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

Комплект
контрольно-оценочных средств

учебной дисциплине
ОП 09. Защита информационных процессов в компьютерных системах

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:
Дешина И.А., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. Паспорт 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 09. Защита информационных процессов в компьютерных системах, 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 09. Защита информационных процессов в компьютерных системах.

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 09. Защита информационных процессов в компьютерных системах.

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, ПК 2.5, ПК 2.6.	– определять виды угроз безопасности информации и информационных процессов; – применять методы защиты информации в компьютерных системах и компьютерных сетях; – применять методы криптографической защиты информации; – классифицировать компьютерные вирусы и использовать антивирусные программы; – проектировать технические средства обеспечения безопасности и применять аппаратно-программные средства защиты информации от НСД; – применять правовые нормы защиты информации и информационных процессов; – ориентироваться в нестандартных	– основные угрозы информации в компьютерных системах; – специфику возникновения угроз в открытых сетях; – основные руководящие документы в области защиты информационных процессов в компьютерных системах; – особенности защиты информации на узлах компьютерной сети; – основные категории требований к программной и программно-аппаратной реализации средств защиты информации; – требования к защите автоматизированных систем от НСД.

	условиях и ситуациях, анализировать возникающие проблемы, разрабатывать и осуществлять план действий.	

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

У1. определять виды угроз безопасности информации и информационных процессов;

У2. применять методы защиты информации в компьютерных системах и компьютерных сетях;

У3. применять методы криптографической защиты информации;

У4. классифицировать компьютерные вирусы и использовать антивирусные программы;

У5. проектировать технические средства обеспечения безопасности и применять аппаратно-программные средства защиты информации от НСД;

У6. применять правовые нормы защиты информации и информационных процессов;

У7. ориентироваться в нестандартных условиях и ситуациях, анализировать возникающие проблемы, разрабатывать и осуществлять план действий.

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

З1. основные угрозы информации в компьютерных системах;

З2. специфику возникновения угроз в открытых сетях;

З3. основные руководящие документы в области защиты информационных процессов в компьютерных системах;

З4. особенности защиты информации на узлах компьютерной сети;

З5. основные категории требований к программной и программно-аппаратной реализации средств защиты информации;

З6. требования к защите автоматизированных систем от НСД.

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, применять стандарты антикоррупционного поведения

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

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

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

Планируемые личностные результаты освоения рабочей программы 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: – основные угрозы информации в компьютерных системах; – специфику возникновения угроз в открытых сетях; – основные руководящие документы в области защиты информационных процессов в компьютерных системах; – особенности защиты информации на узлах компьютерной сети; – основные категории требований к программной и программно-аппаратной реализации средств защиты информации; требования к защите автоматизированных систем от НСД.	Демонстрация знаний основных угроз информации в компьютерных системах. Знание основных руководящих документов в области защиты информационных процессов в компьютерных системах	Контроль выполняется по результатам проведения различных форм опроса, выполнения контрольных работ, тестирования, выполнения практических работ, промежуточной аттестации.

Умения: – определять виды угроз безопасности информации и информационных процессов; – применять методы защиты информации в компьютерных системах и компьютерных сетях; – применять методы криптографической защиты информации; – классифицировать компьютерные вирусы и использовать антивирусные программы; – проектировать технические средства обеспечения безопасности и применять аппаратно-программные средства защиты информации от НСД; – применять правовые нормы защиты информации и информационных процессов; – ориентироваться в нестандартных условиях и ситуациях, анализировать возникающие проблемы, разрабатывать и осуществлять план действий.	Умение определять виды угроз безопасности информации и информационных процессов, применять методы защиты информации и применять методы криптографической защиты информации. Демонстрация навыков в умении применять правовые нормы защиты информации и информационных процессов и ориентироваться в нестандартных условиях и ситуациях, анализировать возникающие проблемы, разрабатывать и осуществлять план действий	Контроль умений осуществляется в ходе выполнения практических и лабораторных 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

Тема 1. Анализ потенциальных угроз безопасности информационных процессов в компьютерных системах

Задание № 1. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У4, У5, З2, З5, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.5.)

Сопоставьте тип угрозы с её описанием:

1. Вирус	а. Программа, которая самовоспроизводится и может повредить систему.
2. Фишинг	б. Неправомерный доступ к конфиденциальной информации.
3. DDoS-атака	в. Атака, направленная на перегрузку сервера.
4. Утечка данных	г. Метод обмана пользователей для получения конфиденциальной информации.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 2. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У3, З1, ОК 03, ОК 06, ОК 09, ПК 2.6.)

Сопоставьте тип угрозы безопасности с её описанием:

1. Вредоносное ПО	а. Перехват и изменение данных между двумя взаимодействующими сторонами.
2.Атака типа "Человек посередине"	б. Неавторизованный доступ к данным или системам с целью кражи информации.
3.Социальная инженерия	в. Программное обеспечение, предназначенное для нанесения ущерба системе.
4.Неавторизованный доступ	г. Манипулирование людьми для получения доступа к информации или системам.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 3. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У6, У7, З6, ОК 06, ОК 10, ПК 2.5.)

Какой из следующих методов является наиболее эффективным для защиты от вирусов?

1. Антивирусное программное обеспечение
2. Использование сложных паролей
3. Регулярное обновление ОС
4. Файрвол

Задание № 4. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У6, З5, З6, ОК 09, ОК 10, ПК 2.6.)

Какой из следующих типов атак направлен на получение доступа к учетным записям пользователей?

1. DDoS-атака
2. SQL-инъекция
3. Фишинг
4. Вредоносное ПО

Задание № 5. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У5, З1, З6, ОК 03, ОК 09, ОК 10, ПК 2.6.)

Какой из следующих факторов не является угрозой безопасности?

1. Уязвимости программного обеспечения
2. Человеческий фактор
3. Высокая скорость интернета
4. Неправомерный доступ

Задание № 6. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У2, У6, У7, З1, З2, З6, ОК 03, ПК 2.5., ПК 2.6.)

Какой из следующих методов является примером физической безопасности?

1. Шифрование данных
2. Установка видеонаблюдения
3. Использование антивируса
4. Обучение сотрудников

Задание № 7. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У5, У6, З1, З6, ОК 09, ОК 10, ПК 2.4.)

Какие из следующих действий могут помочь предотвратить утечку данных?

1. Шифрование данных
2. Регулярное обновление программного обеспечения
3. Использование открытых Wi-Fi сетей
4. Обучение сотрудников по вопросам безопасности

Задание № 8. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У4, У7, З3, З4, ОК 03, ОК 06, ОК 10, ПК 2.5.)

