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

Комплект контрольно-оценочных средств

по учебной дисциплине

ОП 09. Защита информационных процессов в компьютерных системах

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2023

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

Составитель:
Рогачева О.Н., преподаватель ОГАПОУ «Алексеевский колледж»

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП 09. Защита информационных процессов в компьютерных системах.

КОС включают контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы учебной дисциплины ОП 09. Защита информационных процессов в компьютерных системах.

1.2 Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

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 (ПК) и общие (ОК) **компетенции**, которые актуализируются 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

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

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

- **Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении учебной дисциплины:**
- понимание принципов работы специалиста по информационной безопасности и их применение;
- знание принципов и положений безопасной работы в общем и по

отношению к корпоративной среде;
- регламентирующие документы в области безопасности информационных систем;
- регламентирующие документы в области охраны труда и безопасности жизнедеятельности;
- важность организации труда в соответствии с методиками;
- методы и технологии исследования;
- важность управления собственным профессиональным развитием;
- скорость изменения Ит-сферы и области информационной безопасности, а также важность соответствия современному уровню.
- важность умения слушать собеседника как части эффективной коммуникации;
- роли и требования коллег и наиболее эффективные методы коммуникации;
- важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими;
- способы разрешения непонимания и конфликтующих требований;

1) уметь:

- интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований;
- применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении;
- настраивать сетевые устройства;
- администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;
- установка агентской части системы корпоративной защиты от внутренних угроз;
- запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров;
- настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом;
- уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки;

Планируемые личностные результаты освоения рабочей программы

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде 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 Результаты освоения учебной дисциплины, подлежащие проверке

Наименование тем	Коды умений (У), знаний (З), личностных результатов (ЛР), формированию которых способствует элемент программы	Средства контроля и оценки результатов обучения **в рамках текущей аттестации** (номер задания)	Средства контроля и оценки результатов обучения **в рамках промежуточной аттестации** (номер задания/контрольного вопроса/ экзаменационного билета)
Тема 1. Анализ потенциальных угроз безопасности информационных процессов в компьютерных системах	У1-У7 З1-З6 ЛР 4 ЛР 7	ТЗ №1	КВ №1-7 ТЗ №1 ПЗ №1
Тема 2. Методы защиты	У1-У7 З1-З6 Р 4 ЛР 7 ЛР 10 ЛР 11	ТЗ №2	ТЗ №1 КВ №8-13
Тема 3. Информационные процессы и системы	У1-У7 З1-З6 ЛР 4	ТЗ №3	ТЗ №1 КВ №14-20
Тема 4. Особенности защиты информации на узлах компьютерной сети	У1-У7 З1-З6 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ТЗ №4	ТЗ №1 КВ №21-25

2. Комплект оценочных средств

2.1. Практические задания (ПЗ)

ПЗ №1 ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ ЗАЩИТЫ НА ТИПОВОМ ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ.

2.2. Тестовые задания (ТЗ)

ТЗ№1 АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

1. Угроза – это…

А) **потенциальная возможность определенным образом нарушить информационную безопасность**

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

2. Источник угрозы – это..

А) **потенциальный злоумышленник**

Б) злоумышленник

В) нет правильного ответа

3. Атака – это…

А) **попытка реализации угрозы**

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

4 Окно опасности – это…

А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.**

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

5 Какие события должны произойти за время существования окна опасности?

А) **должно стать известно о средствах использования пробелов в защите.**

Б) должны быть выпущены соответствующие заплаты.

В) заплаты должны быть установлены в защищаемой И.С.

6. Угрозы можно классифицировать по нескольким критериям:

А) **по спектру И.Б.**

Б) по способу осуществления

В) по компонентам И.С.

