информации ограничен только теми сотрудниками, которым он необходим для выполнения их работы. Все документы с конфиденциальной информацией должны храниться в закрытом шкафу, а электронные данные — в защищенных системах с шифрованием. Целостность: Регулярные резервные копии всех критически важных данных должны выполняться не

		реже одного раза в неделю. Установить антивирусное программное обеспечение на все рабочие станции и регулярно обновлять его. Внедрить контроль версий для важных документов, чтобы отслеживать изменения и предотвращать случайные потери данных. Доступность: Обеспечить бесперебойное питание для серверов и критически важных систем с помощью ИБП (источников бесперебойного питания). Обучить сотрудников, как обращаться с техникой в случае сбоя системы. Создать план восстановления после сбоев, чтобы минимизировать время простоя.
4	b) AES	В данной ситуации я должен отказать в предоставлении доступа, так как это может нарушить политику конфиденциальности компании и привести к утечке личных данных клиентов. Я должен объяснить сотруднику, что доступ к таким данным предоставляется только в рамках строгих процедур и только тем, кто имеет на это полномочия. Я также могу предложить ему обратиться к своему руководителю или в отдел информационной безопасности для получения необходимой информации, если это действительно требуется для выполнения его работы.
5	b) Увеличение производительности системы	Идентификация инцидента: определить, какие данные были

		скомпрометированы и каким образом произошла утечка. Изоляция: немедленно изолировать затронутые системы, чтобы предотвратить дальнейшие утечки. Оповещение: уведомить руководство и, если необходимо, соответствующие органы о произошедшем инциденте. Анализ: провести детальный анализ инцидента, чтобы понять его причины и последствия. Устранение: принять меры по устранению уязвимостей, которые привели к утечке данных. Восстановление: восстановить системы и данные, если это возможно, и обеспечить
6	Общедоступная информация: включает информацию, которая может быть доступна широкой аудитории без ограничений, например, рекламные материалы, общие отчеты. Ограниченная информация: содержит данные, которые должны быть доступны только определенным группам людей внутри организации, например, внутренние регламенты, финансовые планы. Строго конфиденциальная информация: включает наиболее важные и чувствительные данные, такие как коммерческая тайна, личные данные сотрудников, стратегические планы развития.	A – 1, B -3, C -2

7	План действий: Проведение анализа текущих процессов обработки и хранения данных клиентов. Оценка существующих уязвимостей и потенциальных рисков. Разработка плана по внедрению дополнительных мер защиты, включая шифрование данных, усиление контроля доступа и регулярное обновление программного обеспечения. Организация обучения сотрудников по вопросам информационной безопасности. Мониторинг и аудит выполнения новых процедур.	b -> d -> e -> f -> c -> a
8	Количество возможных символов: 26 (буквы нижнего регистра) + 26 (буквы верхнего регистра) + 10 (цифры) = 62 символа. Количество возможных комбинаций: 62^8= 218,340,105,584,896. Вероятность одной успешной попытки: 1/218,340,105,584,896 Время, необходимое для перебора всех комбинаций: (218,340,105,584,896 / 1000) секунд ≈ 68,417 лет. Таким образом, вероятность успешного подбора пароля крайне мала.	d) Все вышеперечисленные варианты
9	A-6, F-1, B-5 E-2 C-4 D-3	Конфиденциальность информации представляет собой защиту информации от несанкционированного доступа, использования или раскрытия. Обеспечение конфиденциальности информации включает в себя

		реализацию мер по контролю доступа, шифрованию данных и обучению сотрудников. Примеры обеспечения конфиденциальности информации: Контроль доступа: Реализация системы контроля доступа, которая ограничивает доступ к информации только авторизованным сотрудникам. Шифрование данных: Использование шифрования для хранения и передачи данных, что делает их непрочитаемыми для несанкционированных пользователей. Обучение сотрудников: Обучение сотрудников важности конфиденциальности информации и правилам обращения с конфиденциальными данными.
10	b -> c -> d -> a -> e	Я должен обратиться к сотруднику и объяснить ему, что использование общего пароля для доступа к нескольким системам представляет угрозу информационной безопасности компании. Я также должен предложить ему изменить пароль на уникальный для каждой системы и обучить его правилам безопасного пароля.
11	a) ISO/IEC 27001	c) Федеральный закон «О персональных данных»
12	Методики определения требований к защите информации представляют собой систематические подходы к выявлению и	b)Политика информационной безопасности