Какие из следующих угроз могут быть связаны с использованием облачных технологий?

1. Утечка данных
2. Неправомерный доступ
3. Физическое повреждение серверов
4. Устаревшее программное обеспечение

Задание № 9. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У5, У7, З5, З6, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какие из следующих угроз могут быть связаны с использованием облачных технологий?

1. Утечка данных
2. Неправомерный доступ
3. Физическое повреждение серверов
4. Устаревшее программное обеспечение

Задание № 10. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У4, У7, З1, З2, З3ОК 06, ОК 09, ПК 2.5.)

Какие из следующих угроз могут быть связаны с использованием облачных технологий? (Выберите все подходящие варианты)

1. Утечка данных
2. Неправомерный доступ
3. Физическое повреждение серверов
4. Устаревшее программное обеспечение

Задание № 11. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У3, У4, У7, З1, З2, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Опишите основные меры, которые могут быть предприняты для защиты информации в компьютерных системах от потенциальных угроз

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 12. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У2, У6, У7, З1, З3, З6, ОК 03, ОК 10, ПК 2.4.)

Объясните, как человеческий фактор может влиять на безопасность информационных процессов и какие меры можно предпринять для минимизации рисков.

Ответ:

_____
_____
_____

_____
_____
_____
_____
_____
_____

Задание № 13. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У4, З5, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Процесс преобразования информации в неразборчивый формат с использованием алгоритмов, чтобы защитить её от несанкционированного доступа. Только обладатель соответствующего ключа может расшифровать и получить доступ к исходным данным?

Ответ:

_____
_____

Задание № 14. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У4, У5, У6, З2, З3, , З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Назовите два примера вредоносного ПО?

Ответ:

_____
_____

Задание № 15. Прочитайте ситуационную задачу и опишите, какие шаги вы предпримете для расследования инцидента и предотвращения подобных ситуаций в будущем.
(оцениваемые знания, умения, компетенции: У1, У2, З2, З3, ОК 03, ОК 06, ПК 2.4., ПК 2.5.)

Ваша компания столкнулась с утечкой данных, в результате которой конфиденциальная информация клиентов была доступна третьим лицам
Ответ:

_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____

Ключи ответов

Номер задания	Правильный ответ
1	1-а 2-г 3-в 4-б
2	1-в 2-а 3-г 4-б
3	1
4	3
5	3
6	2
7	1,2,4
8	1,2,3
9	1,2
10	1,3
11	Использование антивирусного программного обеспечения: Регулярное обновление и сканирование системы для обнаружения и удаления вредоносного ПО. Шифрование данных: Защита конфиденциальной информации с помощью шифрования, чтобы сделать её недоступной для несанкционированных пользователей. Регулярные обновления программного обеспечения: Установка обновлений и патчей для устранения уязвимостей в операционных системах и приложениях. Файрволы: Использование программных и аппаратных фаерволов

	для контроля входящего и исходящего трафика. Обучение сотрудников: Проведение регулярных тренингов по вопросам безопасности для повышения осведомленности о потенциальных угрозах и методах их предотвращения. Резервное копирование данных: Регулярное создание резервных копий критически важной информации для защиты от потери данных. Двухфакторная аутентификация: Внедрение дополнительных уровней аутентификации для доступа к системам и данным.
12	Человеческий фактор является одной из основных причин утечек данных и инцидентов безопасности. Ошибки пользователей, такие как использование слабых паролей, открытие подозрительных ссылок или загрузка вредоносных файлов, могут привести к компрометации систем. Для минимизации рисков можно предпринять следующие меры: Обучение и повышение осведомленности: Регулярные тренинги для сотрудников о методах защиты информации и распознавании фишинговых атак. Создание политики безопасности: Разработка и внедрение четких правил и процедур по безопасности, которые должны соблюдаться всеми сотрудниками. Проверка и аудит: Регулярные проверки соблюдения политики безопасности и аудит действий сотрудников для выявления потенциальных рисков. Использование технологий: Внедрение систем мониторинга и управления доступом, которые могут помочь в обнаружении и предотвращении несанкционированного доступа.
13	Шифрование данных
14	Вирус, Троянский конь
15	1. **Немедленное уведомление:** Уведомить руководство и соответствующие команды о произошедшем инциденте. 2. **Ограничение доступа:** Приостановить доступ к затронутым системам и данным, чтобы предотвратить дальнейшую утечку информации. 3. **Расследование инцидента:** Провести детальное расследование для определения источника утечки, включая анализ логов, проверку систем безопасности и опрос сотрудников. 4. **Оценка ущерба:** Оценить объем утечек и потенциальные последствия для клиентов и компании. 5. **Уведомление клиентов:** Уведомить затронутых клиентов о произошедшем инциденте и предоставить рекомендации по защите их данных.

	6. **Внедрение мер безопасности:** На основе результатов расследования разработать и внедрить дополнительные меры безопасности, такие как обновление программного обеспечения, улучшение шифрования данных и обучение сотрудников. 7. **Мониторинг и аудит:** Установить системы мониторинга для раннего обнаружения потенциальных угроз и проводить регулярные аудиты безопасности. 8. **Документация:** Задокументировать инцидент и предпринятые меры для анализа и улучшения процессов безопасности в будущем.

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**
0-4 баллов	2 (неудовлетворительно)	0-26%	низкий
5-9 баллов	3 (удовлетворительно)	33-60%	базовый
10-12 баллов	4 (хорошо)	66-83%	повышенный
13-15 баллов	5 (отлично)	86-100%	высокий

Тема 2. Методы защиты

Задание № 1. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У4, У5, У6, У7, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Сопоставьте тип угрозы с её описанием:

1.Шифрование данных	а. Проверка подлинности пользователя по биометрическим данным.
2.Межсетевой экран (Firewall)	б. Преобразование данных в нечитаемый формат для защиты от несанкционированного доступа.
3.Биометрическая аутентификация	в. Программное или аппаратное средство для контроля сетевого трафика.
4.Резервное копирование	г. Создание копий данных для восстановления в случае утери или повреждения.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 2. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У5, З1, З3, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Сопоставьте тип угрозы безопасности с её описанием:

1. Фишинг	а. Использование антивирусного ПО и регулярное обновление баз данных.
2. DDoS-атака	б. Обучение пользователей и использование двухфакторной аутентификации.
3. Вредоносное ПО	в. Настройка систем обнаружения и предотвращения вторжений (IDS/IPS).
4. SQL-инъекция	г. Валидация входных данных и использование параметризованных запросов.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 3. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У5, У6, З1, З5, З6, ОК 03, ОК 06, ОК 09, ПК 2.6.)