7. По каким компонентам классифицируется угрозы доступности:

А) **отказ пользователей**

Б) отказ поддерживающей инфраструктуры

В) ошибка в программе

8. Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации

Б) разрушение данных

В) **все ответы правильные**

9. Основными источниками внутренних отказов являются:

А) **ошибки при конфигурировании системы**
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации
10. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа
11. Какие существуют грани вредоносного П.О.?
А) **вредоносная функция**
Б) внешнее представление
В) способ распространения
12. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) **все ответы правильные**
13. Вирус – это…
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи
14. Черви – это…
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами
15. Конфиденциальную информацию можно разделить:
А**) предметную**
Б) служебную
В) глобальную
16. Природа происхождения угроз:
А) **случайные**
Б) преднамеренные
В) природные
17. Предпосылки появления угроз:
А) **объективные**
Б) субъективные
В) преднамеренные
18. К какому виду угроз относится присвоение чужого права?
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда
19. Отказ, ошибки, сбой – это:
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы

ТЗ№2 МЕТОДЫ ЗАЩИТЫ

1. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации?

A. Информационная защита информации

B. Информационная безопасность

C. Зашита информации

2. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?

A. Препятствие

B. Управление доступом

C. Маскировка

3. Какой метод защиты информации связан с регулированием использования всех ресурсов информационной системы?

A. Маскировка

B. Препятствие

C. Управление доступом

4. Как называется установления подлинности объекта по предъявленному им идентификатору (имени)?

A. Аутентификация

B. Идентификация

C. Маскировка

5. Как называется метод защиты информации в информационной системе организации путем ее криптографического закрытия?

A. Аутентификация

B. Идентификация

C. Маскировка

6. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

A. Принуждение

B. Маскировка

C. Идентификация

7. Какой метод защиты информации мотивирует сотрудников не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм?

A. Принуждение

B. Побуждение

C. Маскировка

8. Какие средства защиты информации предназначены для внешней охраны территории объектов и защиты компонентов информационной системы организации?

A. Аппаратные

B. Программные

C. Физические

9. Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи?

A. Аппаратные

B. Программные

C. Физические

10. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

A. Аппаратные

B. Программные

C. Физические

D. Ключ к тесту

№ п/п	Ответ
1	B
2	A
3	C
4	A
5	C
6	A
7	B
8	C
9	A
10	B

ТЗ№3 ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И СИСТЕМЫ

1. Модель OSI описывает:

А) правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи;

Б) только правила передачи данных в различных сетевых средах при организации сеанса связи;

В) только процедуры передачи данных в различных сетевых средах при организации сеанса связи.

2. На сколько уровней модель OSI разделяет коммуникационные функции:

А) 5;

Б) 8;

В) 7.

3. Какие задачи выполняют уровни OSI в процессе передачи данных по сети:

А) уровни выполняют одинаковые задачи, постоянно повторяя передающие сигналы по сети;

Б) каждый уровень выполняет свою определенную задачу;

В) первых три уровня выполняют одинаковые задачи, последующие выполняют определенные задачи.

4. Выбрать правильное расположение уровней модели OSI от 7 до 1:

А) прикладной, канальный, представительский, сеансовый, транспортный, сетевой, физический;

Б) представительский, прикладной, сеансовый, транспортный, сетевой, канальный, физический;

В) прикладной, представительский, сеансовый, транспортный, сетевой, канальный, физический.

5. Верно ли утверждение: «Каждый уровень модели выполняет свою функции. Чем выше уровень, тем более сложную задачу он решает»:

А) верно;

Б) не верно.

6. На базе протоколов, обеспечивающих механизм взаимодействия программ и процессов на различных машинах, строится:

А) горизонтальная модель;

Б) вертикальная модель;

В) сетевая модель.

7. На основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине строится:

А) горизонтальная модель;

Б) вертикальная модель;

В) сетевая модель.

8. Какой уровень представляет собой набор интерфейсов, позволяющим получить доступ к сетевым службам:

А) представительский;

Б) прикладной;

В) сеансовый.

9. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде:

А) представительский;

Б) прикладной;

В) канальный.

10. Какой уровень преобразует данные в общий формат для передачи по сети:

А) сетевой;

Б) представительский;

В) сеансовый.

11. Какой уровень обеспечивает битовые протоколы передачи информации:

А) сетевой;

Б) транспортный;

В) физический.

12. Какой уровень управляет передачей данных по сети и обеспечивает подтверждение передачи:

А) транспортный;

Б) канальный;

В) сеансовый.

13. Какой уровень поддерживает взаимодействие между удаленными процессами:

А) транспортный;

Б) канальный;

В) сеансовый.

14. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические:

А) сетевой;

Б) представительский;

В) транспортный.

15. Единица данных, которой оперирует прикладной уровень, называется:

А) пакетом;

Б) сообщением;

В) потоком.

16. При какой передаче прикладные процессы будут передавать данные, и принимать их одновременно?

А) дуплексная передача;

Б) полудуплексная передача.

17. При какой передаче прикладные процессы будут передавать и принимать данные по очереди?

А) дуплексная передача;

Б) полудуплексная передача.

18. Единицей информации канального уровня являются:

А) сообщения;

Б) потоки;

В) кадры.

19. Под физической средой понимают:

А) материальную субстанцию, через которую осуществляется передача сигнала;

Б) материальную субстанцию, из которой состоит материнская плата;

В) совокупность сигналов.

20. Основными элементами модели OSI являются:

А) уровни;

Б) уровни и прикладные процессы;

В) уровни, прикладные процессы и физические средства соединения.

Ответы на тест:

1-А	6-А	11-В	16-А
2-В	7-Б	12-А	17-Б
3-Б	8-Б	13-В	18-В
4-В	9-В	14-А	19-А
5-А	10-Б	15-Б	20-В

ТЗ №4 ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА УЗЛАХ КОМПЬЮТЕРНОЙ СЕТИ

1«маски» вирусов используются

+для поиска известных вирусов

- для поиска неизвестных вирусов
- для уничтожения известных вирусов
- для размножения вирусов
- для создания известных вирусов

2 ip-адрес имеет длину

+4 байта

- 8 байт
- 1 бит
- 8 бит
- 16 байт

3 security updates (обновления безопасности) необходимы

+для устранения обнаруженных недочетов в установленном по в операционных системах, установки патчей для предотвращения возможности эксплуатации уязвимостей, для поддержания внутренней самозащиты программ

- для поддержания внутренней самозащиты программ
- для обогащения вендоров, т.к. За дополнительные данные нужно платить
- для обновления внутренних модулей программ, чтобы приложения работали быстрее
- для облегчения работы с программами и улучшения восприятия интерфейса

4 алгоритм des использует длину блока:

+ 64 бит

- 256 бит
- 128 бит

- 8 бит
- 16 бит

5 алгоритм des использует длину ключа

+ 56 бит
- 256 бит
- 128 бит
- 8 бит
- 16 бит

6 алгоритм диффи-хеллмана используется для

+ открытого распределения ключей
- вычисления хэш-функции
- генерации простых чисел
- генерации случайных чисел
- безопастного хранения ключей

7 алгоритм диффи-хелмана позволяет

+использовать незащищенный от прослушивания, но защищённый от подмены, канал связи
- генерировать новые простые числа
- вычислить хэш функцию
- генерировать случайные числа
- безопасно хранить ключи

8 алгоритм шифрования sha предназначен для использования совместно с алгоритмом цифровой подписи

+ dsa
- dos
- des
- egs
- rsa

9 объект «а» заявляет, что он не посылал сообщение объекту «б», хотя на самом деле он все-таки посылал:

+отказ (ренегатство)
- подделка
- модификация (переделка)
- маскировка
- активный перехват

10 антивирус – это программа, которая

+ удаляет некоторые категории вредоносных программ, достигая успеха менее чем в 100 процентах случаев
- удаляет все виды вредоносного по с вашего компьютера
- может быть обновлена средствами «автоматического обновления windows» для получения новых сигнатур
- позволяет «откатить» все изменения, произведенные с момента активации враждебной программы, либо воспрепятствует ее активации в первую очередь
- удаляет все виды вредоносного по с компьютера

11аспектами информационной безопасности являются

+ конфиденциальность, доступность, целостность
- неизменность, доступность, целостность
- неизменность , конфиденциальность
- конфиденциальность, целостность
- доступность, конфиденциальность

12 аудит информационной безопасности должен включать в себя

+ анализ информационных рисков с целью оценки вероятного ущерба и инструментальной проверки защищенности для определения возможности реализации угроз
- оценку угроз
- анализ и классификацию угроз безопасности согласно модели нарушителя
- оценку стоимости ресурсов и информации.
- оценку зависимости компании от внешних связей и тесты на проникновение