	анализу потребностей в защите информации в организации. Они должны учитывать следующие ключевые аспекты: Оценка рисков: определение угроз и уязвимостей, которые могут повлиять на конфиденциальность, целостность и доступность информации. Регуляторные требования: учет законов и стандартов, касающихся защиты данных и конфиденциальности. Типы информации: идентификация типов информации, которые требуют защиты, и их классификация по уровням чувствительности. Требования пользователей: учет потребностей и ожиданий пользователей в отношении защиты информации. Технические и организационные меры: определение необходимых мер безопасности для защиты информации на разных уровнях.	
13	Анализ рисков для «АО Рога и копыта»: Основные угрозы: Утечка данных из-за взлома системы. Неправомерный доступ к конфиденциальной информации сотрудниками. Потеря данных из-за технических сбоев. Меры для минимизации: Внедрение многофакторной	Информационная безопасность — это состояние защищенности информации от несанкционированного доступа, использования, раскрытия, разрушения или изменения. Она включает в себя как технические, так и организационные меры, направленные на защиту информации в различных формах. На законодательном

	аутентификации для доступа к системам. Регулярное обучение сотрудников по вопросам безопасности. Резервное копирование данных и создание планов восстановления после сбоев	уровне информационная безопасность регулируется различными законами и нормативными актами, такими как Федеральный закон «О персональных данных», который устанавливает требования к обработке и защите персональных данных, а также нормативные акты, касающиеся защиты информации в государственных и коммерческих структурах. Важным аспектом является также соблюдение международных стандартов и норм, таких как ISO/IEC 27001, которые помогают организациям внедрять эффективные системы управления информационной безопасностью.
14	Я должен объяснить коллеге, что игнорирование требований к защите информации может привести к серьезным последствиям, включая утечку данных, штрафы за несоответствие регуляторным требованиям и потерю доверия клиентов. Я предложу провести анализ рисков, чтобы продемонстрировать потенциальные угрозы и последствия, а также рассмотреть более эффективные и экономически целесообразные решения для соблюдения требований.	Политика информационной безопасности для «Технопарк»: Цель: обеспечение защиты конфиденциальной информации и персональных данных клиентов и сотрудников. Обязанности: назначить ответственных за безопасность информации и проводить регулярные тренинги для сотрудников. Контроль доступа: ограничить доступ к информации на основе принципа минимизации, предоставляя доступ только тем, кто его требует для выполнения своих обязанностей. Обработка данных: все персональные данные должны обрабатываться в соответствии

		с Федеральным законом «О персональных данных».). Мониторинг: регулярно проводить аудит и мониторинг системы безопасности для выявления и устранения уязвимостей.
15	План внедрения методики оценки требований: Формирование рабочей группы: создать команду из специалистов по безопасности, ИТ и правовым вопросам. Оценка текущего состояния: провести аудит существующих процессов и систем безопасности. Идентификация требований: определить требования к защите информации на основе анализа рисков и регуляторных норм. Разработка политики: создать и утвердить политику защиты информации. Обучение сотрудников: провести обучение для всех сотрудников по новым требованиям и процедурам. Мониторинг и пересмотр: установить регулярный мониторинг и пересмотр политики и методик	Первым делом, необходимо провести внутреннее расследование для выяснения обстоятельств утечки данных. Следует собрать информацию о том, как и почему произошел инцидент, и кто был причастен. После этого необходимо уведомить клиента о ходе расследования и принять меры для минимизации последствий, включая предложение услуг по мониторингу его персональных данных. Также следует уведомить уполномоченный орган по защите данных, если это предусмотрено законодательством, и разработать меры по предотвращению подобных инцидентов в будущем.
16	а) Принцип минимизации	3 – 5 – 2 - 4
17	a) - 1 b) - 2 c) - 3 d) - 4	A - 2 B - 1 C - 3
18	1 - 3 - 5 – 2 - 4	Провести анализ текущих процессов и выявить недостатки. Разработать или обновить