Какой метод защиты используется для предотвращения несанкционированного доступа к данным?

1. Шифрование данных
2. Резервное копирование
3. Дефрагментация диска
4. Обновление программного обеспечения

Задание № 4. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У3, У6, У7, З1, З2, З4, ОК 03, ОК 06, ОК 09, ПК 2.4., ПК 2.6.)

Что такое межсетевой экран (Firewall)?

1. Программа для удаления вирусов
2. Средство контроля сетевого трафика
3. Метод шифрования данных
4. Способ резервного копирования

Задание № 5. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У4, У7, 31, 34, 35, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.5.)

Какой метод защиты помогает восстановить данные после сбоя?

1. Двухфакторная аутентификация
2. Резервное копирование
3. Использование антивируса
4. Шифрование данных

Задание № 6. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У2, У7, 31, 32, ОК 03, ОК 06, ПК 2.4.)

Что такое биометрическая аутентификация?

1. Использование паролей для доступа
2. Проверка подлинности по отпечатку пальца или радужной оболочке глаза
3. Шифрование данных
4. Контроль сетевого трафика

Задание № 7. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.

(оцениваемые знания, умения, компетенции: У1, У5, 33, 36, ОК 03, ОК 09, ОК 10, ПК 2.4.)

Какие методы защиты используются для предотвращения атак на сетевые ресурсы?

1. Использование межсетевого экрана (Firewall)
2. Резервное копирование данных
3. Настройка систем обнаружения вторжений (IDS)
4. Дефрагментация диска

Задание № 8. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.

(оцениваемые знания, умения, компетенции: У1, У7, 35, ОК 06, ОК 10, ПК 2.6.)

Какие методы защиты данных относятся к криптографическим?

1. Шифрование данных
2. Использование антивируса
3. Цифровая подпись
4. Резервное копирование

Задание № 9. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У6, З4, З6, ОК 03, ОК 09, ОК 10, ПК 2.4.)

Какие меры защиты помогают предотвратить утечку данных?

1. Двухфакторная аутентификация
2. Шифрование данных
3. Обновление операционной системы
4. Использование VPN

Задание № 10. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У5, У6, У7, З1, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Какие методы защиты используются для обеспечения доступности данных?

1. Резервное копирование
2. Использование антивируса
3. Настройка отказоустойчивых систем
4. Шифрование данных

Задание № 11. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У7, З1, З4, З6, ОК 03, ОК 09, ОК 10, ПК 2.6.)

Опишите принцип работы межсетевого экрана (Firewall) и его роль в защите компьютерных систем

Ответ:

_____
_____
_____
_____
_____
_____
_____

_____
_____
_____

Задание № 12. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У2, У4, З1, З2, ОК 03, ОК 06, ПК 2.5.)

Какие преимущества предоставляет шифрование данных в контексте информационной безопасности?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 13. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У2, У7, З3, З5, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Назовите два основных типа шифрования

Ответ:

_____
_____

Задание № 14. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1, У6, У7, З3, З4, З5, ОК 03, ОК 06, ОК 10, ПК 2.6.)

Метод аутентификации, при котором пользователь подтверждает свою личность с помощью двух различных факторов (например, пароля и SMS-кода)?

Ответ:

_____
_____

Задание № 15. Прочитайте ситуационную задачу и опишите, какие меры защиты могли бы предотвратить эту ситуацию? Предложите план действий для улучшения безопасности компании.

(оцениваемые знания, умения, компетенции: У1, У4, У5, З1, З2, З3, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

В компании произошла утечка конфиденциальных данных клиентов. Расследование показало, что злоумышленник использовал фишинговую атаку для получения доступа к учетной записи администратора

Ответ:

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

Ключи ответов

Номер задания	Правильный ответ
1	1-а 2-г 3-в 4-б
2	1-в 2-а 3-г 4-б
3	1
4	2
5	2

6	2
7	1,3
8	1,3
9	1,2
10	1,3
11	Межсетевой экран (Firewall) — это программное или аппаратное средство, которое контролирует входящий и исходящий сетевой трафик на основе заданных правил безопасности. Он блокирует несанкционированный доступ к сети, предотвращает атаки и утечку данных, а также фильтрует вредоносный трафик.
12	Шифрование данных обеспечивает конфиденциальность информации, преобразуя её в нечитаемый формат, который может быть расшифрован только с использованием специального ключа. Это защищает данные от несанкционированного доступа, даже если они будут перехвачены злоумышленниками
13	Симметричное и асимметричное шифрование
14	двухфакторная аутентификация
15	1. Внедрить двухфакторную аутентификацию для всех учетных записей. 2. Провести обучение сотрудников по распознаванию фишинговых атак. 3. Установить и настроить межсетевой экран (Firewall) и систему обнаружения вторжений (IDS). 4. Регулярно обновлять программное обеспечение и антивирусные базы. 5. Провести аудит безопасности и тестирование на проникновение

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**
0-4 баллов	2 (неудовлетворительно)	0-26%	низкий

5-9 баллов	3 (удовлетворительно)	33-60%	базовый
10-12 баллов	4 (хорошо)	66-83%	повышенный
13-15 баллов	5 (отлично)	86-100%	высокий

Тема 3. Информационные процессы и системы

Задание № 1. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У3, У4, У7, З1, З3, З6, ОК 03, ОК 06, ПК 2.6.)

Сопоставьте уровень модели ISO/OSI с его описанием:

1. Физический	а. Управляет доступом к среде передачи и исправлением ошибок.
2. Канальный	б. Отвечает за физическую передачу битов по каналу связи.
3. Сетевой	в. Обеспечивает маршрутизацию данных между устройствами в сети.
4. Прикладной	г. Обеспечивает передачу данных между приложениями.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 2. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У5, У6, У7, З5, З6, ОК 03, ОК 06, ОК 10, ПК 2.4.)

Сопоставьте метод криптографической защиты с его описанием:

1.Симметричное шифрование	а. Преобразует данные в уникальную строку фиксированной длины
2.Асимметричное шифрование	б.Обеспечивает аутентификацию и целостность данных.
3. Хэширование	в. Использует один ключ для шифрования и расшифрования.
4. Цифровая подпись	г. Использует пару ключей: открытый и закрытый.

Запишите ответ:

1.	

2.	
3.	
4.	

Задание № 3. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У3, У7, З1, З2, ОК 03, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Какой уровень модели ISO/OSI отвечает за маршрутизацию данных?