13 безопасность данных в информационной базе обеспечивается
+ конфиденциальностью, целостностью и доступностью информации
- периодичностью обновления информации
- шифрованием информации
- идентификацией абонентов
- определением полномочий

14 абонент «а» изменяет сообщение и утверждает, что данное (измененное) сообщение послал ему абонент «б»
+ модификация (переделка)
- маскировка
- активный перехват
- отказ
- подделка

15абонент «а» формирует сообщение и утверждает, что данное (измененное) сообщение послал ему абонент «б»
+ подделка
- активный перехват
- отказ
- модификация
- маскировка

16 более усовершенствованный вид мнемокодов
+ автокоды
- rss-коды
- штрихкоды
- чит-коды
- отладочный код

17в каком году был представлен алгоритм диффи-хелмана:
+ 1975г
- 1974г
- 1978г
- 1977г
- 1976г

18в каком году и где был разработан алгоритм sha
+ 1993 году в сша
- 1991 году в сша
- 1995 году в сша
- 1992 году в сша
- 1994 году в сша

19 в версиях ms office 2007 \ 2010 компания microsoft использует алгоритм шифрования
+ aes с 128-битным ключом
- aes с 256-битным ключом
- aes с 16-битным ключом
- aes с 32-битным ключом
- aes с 8 -битным ключом

20в процедуре постановки подписи используется

+секретный ключ отправителя сообщения
- закрытый ключ отправителя сообщения
- открытый ключ отправителя сообщения
- чит-код
- хеш-функция

21в процедуре проверки подписи используется:

+открытый ключ отправителя
- генерация пары ключей
- секретный ключ отправителя
- хеш-функция
- аудит подписи

22в процедуре формирования подписи используется

+секретный ключ отправителя
- открытый ключ отправителя
- генерация пары ключей
- идентификация субъекта
- идентификация объекта

23 абонент «а» только что прислал вам по icq ссылку на *.exe файл в интернете, предложил запустить его и вышел из сети, так что вы не можете уточнить детали. Правильные действия:

+никогда не открою ссылку, даже если она от друга
- открою ссылку
- открою ссылку, если известен ключ
- .exe файл заблокируется
- открою ссылку после перезагрузки

24 вид злоумышленного действия , если абонент с повторяет ранее переданный документ, который абонент а посылал абоненту в.

+повтор
- замена
- подмена
- ренегатство
- копирование

25 абонент «в» перехватывает сообщения между абонентом «а» и абонентом «б» с целью их скрытой модификации:

+активный перехват
- подделка
- отказ
- маскировка
- модификация

26абонент «в» повторяет ранее переданное сообщение, которое абонент «а» посылал ранее «б»

+повтор
- маскировка
- имитация
- модификация
- подделка

27абонент «в» посылает абоненту «б» сообщение от имени абонента «а»

+маскировка (имитация)
- модификация
- отказ
- подделка
- активный перехват

28возможность использовать одинаковые имена для методов входящих различные классы называются:

+ полиформизм
- метоморфизм
- декапсуляция
- наследование
- инкапсуляция

29 возможные последствия botnet-инфекции:

+заражение boot-секторов дисков, могут привести к полной потере всей информации, хранящейся на диске
- компьютер будет захвачен и втайне использован для рассылки спама и проведения атак на другие пк
- ваш пк будет действовать как сервер, подчиняясь удаленным командам хакера
- часть вашего интернет-канала будет использоваться под вредоносный исходящий трафик
- проведение атак на другие пк

30 вы получаете email от вашего банка с просьбой в течение недели подтвердить ваши последние покупки, перейдя на соответствующую страницу сайта банка. Ваши действия

+ буду бдительным - уточню в банке подлинность письма, не буду кликать ни по каким ссылкам в письме и проверю свой счет, вручную набрав нужный адрес в адресной строке браузера
- проследую по ссылке из письма и введу требуемую информацию, т.к письмо имеет все признаки послания от легитимной организации
- развлекусь, введя на требуемой странице ложную информацию -
- все равно я ничего не теряю; - я знаю, что это phishing - поэтому удалю сообщение из почтового ящика
- решу, как поступить позже