		политику безопасности информации. Определить роли и обязанности сотрудников в рамках новой системы. Подготовить регламенты и инструкции для пользователей. Организовать обучение сотрудников по новым процедурам и технологиям.
19	А) Аутентификация	Основные компоненты системы защиты информации включают: Политики и процедуры безопасности – формируют основу для защиты информации, определяя правила и стандарты для работы с данными. Технические средства защиты – программные и аппаратные решения (антивирусы, фаерволы, системы обнаружения вторжений), которые защищают информацию от угроз. Физическая защита – меры, направленные на защиту оборудования и помещений, где хранятся данные (замки, видеонаблюдение, контроль доступа). Обучение и осведомленность сотрудников – важный элемент, так как большая часть утечек информации происходит из-за человеческого фактора. Обучение помогает снизить риски. . Мониторинг и аудит – постоянный контроль за состоянием системы защиты, что позволяет выявлять и устранять уязвимости.

20	b) Шифрование данных	Оценка текущего состояния безопасности: Проведите аудит существующей системы безопасности, чтобы выявить уязвимости и недостатки. Оцените риски, связанные с утечкой данных, кибератаками и другими угрозами. Разработка стратегии и политики безопасности: Определите цели и задачи системы защиты информации. Разработайте политику безопасности, включая правила доступа, обработки и хранения данных. . Определение требований к безопасности: Установите требования к шифрованию данных, аутентификации пользователей и контролю доступа. Определите, какие данные требуют особой защиты (например, персональные данные клиентов). . Выбор и внедрение средств защиты: Исследуйте и выберите соответствующие технические средства защиты, такие как антивирусные программы, фаерволы и системы обнаружения вторжений. Обеспечьте физическую безопасность серверов и рабочих станций (замки, видеонаблюдение). . Обучение персонала: Проведите обучение сотрудников по вопросам информационной безопасности, включая правила работы с

		данными и реагирования на инциденты. Объясните важность соблюдения политики безопасности и последствия нарушения. . Мониторинг и аудит: Настройте системы мониторинга для отслеживания активности в сети и выявления подозрительных действий. Проводите регулярные аудиты безопасности для оценки эффективности системы защиты и внесения необходимых корректировок. . План реагирования на инциденты: Разработайте план реагирования на инциденты, включая процедуры для быстрого реагирования на кибератаки и утечки данных. Назначьте ответственных за реагирование на инциденты и проведите тренировки по реагированию.

Критерии оценивания ответов, полученных в ходе тестирования

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

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

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-5 балл	2 (неудовлетворительно)	0-25%	низкий
6-10 баллов	3 (удовлетворительно)	30-50%	базовый
11-15 баллов	4 (хорошо)	55-75%	повышенный
16-20 баллов	5 (отлично)	80-100%	высокий

4. 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. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. -М.: Академия. 2019-256 с.

Дополнительные источники:

2. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. - М.: Издательство КДУ.

3. Беглов Е.Б., Лось В.П., Метцеряков Р.В., Шелупанов А.А. Основы информа-ционной безопасности: Учебн. пособие для вузов. - М: Горячая линия-ТелеКом, 2006. - 544 с.: ил. Допущено У МО ИБ.

4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. - М.: Инфа-М. 2016.

5. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. - М. : КНОРУС, 2016.

6. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. - М.: МГТУ им. Баумана. 2016.

7. Нестеров С.А. Основы информационной безопасности. Учебное пособие. - С-Пб.: Лань. 2016.

8. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. -М.: Академия. 2015.

9. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - -М.: Академия. 2012.

10. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - С-Пб.: Изд. Питер. 2017.

11. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2012.

Электронные издания (электронные ресурсы)

12.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

13.Казарин, О. В. 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. —https://urait.ru/bcode/456792

14.Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Цифровая образовательная среда СПО РКОГобразование:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО РКОГобразование : [сайт]. — URL: https://profspo.ru/books/97562 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей

2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО РКОГобразование : [сайт]. — URL: https://profspo.ru/books/91640 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей

3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва,Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/89453 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:
IPR BOOKS
https://www.iprbookshop.ru/10746.html
https://www.iprbookshop.ru/43960.html

Веб-система для организации дистанционного обучения и управления им:

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