1. Физический
2. Канальный
3. Сетевой
4. Транспортный

Задание № 4. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У5, З1, З2, З5, З6, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.5.)

Какой метод криптографии использует один ключ для шифрования и расшифрования?

1. Симметричное шифрование
2. Асимметричное шифрование
3. Хэширование
4. Цифровая подпись

Задание № 5. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У5, У6, З3, З4, З6, ОК 03, ОК 09, ПК 2.4.)

Какой уровень модели ISO/OSI отвечает за физическую передачу битов?

1. Физический
2. Канальный
3. Сетевой
4. Прикладной

Задание № 6. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У2, З3, З6, ОК 03, ОК 06, ОК 09, ПК 2.5.)

Какой метод криптографии обеспечивает аутентификацию и целостность данных?

1. Симметричное шифрование
2. Асимметричное шифрование
3. Хэширование
4. Цифровая подпись

Задание № 7. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У2, У5, У6, З1, З2, З3, З4, З5, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какие уровни модели ISO/OSI относятся к нижним уровням?

1. Физический
2. Сетевой
3. Транспортный
4. Канальный

Задание № 8. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У6, У7, З4, З5, З6, ОК 03, ОК 06, ПК 2.6.)

Какие методы криптографии используют ключи?

1. Симметричное шифрование
2. Хэширование
3. Асимметричное шифрование
4. Цифровая подпись

Задание № 9. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У2, У4, У5, З1, З4, З6, ОК 03, ОК 09, ПК 2.5., ПК 2.6.)

Какие функции выполняет транспортный уровень модели ISO/OSI?

1. Маршрутизация данных
2. Обеспечение надежной передачи данных
3. Управление потоком данных
4. Физическая передача битов

Задание № 10. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У2, У6, У7, З5, З6, ОК 03, ОК 06, ОК 10, ПК 2.4., ПК 2.6.)

Какие методы криптографии обеспечивают конфиденциальность данных?

1. Симметричное шифрование
2. Хэширование
3. Асимметричное шифрование
4. Цифровая подпись

Задание № 11. Прочитайте вопрос, запишите развернутый ответ. ***(оцениваемые знания, умения, компетенции: У1, У5, У7, З3, З5, ОК 03, ОК 09, ОК 10, ПК 2.5., ПК 2.6.)***

Опишите принцип работы асимметричного шифрования и его преимущества

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 12. Прочитайте вопрос, запишите развернутый ответ. ***(оцениваемые знания, умения, компетенции: У1, У5, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)***

Какие задачи решает модель ISO/OSI и как она упрощает проектирование сетей?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 13. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1, У7, З1, З5, З6, ОК 03, ОК 10, ПК 2.4.)

Назовите два основных типа шифрования?

Ответ:

_____
_____

Задание № 14. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1, У5, З4, З5, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4.)

Какой уровень модели ISO/OSI отвечает за передачу данных между приложениями?

Ответ:

_____
_____

Задание № 15. Прочитайте ситуационную задачу и опишите, какие уровни модели будут задействованы и какие методы криптографии следует применить.
(оцениваемые знания, умения, компетенции: У1, У2, У6, У7, З1, З2, З5, З6, ОК 03, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

В компании необходимо обеспечить безопасную передачу конфиденциальных данных между филиалами. Предложите решение, используя знания о модели ISO/OSI и криптографической защите

Ответ:

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

_____
_____

Ключи ответов

Номер задания	Правильный ответ
1	1-г 2-б 3-в 4-а
2	1-в 2-г 3-а 4-б
3	3
4	1
5	1
6	4
7	1,4
8	1,3
9	2,3
10	1,3
11	Асимметричное шифрование использует пару ключей: открытый (для шифрования) и закрытый (для расшифрования). Открытый ключ может быть передан кому угодно, а закрытый хранится в секрете. Преимущества: 1. Безопасный обмен ключами. 2. Возможность создания цифровых подписей. 3. Высокая безопасность за счет сложности взлома.
12	Модель ISO/OSI разделяет процесс передачи данных на 7 уровней, каждый из которых выполняет определенные функции. Это упрощает проектирование, разработку и диагностику сетей, так как позволяет работать с каждым уровнем независимо. Например, можно изменить протокол на одном уровне, не затрагивая другие.
13	Симметричное и асимметричное
14	Прикладной уровень.
15	1. На сетевом уровне использовать VPN для создания

	защищенного канала связи. 2. На транспортном уровне применить протокол TLS для шифрования данных. 3. Использовать асимметричное шифрование для безопасного обмена ключами. 4. На прикладном уровне обеспечить аутентификацию пользователей с помощью цифровых подписей. 5. Регулярно обновлять ключи шифрования и проводить аудит безопасности.

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**
0-4 баллов	2 (неудовлетворительно)	0-26%	низкий
5-9 баллов	3 (удовлетворительно)	33-60%	базовый
10-12 баллов	4 (хорошо)	66-83%	повышенный
13-15 баллов	5 (отлично)	86-100%	высокий

Тема 4. Особенности защиты информации на узлах компьютерной сети

Задание № 1. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, З1, З2, , З6, ОК 03, ОК 10, ПК 2.6.)

Сопоставьте тип угрозы с методом защиты:

1. Несанкционированный доступ	а. Использование межсетевого экрана (Firewall).
2. Утечка данных	б. Шифрование данных.
3. DDoS-атака	в. Настройка систем обнаружения и предотвращения вторжений (IDS/IPS).
4. Вредоносное ПО	г. Установка антивирусного программного обеспечения.

Запишите ответ:

1.	

2.	
3.	
4.	

Задание № 2. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У6, У7, З5, З6, ОК 03, ОК 06, ОК 09, ПК 2.4., ПК 2.5.)

Сопоставьте узел сети с возможной угрозой:

1. Сервер	а. Перехват данных при передаче.
2. Рабочая станция	б. Несанкционированный доступ к данным.
3.Сетевой маршрутизатор	в. Атака на доступность (DDoS).
4. Канал связи	г. Заражение вредоносным ПО.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 3. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У6, У7, З1, З5, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какой метод защиты используется для предотвращения DDoS-атак?

1. Шифрование данных
2. Настройка межсетевого экрана (Firewall)
3. Использование систем обнаружения вторжений (IDS)
4. Установка антивируса

Задание № 4. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У2, У6, У7, З3, З6, ОК 03, ОК 06, ПК 2.6.)

Какой узел сети наиболее уязвим к атакам на доступность?

1. Сервер
2. Рабочая станция
3. Сетевой маршрутизатор
4. Канал связи

Задание № 5. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У2, З5, З6, ОК 03, ПК 2.5., ПК 2.6.)