3. Комплект оценочных средств

3.1. Контрольные вопросы (КВ)

КВ№1 Проблемы информационной безопасности.
КВ№2 Правовые основы защиты информации информационных процессов в компьютерных системах.
КВ№3 Источники угроз.
КВ№4 Постановка задачи анализа потенциальных угроз.
КВ№5 Анализ и защита от утечки компьютерной информации по каналам ПЭМИН.
КВ№6 Анализ электромагнитных излучений и наводок в компьютерных системах.
КВ№7 Организационные методы защиты информационных процессов в компьютерных системах.
КВ№8 Ограничение и контроль доступа, идентификация и установление доступа
КВ№9 Инженерно-технические методы защиты информационных процессов.
КВ№10 Программно-аппаратные методы защиты информации.
КВ№11 Программно-аппаратные методы защиты информационных процессов.
КВ№12 Защита электронных документов.
КВ№13 Модель ISO/OSI. Физический уровень.
КВ№14 Канальный уровень.
КВ№15 Модель ISO/OSI. Сетевой уровень.
КВ№16 Транспортный уровень
КВ№17 Открытый ключ..
КВ№18 Администрирование серверных систем и приложений.
КВ№19 Основные виды работ администрирования серверных систем и приложений.
КВ№20 Резервное копирование.
КВ№21 Мультиплексирование и архивирование.
КВ№22 Случайные и преднамеренные угрозы.
КВ№23 Основные понятия и положения защиты информации в компьютерных сетях
КВ№24 Система электронной подписи
КВ№25 Журнализация изменений

3.2. Тестовые задания (ТЗ)

ТЗ №1

1. Под информационной безопасностью понимается…

А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных**

отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) **комплекс мероприятий, направленных на обеспечение информационной безопасности.**

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) **от компьютеров**

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…

А) **возможность за приемлемое время получить требуемую информационную услугу.**

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

А) **целостность информации**

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность – это..

А) **защита от несанкционированного доступа к информации**

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

А) **получения определенных информационных услуг**

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

А) **статическую**

Б) динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?

А) **анализе потока финансовых сообщений**

Б) обработке данных

В) **при выявлении кражи, дублирования отдельных сообщений**

11. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) **все ответы правильные**

12. Угроза – это…

А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа
13. Атака – это…
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.
14. Источник угрозы – это..
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа
15. Окно опасности – это…
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
16. Какие события должны произойти за время существования окна опасности?
А) **должно стать известно о средствах использования пробелов в защите.**
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.
17. Угрозы можно классифицировать по нескольким критериям:
А) **по спектру И.Б.**
Б) по способу осуществления
В) по компонентам И.С.
18. По каким компонентам классифицируется угрозы доступности:
А) **отказ пользователей**
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе
19. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) **все ответы правильные**
20. Основными источниками внутренних отказов являются:
А) **ошибки при конфигурировании системы**
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации
21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа
22. Какие существуют грани вредоносного П.О.?
А) **вредоносная функция**
Б) внешнее представление
В) способ распространения

23. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) **все ответы правильные**
24. Вирус – это…
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи
25. Черви – это…
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами
26. Конфиденциальную информацию можно разделить:
А**) предметную**
Б) служебную
В) глобальную
27. Природа происхождения угроз:
А) **случайные**
Б) преднамеренные
В) природные
28. Предпосылки появления угроз:
А) **объективные**
Б) субъективные
В) преднамеренные
29. К какому виду угроз относится присвоение чужого права?
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда
30. Отказ, ошибки, сбой – это:
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы
31. Отказ - это…
А) **нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов
32. Ошибка – это…
А) **неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния**
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу
33. Сбой – это…
А) **такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**

Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод
34. Побочное влияние – это…
А) **негативное воздействие на систему в целом или отдельные элементы**
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
35. СЗИ (система защиты информации) делится:
А) **ресурсы автоматизированных систем**
Б) организационно-правовое обеспечение
В) человеческий компонент
36. Что относится к человеческому компоненту СЗИ?
А) **системные порты**
Б) администрация
В) программное обеспечение
37. Что относится к ресурсам А.С. СЗИ?
А) лингвистическое обеспечение
Б) техническое обеспечение
В) **все ответы правильные**
38. По уровню обеспеченной защиты все системы делят:
А) **сильной защиты**
Б) особой защиты
В) слабой защиты
39. По активности реагирования СЗИ системы делят:
А) **пассивные**
Б) активные
В) полупассивные
40. Правовое обеспечение безопасности информации – это…
А) **совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа
41. Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) **все ответы правильные**
42. Информацию с ограниченным доступом делят:
А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию
43. Что относится к государственной тайне?
А) **сведения, защищаемые государством в области военной, экономической … деятельности**
Б) документированная информация
В) нет правильного ответа
44. Вредоносная программа - это…
А) **программа, специально разработанная для нарушения нормального функционирования систем**
Б) упорядочение абстракций, расположение их по уровням

В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

45. Основополагающие документы для обеспечения безопасности внутри организации:

А) **трудовой договор сотрудников**

Б) должностные обязанности руководителей

В) коллективный договор

46. К организационно - административному обеспечению информации относится:

А) **взаимоотношения исполнителей**

Б) подбор персонала

В) регламентация производственной деятельности

47. Что относится к организационным мероприятиям:

А) **хранение документов**

Б) проведение тестирования средств защиты информации

В) **пропускной режим**

48. Какие средства используется на инженерных и технических мероприятиях в защите информации:

А) **аппаратные**

Б) криптографические

В) физические

49. Программные средства – это…

А) **специальные программы и системы защиты информации в информационных системах различного назначения**

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это…

А) **средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования**

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

3.3. Практические задания (ПЗ)

ПЗ **№1**

Модуль 1: Анализа информационного пространства

Разработать политики информационной безопасности, используя инструментарий автоматизированной системы IWTM 6 и успешно их применить для выявления и/или блокирования инцидентов безопасности. Для создания инцидентов и других событий в IWTM используется специальное программное обеспечение – специальный Генератор трафика и инцидентов. Участнику необходимо:

1. Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания;

2. Занести политики информационной безопасности в DLP-систему;

3. Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п.;

4. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором трафика и инцидентов. Максимизировать число выявленных инцидентов безопасности;

5. Продемонстрировать владение технологиями и умение работать с интерфейсом управления системы корпоративной защиты информации IWTM. Участнику необходимо применить политики информационной безопасности в системе IWTM, автоматически выполнить поиск инцидентов информационной безопасности, внесенных членами жюри (с использованием стенда и Генератора трафика и инцидентов). Политики можно модифицировать, с целью выявления максимального числа инцидентов и утечек. Необходимо использовать весь набор технологий поиска и выявления уязвимостей, доступный в системе корпоративной защиты. Итоговый вариант политик должен быть зафиксированы в отчете. В число инцидентов могут входить, например:

– передача персональных данных сотрудников и контрагентов по электронной почте;

– передача базы клиентов организации в архиве с использованием файловых протоколов;

– нецензурная лексика сотрудников в переписке с контрагентами;

– передача информации, составляющей коммерческую тайну и др. Задание выполняется с помощью программного обеспечения DLP (Data Leaks Prevention) IWTM 6.

4. Критерии оценивания

«5» «отлично» или «зачтено» – студент показывает глубокое и полное овладение содержанием программного материала по УД, 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» или «зачтено» – студент в полном объеме освоил программный материал по УД, 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» или «зачтено» – студент обнаруживает знание и понимание основных положений программного материала по УД, 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» или «не зачтено» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по УД, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

5. Информационное обеспечение

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

Основные источники:

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб.пособие / В.Ф. Шаньгин. – Москва : ИД «ФОРУМ» : ИНФРА-М, 2020.- 416с.
2. Основы информационной безопасности: учебник/Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А.. – М.: Академия. 2019-256 с.

Дополнительные источники:

3. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
4. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
5. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.
6. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
7. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008
8. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
9. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
10. Мельников Д. Информационная безопасность открытых систем.-М.: Форум, 2013.
11. 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.
12. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.
13. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д.А.–М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 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 PROFобразование:

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 c. — ISBN 978-5-4497-0666-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: 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 c. — ISBN 978-5-4487-0299-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/77318 (дата обращения: 13.11.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPR BOOKS

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/