Какой метод защиты предотвращает утечку данных?

1. Шифрование данных
2. Настройка Firewall
3. Установка антивируса
4. Резервное копирование

Задание № 6. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У2, У5, У6, У7, З1, З4, ОК 03, ОК 06, ПК 2.5.)

Какой узел сети чаще всего подвергается заражению вредоносным ПО?

1. Сервер
2. Рабочая станция
3. Сетевой маршрутизатор
4. Канал связи

Задание № 7. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У2, У5, З2, З5, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какие методы защиты используются для обеспечения безопасности серверов?

1. Настройка межсетевого экрана (Firewall)
2. Шифрование данных
3. Установка антивируса
4. Резервное копирование

Задание № 8. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У3, З1, З2, З3, ОК 06, ОК 09, ПК 2.4.)

Какие угрозы могут возникнуть на канале связи?

1. Перехват данных
2. Несанкционированный доступ
3. Заражение вредоносным ПО
4. Искажение данных

Задание № 9. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У5, У6, У7, З1, З4, З5, ОК 03, ОК 06, ПК 2.6.)

Какие меры защиты применяются для рабочих станций?

1. Установка антивируса
2. Настройка Firewall
3. Шифрование данных
4. Резервное копирование

Задание № 10. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У7, З4, З6, ОК 03, ОК 06, ОК 09, ПК 2.5.)

Какие методы защиты помогают предотвратить атаки на сетевые узлы?

1. Использование IDS/IPS
2. Шифрование данных
3. Настройка VPN
4. Резервное копирование

Задание № 11. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У7, З5, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Опишите основные меры защиты информации на серверах в компьютерной сети

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 12. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У4, У6, З5, З6, ОК 03, ОК 06, ПК 2.6.)

Какие особенности защиты информации необходимо учитывать на рабочих станциях?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 13. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1, У4, У5, З5, З6, ОК 03, ОК 09, ОК 10, ПК 2.6.)

Назовите два основных метода защиты данных на каналах связи.

Ответ:

_____
_____

Задание № 14. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1, У5, У6, З5, З6, ОК 03, ОК 06, ОК 09, ПК 2.4., ПК 2.5.)

Какой метод защиты предотвращает несанкционированный доступ к сетевым узлам?

Ответ:

_____
_____

Задание № 15. Прочитайте ситуационную задачу и опишите, какие меры защиты могли бы предотвратить эту ситуацию? Предложите план действий для улучшения безопасности сети.
(оцениваемые знания, умения, компетенции: У2, У3, У6, У7, З1, З2, З4, З5, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

В компании произошла утечка конфиденциальных данных с сервера. Расследование показало, что злоумышленник использовал уязвимость в сетевом экране для получения доступа

Ответ:

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

Ключи ответов

Номер задания	Правильный ответ
1	1-а 2-б 3-в 4-г
2	1-б 2-г 3-в 4-а
3	3
4	3
5	1
6	2
7	1,2
8	1,4
9	1,2

10	1,3
11	Для защиты информации на серверах применяются следующие меры: 1. Настройка межсетевого экрана (Firewall) для фильтрации входящего и исходящего трафика. 2. Использование систем обнаружения и предотвращения вторжений (IDS/IPS). 3. Шифрование данных для защиты от утечек. 4. Регулярное обновление программного обеспечения и установка патчей. 5. Ограничение доступа к серверу с помощью аутентификации и авторизации.
12	На рабочих станциях важно: 1. Установить антивирусное ПО и регулярно обновлять его базы. 2. Настроить межсетевой экран для блокировки несанкционированного доступа. 3. Ограничить права пользователей для предотвращения случайного или умышленного вреда. 4. Регулярно проводить обучение сотрудников по вопросам кибербезопасности. 5. Использовать шифрование данных при передаче конфиденциальной информации.
13	Шифрование данных и использование VPN
14	Настройка межсетевого экрана (Firewall).
15	1. Установить и настроить систему обнаружения и предотвращения вторжений (IDS/IPS). 2. Регулярно обновлять межсетевой экран и программное обеспечение сервера. 3. Внедрить двухфакторную аутентификацию для доступа к серверу. 4. Использовать шифрование данных на сервере и при передаче. 5. Провести аудит безопасности и тестирование на проникновение.

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**
0-4 баллов	2 (неудовлетворительно)	0-26%	низкий
5-9 баллов	3 (удовлетворительно)	33-60%	базовый
10-12 баллов	4 (хорошо)	66-83%	повышенный
13-15 баллов	5 (отлично)	86-100%	высокий

2.2. Вопросы для устного опроса.

Тема 1. Анализ потенциальных угроз безопасности информационных процессов в компьютерных системах

Вопросы:

1. Источники угроз. Случайные и преднамеренные угрозы ***(оцениваемые знания, умения, компетенции: У1, З3, З4, З5, ОК 09, ОК 10, ПК 2.4.)***
2. Анализ и защита от утечки компьютерной информации по каналам ПЭМИН ***(оцениваемые знания, умения, компетенции: У4, З3, ОК 06, ОК 10, ПК 2.5.)***
3. Основные принципы формирования режима обеспечения безопасности ***(оцениваемые знания, умения, компетенции: У1, У5, З4, З6, ОК 03, ОК 06, ОК 09, ПК 2.6.)***
4. Анализ спектра протоколов обмена ***(оцениваемые знания, умения, компетенции: У1, З4, ОК 03, ОК 06, ОК 09, ПК 2.5.)***

Тема 2. Методы защиты

Вопросы:

1. Организационные методы защиты информационных процессов в компьютерных системах. ***(оцениваемые знания, умения, компетенции: У1, У4, У5, У7, З6, ОК 10, ПК 2.4.)***
2. Инженерно-технические методы защиты информационных процессов ***(оцениваемые знания, умения, компетенции: У2, У6, З5, З6, ОК 03, ОК 10, ПК 2.5.)***
3. Программно-аппаратные методы защиты информационных процессов. ***(оцениваемые знания, умения, компетенции: У1, У6, У7, З5, З6, ОК 03, ОК 06, ОК 09, ПК 2.6.)***
4. Защита электронных документов. ***(оцениваемые знания, умения, компетенции: У2, З6, ОК 03, ОК 10, ПК 2.4.)***
5. Концепция построения систем разграничения доступа. ***(оцениваемые знания, умения, компетенции: У1, У6, З3, З6, ОК 03, ОК 09, ПК 2.6.)***
6. Защита документа при его обработке, хранении и исполнении. ***(оцениваемые знания, умения, компетенции: У2, У5, З2, З6, ОК 06, ОК 09, ПК 2.5., ПК 2.6.)***

Тема 3. Информационные процессы и системы

Вопросы:

1. Модель ISO/OSI ***(оцениваемые знания, умения, компетенции: У3, У7, З6, ОК 09, ОК 10, ПК 2.6.)***
2. Открытый ключ. Система электронной подписи ***(оцениваемые знания, умения, компетенции: У1, У5, З1, З3, ОК 06, ОК 09, ОК 10, ПК 2.5.)***
3. Криптографическая защита ***(оцениваемые знания, умения, компетенции: У4, У7, З3, З6, ОК 09, ОК 10, ПК 2.6.)***
4. Алгоритм выработки уникальных секретных ключей ***(оцениваемые знания, умения, компетенции: У1, З2, З4, З6, ОК 03, ОК 10, ПК 2.4.)***

Тема 4. Особенности защиты информации на узлах компьютерной сети

Вопросы:

1. Администрирование серверных систем и приложений ***(оцениваемые знания, умения, компетенции: У5, У7, З2, З6, ОК 10, ПК 2.4., ПК 2.6.)***
2. Резервное копирование. Журнализация изменений. Мультиплексирование и архивирование ***(оцениваемые знания, умения, компетенции: У3, З5, З6, ОК 03, ОК 10, ПК 2.6.)***
3. Настройка и администрирование сервера. ***(оцениваемые знания, умения, компетенции: У1, У7, З4, ОК 06, ОК 09, ОК 10, ПК 2.4.)***
4. Обеспечение информационной безопасности СУБД. ***(оцениваемые знания, умения, компетенции: У6, У7, З6, ОК 03, ПК 2.5., ПК 2.6.)***

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. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У4, У5, У6, У7, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Сопоставьте тип угрозы с её описанием:

1.Шифрование данных	а. Проверка подлинности пользователя по биометрическим данным.
2.Межсетевой экран (Firewall)	б. Преобразование данных в нечитаемый формат для защиты от несанкционированного доступа.
3.Биометрическая аутентификация	в. Программное или аппаратное средство для контроля сетевого трафика.
4.Резервное копирование	г. Создание копий данных для восстановления в случае утери или повреждения.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 2. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У5, З1, З3, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Сопоставьте тип угрозы безопасности с её описанием:

1. Фишинг	а. Использование антивирусного ПО и регулярное обновление баз данных.
2. DDoS-атака	б. Обучение пользователей и использование двухфакторной аутентификации.
3. Вредоносное ПО	в. Настройка систем обнаружения и предотвращения вторжений (IDS/IPS).
4. SQL-инъекция	г. Валидация входных данных и использование параметризованных запросов.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 3. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У5, У6, З1, З5, З6, ОК 03, ОК 06, ОК 09, ПК 2.6.)

Какой метод защиты используется для предотвращения несанкционированного доступа к данным?

1. Шифрование данных
2. Резервное копирование
3. Дефрагментация диска
4. Обновление программного обеспечения

Задание № 4. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У3, У6, У7, З1, З2, З4, ОК 03, ОК 06, ОК 09, ПК 2.4., ПК 2.6.)

Что такое межсетевой экран (Firewall)?

1. Программа для удаления вирусов
2. Средство контроля сетевого трафика
3. Метод шифрования данных
4. Способ резервного копирования

Задание № 5. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У4, У7, З1, З4, З5, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.5.)

Какой метод защиты помогает восстановить данные после сбоя?

1. Двухфакторная аутентификация
2. Резервное копирование
3. Использование антивируса
4. Шифрование данных

Задание № 6. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У2, У7, З1, З2, ОК 03, ОК 06, ПК 2.4.)

Что такое биометрическая аутентификация?

1. Использование паролей для доступа
2. Проверка подлинности по отпечатку пальца или радужной оболочке глаза
3. Шифрование данных
4. Контроль сетевого трафика

Задание № 7. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У5, З3, З6, ОК 03, ОК 09, ОК 10, ПК 2.4.)

Какие методы защиты используются для предотвращения атак на сетевые ресурсы?

1. Использование межсетевого экрана (Firewall)
2. Резервное копирование данных
3. Настройка систем обнаружения вторжений (IDS)
4. Дефрагментация диска

Задание № 8. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У7, З5, ОК 06, ОК 10, ПК 2.6.)

Какие методы защиты данных относятся к криптографическим?

1. Шифрование данных
2. Использование антивируса
3. Цифровая подпись
4. Резервное копирование

Задание № 9. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У6, З4, З6, ОК 03, ОК 09, ОК 10, ПК 2.4.)

Какие меры защиты помогают предотвратить утечку данных?

1. Двухфакторная аутентификация
2. Шифрование данных
3. Обновление операционной системы
4. Использование VPN

Задание № 10. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У5, У6, У7, З1, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Какие методы защиты используются для обеспечения доступности данных?

1. Резервное копирование
2. Использование антивируса
3. Настройка отказоустойчивых систем
4. Шифрование данных

Задание № 11. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У7, З1, З4, З6, ОК 03, ОК 09, ОК 10, ПК 2.6.)

Опишите принцип работы межсетевого экрана (Firewall) и его роль в защите компьютерных систем

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 12. Прочитайте вопрос, запишите развернутый ответ.

(оцениваемые знания, умения, компетенции: У1, У2, У4, З1, З2, ОК 03, ОК 06, ПК 2.5.)

Какие преимущества предоставляет шифрование данных в контексте информационной безопасности?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 13. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У2, У7, З3, З5, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Назовите два основных типа шифрования

Ответ:

_____
_____

Задание № 14. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1,, У6, У7, З3, З4, З5, ОК 03, ОК 06, ОК 10, ПК 2.6.)

Метод аутентификации, при котором пользователь подтверждает свою личность с помощью двух различных факторов (например, пароля и SMS-кода)?

Ответ:

_____
_____

Задание № 15. Прочитайте ситуационную задачу и опишите, какие меры защиты могли бы предотвратить эту ситуацию? Предложите план действий для улучшения безопасности компании.
(оцениваемые знания, умения, компетенции: У1, У4, У5, З1, З2, З3, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

В компании произошла утечка конфиденциальных данных клиентов. Расследование показало, что злоумышленник использовал фишинговую атаку для получения доступа к учетной записи администратора

Ответ:

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

Задание № 16. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У3, У4, У7, З1, З3, З6, ОК 03, ОК 06, ПК 2.6.)

Сопоставьте уровень модели ISO/OSI с его описанием:

1. Физический	а. Управляет доступом к среде передачи и исправлением ошибок.
2. Канальный	б. Отвечает за физическую передачу битов по каналу связи.
3. Сетевой	в. Обеспечивает маршрутизацию данных между устройствами в сети.
4. Прикладной	г. Обеспечивает передачу данных между приложениями.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 17. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, У5, У6, У7, З5, З6, ОК 03, ОК 06, ОК 10, ПК 2.4.)

Сопоставьте метод криптографической защиты с его описанием:

1.Симметричное шифрование	а. Преобразует данные в уникальную строку фиксированной длины
2.Асимметричное шифрование	б.Обеспечивает аутентификацию и целостность данных.
3. Хэширование	в. Использует один ключ для шифрования и расшифрования.
4. Цифровая подпись	г. Использует пару ключей: открытый и закрытый.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 18. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У3, У7, З1, З2, ОК 03, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

Какой уровень модели ISO/OSI отвечает за маршрутизацию данных?

1. Физический
2. Канальный
3. Сетевой
4. Транспортный

Задание № 19. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У5, З1, З2, З5, З6, ОК 06, ОК 09, ОК 10, ПК 2.4., ПК 2.5.)

Какой метод криптографии использует один ключ для шифрования и расшифрования?

1. Симметричное шифрование
2. Асимметричное шифрование
3. Хэширование
4. Цифровая подпись

Задание № 20. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У5, У6, З3, З4, З6, ОК 03, ОК 09, ПК 2.4.)

Какой уровень модели ISO/OSI отвечает за физическую передачу битов?

1. Физический
2. Канальный
3. Сетевой
4. Прикладной

ВАРИАНТ 2

Задание № 1. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У1, У2, З3, З6, ОК 03, ОК 06, ОК 09, ПК 2.5.)

Какой метод криптографии обеспечивает аутентификацию и целостность данных?

1. Симметричное шифрование
2. Асимметричное шифрование
3. Хэширование
4. Цифровая подпись

Задание № 2. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У2, У5, У6, З1, З2, З3, З4, З5, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какие уровни модели ISO/OSI относятся к нижним уровням?

1. Физический
2. Сетевой
3. Транспортный
4. Канальный

Задание № 3. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У6, У7, З4, З5, З6, ОК 03, ОК 06, ПК 2.6.)

Какие методы криптографии используют ключи?

1. Симметричное шифрование
2. Хэширование
3. Асимметричное шифрование

4. Цифровая подпись

Задание № 4. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У2, У4, У5, З1, З4, З6, ОК 03, ОК 09, ПК 2.5., ПК 2.6.)

Какие функции выполняет транспортный уровень модели ISO/OSI?

1. Маршрутизация данных
2. Обеспечение надежной передачи данных
3. Управление потоком данных
4. Физическая передача битов

Задание № 5. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У2, У6, У7, З5, З6, ОК 03, ОК 06, ОК 10, ПК 2.4., ПК 2.6.)

Какие методы криптографии обеспечивают конфиденциальность данных?

1. Симметричное шифрование
2. Хэширование
3. Асимметричное шифрование
4. Цифровая подпись

Задание № 6. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У5, У7, З3, З5, ОК 03, ОК 09, ОК 10, ПК 2.5., ПК 2.6.)

Опишите принцип работы асимметричного шифрования и его преимущества

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 7. Прочитайте вопрос, запишите развернутый ответ.
(оцениваемые знания, умения, компетенции: У1, У5, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какие задачи решает модель ISO/OSI и как она упрощает проектирование сетей?

Ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 8. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1, У7, З1, З5, З6, ОК 03, ОК 10, ПК 2.4.)

Назовите два основных типа шифрования?

Ответ:

_____
_____

Задание № 9. Прочитайте вопрос, запишите короткий ответ.
(оцениваемые знания, умения, компетенции: У1, У5, З4, З5, З6, ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4.)

Какой уровень модели ISO/OSI отвечает за передачу данных между приложениями?

Ответ:

_____
_____

Задание № 10. Прочитайте ситуационную задачу и опишите, какие уровни модели будут задействованы и какие методы криптографии следует применить.
(оцениваемые знания, умения, компетенции: У1, У2, У6, У7, З1, З2, З5, З6, ОК 03, ОК 09, ОК 10, ПК 2.4., ПК 2.6.)

В компании необходимо обеспечить безопасную передачу конфиденциальных данных между филиалами. Предложите решение, используя знания о модели ISO/OSI и криптографической защите

Ответ:

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

Задание № 11. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У1, З1, З2, З6, ОК 03, ОК 10, ПК 2.6.)

Сопоставьте тип угрозы с методом защиты:

1. Несанкционированный доступ	а. Использование межсетевого экрана (Firewall).
2. Утечка данных	б. Шифрование данных.
3. DDoS-атака	в. Настройка систем обнаружения и предотвращения вторжений (IDS/IPS).
4. Вредоносное ПО	г. Установка антивирусного программного обеспечения.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 12. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.

(оцениваемые знания, умения, компетенции: У1, У6, У7, З5, З6, ОК 03, ОК 06, ОК 09, ПК 2.4., ПК 2.5.)

Сопоставьте узел сети с возможной угрозой:

1. Сервер	а. Перехват данных при передаче.
2. Рабочая станция	б. Несанкционированный доступ к данным.
3.Сетевой маршрутизатор	в. Атака на доступность (DDoS).
4. Канал связи	г. Заражение вредоносным ПО.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 13. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У6, У7, З1, З5, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какой метод защиты используется для предотвращения DDoS-атак?

1. Шифрование данных
2. Настройка межсетевого экрана (Firewall)
3. Использование систем обнаружения вторжений (IDS)
4. Установка антивируса

Задание № 14. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У2, У6, У7, З3, З6, ОК 03, ОК 06, ПК 2.6.)

Какой узел сети наиболее уязвим к атакам на доступность?

1. Сервер
2. Рабочая станция
3. Сетевой маршрутизатор
4. Канал связи

Задание № 15. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.

(оцениваемые знания, умения, компетенции: У1, У2, З5, З6, ОК 03, ПК 2.5., ПК 2.6.)

Какой метод защиты предотвращает утечку данных?

1. Шифрование данных
2. Настройка Firewall
3. Установка антивируса
4. Резервное копирование

Задание № 16. Прочитайте вопрос, выберите один правильный ответ. Обведите кружочком номер правильного ответа.
(оцениваемые знания, умения, компетенции: У2, У5, У6, У7, З1, З4, ОК 03, ОК 06, ПК 2.5.)

Какой узел сети чаще всего подвергается заражению вредоносным ПО?

1. Сервер
2. Рабочая станция
3. Сетевой маршрутизатор
4. Канал связи

Задание № 17. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У2, У5, З2, З5, ОК 06, ОК 09, ОК 10, ПК 2.6.)

Какие методы защиты используются для обеспечения безопасности серверов?

1. Настройка межсетевого экрана (Firewall)
2. Шифрование данных
3. Установка антивируса
4. Резервное копирование

Задание № 18. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У1, У3, З1, З2, З3, ОК 06, ОК 09, ПК 2.4.)

Какие угрозы могут возникнуть на канале связи?

1. Перехват данных
2. Несанкционированный доступ
3. Заражение вредоносным ПО
4. Искажение данных

Задание № 19. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У5, У6, У7, З1, З4, З5, ОК 03, ОК 06, ПК 2.6.)

Какие меры защиты применяются для рабочих станций?

1. Установка антивируса
2. Настройка Firewall
3. Шифрование данных
4. Резервное копирование

Задание № 20. Прочитайте вопрос, выберите несколько правильных ответов. Обведите кружочками номера правильных ответов.
(оцениваемые знания, умения, компетенции: У7, З4, З6, ОК 03, ОК 06, ОК 09, ПК 2.5.)

Какие методы защиты помогают предотвратить атаки на сетевые узлы?

1. Использование IDS/IPS
2. Шифрование данных
3. Настройка VPN
4. Резервное копирование

Ключи ответов

ВАРИАНТ 1	
Номер задания	Правильный ответ
1	1-а 2-г 3-в 4-б
2	1-в 2-а 3-г 4-б
3	1
4	2
5	2
6	2
7	1,3
8	1,3
9	1,2
10	1,3

11	Межсетевой экран (Firewall) — это программное или аппаратное средство, которое контролирует входящий и исходящий сетевой трафик на основе заданных правил безопасности. Он блокирует несанкционированный доступ к сети, предотвращает атаки и утечку данных, а также фильтрует вредоносный трафик.
12	Шифрование данных обеспечивает конфиденциальность информации, преобразуя её в нечитаемый формат, который может быть расшифрован только с использованием специального ключа. Это защищает данные от несанкционированного доступа, даже если они будут перехвачены злоумышленниками
13	Симметричное и асимметричное шифрование
14	двухфакторная аутентификация
15	1. Внедрить двухфакторную аутентификацию для всех учетных записей. 2. Провести обучение сотрудников по распознаванию фишинговых атак. 3. Установить и настроить межсетевой экран (Firewall) и систему обнаружения вторжений (IDS). 4. Регулярно обновлять программное обеспечение и антивирусные базы. 5. Провести аудит безопасности и тестирование на проникновение
16	1-г 2-б 3-в 4-а
17	1-в 2-г 3-а 4-б
18	3
19	1
20	1
ВАРИАНТ 2	
Номер задания	Правильный ответ
1	4
2	1,4
3	1,3

4	2,3
5	1,3
6	Асимметричное шифрование использует пару ключей: открытый (для шифрования) и закрытый (для расшифрования). Открытый ключ может быть передан кому угодно, а закрытый хранится в секрете. Преимущества: 1. Безопасный обмен ключами. 2. Возможность создания цифровых подписей. 3. Высокая безопасность за счет сложности взлома.
7	Модель ISO/OSI разделяет процесс передачи данных на 7 уровней, каждый из которых выполняет определенные функции. Это упрощает проектирование, разработку и диагностику сетей, так как позволяет работать с каждым уровнем независимо. Например, можно изменить протокол на одном уровне, не затрагивая другие.
8	Симметричное и асимметричное
9	Прикладной уровень.
10	1. На сетевом уровне использовать VPN для создания защищенного канала связи. 2. На транспортном уровне применить протокол TLS для шифрования данных. 3. Использовать асимметричное шифрование для безопасного обмена ключами. 4. На прикладном уровне обеспечить аутентификацию пользователей с помощью цифровых подписей. 5. Регулярно обновлять ключи шифрования и проводить аудит безопасности.
11	1-а 2-б 3-в 4-г
12	1-б 2-г 3-в 4-а
13	3
14	3
15	1
16	2
17	1,2

18	1,4
19	1,2
20	1,3

Критерии оценивания ответов, полученных в ходе тестирования

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

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

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-5 баллов	2 (неудовлетворительно)	0-25%	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. Шаньгин ВО. Информационная безопасность компьютерных систем и сетей: учеб.пособие / ВО. Шаньгин. - Москва : ИД «ФОРУМ» : ТОРАм, 2020.- 416 с.

Дополнительные источники:

2. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
3. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
4. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. — 224 с.
5. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
6. Кулаков ВГ., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие. - М.: Радио и связь, 2008

7. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей — готовые решения, 4-е изд. — М.: Вильямс, 2004. — 656 с.
8. Малюк А.А., Пазизин СВ., Погожин НС. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
9. Мельников Д. Информационная безопасность открытых систем.-М.: Форум, 2013.
10. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. — М.: Академия, 2006. — 240 с.
1 1 Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008.-368 с.
12. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д.А.—М.: Интернет-Университет Информационных Технологий (ШПУИТ), 2016.

Электронные издания (электронные ресурсы)

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Российский биометрический портал www.biometrics.ru
4. Сайт журнала Информационная безопасность http://www.itsec.ru —
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Справочно-правовая система «Консультант Плюс» www.consultant.ru 9. Федеральная служба по техническому и экспортному контролю
7. (ФСТЭК России) www.fstec.ru

Цифровая образовательная среда СПО РВОобразование:

1. Ложников, П. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / П. С. Ложников, Е. М. Михайлов. — 3-е изд. — Москва : Интернет-Университет Информационных технологий (ИНТУИТ), Ай пи Ар Медиа, 2020. — 263 с. — ISBN 978-5-44970666-9. Текст электронный // Электронный ресурс цифровой образовательной среды СПО PROF06pa30BaHI,re [сайт]. — https://profspo.ru/books/97553 (дата обращения: 12.11.2020). — Режим доступа: для авторизир. Пользователей
2. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д. В. Фомин. Саратов : Вузовское образование, 2018. 125 с. ISBN 978-5-4487-0299-0. Текст :электронный // Электронный ресурс цифровой образовательной среды СПО Образование [сайт]. — URL: https://profspo.ru/books/77318 (дата обращения: 13.112020). — Режим доступа: для авторизир. пользователей Электронно-библиотечная

система: IPR B00kS https://www.iprbookshop.ru/89443.html https ://www.iprbookshop.ru/6991 .html

Веб-система для организации дистанционного обучения и управления им:

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