Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Искаков Ирлан Жангазыевич
Должность: Ректор
Дата подписания: 15.08.2022 11:17:27
Уникальный программный ключ:
a748d5b672796bd7b37612bb23a3449357804892a0d120774ea9def3ef7a2bc0

Автономная некоммерческая организация высшего образования
«Университет при Межпарламентской Ассамблее ЕврАзЭС»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

Направление подготовки 54.03.01 Дизайн

Квалификация выпускника Бакалавр

Направленность (профиль) Дизайн среды

2022 г.

1. Место дисциплины в структуре образовательной программы, входные требования для освоения дисциплины (при необходимости)

Дисциплина «Информационная безопасность» относится к дисциплинам базовой части Блока 1 «Дисциплины (модули)» программы бакалавриата.

2. Объем дисциплины в зачетных единицах

Объем дисциплины составляет 2 зачетные единицы.

3. Содержание дисциплины, структурированное по темам (разделам)

Раздел 1. Защита информации. Место информационной безопасности в национальной безопасности РФ.

Тема 1.1 Цели и задачи информационной безопасности.

Тема 1.2. Построение системы защиты информации (СЗИ) в организации.

Тема 1.3. Современные методики анализа и управления рисками информационной безопасности.

Раздел 2. Информационная безопасность, как основа стабильности организации.

Тема 2.1 Криптографическая защита информации.

Тема 2.2. Программы, обеспечивающие защиту информации.

4. Методические рекомендации по организации изучения учебной дисциплины

Изучение дисциплины включает контактную работу обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях в форме занятий различных типов в соответствии со спецификой дисциплины и самостоятельную работу обучающихся в объемах соответственно учебному плану. Контактная работа может проводиться с применением электронного обучения, дистанционных образовательных технологий.

Теоретические занятия

Раздел 1. Защита информации. Место информационной безопасности в национальной безопасности РФ.

Тема 1.1 Цели и задачи информационной безопасности.

Понятие информации. Фазы обращения информации в информационных системах.

Место информационной безопасности в национальной безопасности РФ.

Цели и задачи обеспечения информационной безопасности.

Составляющие информационной безопасности.

Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.

Виды и источники угроз информационной безопасности РФ.

Структура государственной системы обеспечения информационной безопасности РФ.

Тема 1.2. Построение системы защиты информации (СЗИ) в организации.

Архитектура СЗИ организации и основные требования к средствам защиты.

Функциональное построение СЗИ организации и назначение основных подразделений.

Элементарные модели СЗИ организации. Семирубежная модель защиты.

Последовательность и содержание основных этапов проектирования СЗИ организации.

Содержание процесса эксплуатации СЗИ организации.

Анализ угроз информационной безопасности.

Внутренние и внешние источники угроз информационной безопасности.

Схема воздействия угроз на информационную систему.

Перечень основных формальных и неформальных средств защиты информации.

Стратегии защиты информации на объекте информатизации.

Основы защиты информации в телекоммуникационных сетях.

Роль персонала в обеспечении информационной безопасности предприятия.

Тема 1.3. Современные методики анализа и управления рисками информационной безопасности.

Управление рисками на различных стадиях жизненного цикла информационной системы.

Трехмерная модель "куб безопасности".

Анализ информационных рисков, угроз и уязвимостей системы.

Оценка рисков по двум факторам.

Анализ информационных рисков, угроз и уязвимостей системы.

Оценка рисков по трем факторам.

Программное обеспечение для анализа рисков информационной безопасности.

Раздел 2. Информационная безопасность, как основа стабильности организации.

Тема 2.1 Криптографическая защита информации.

Классические криптоалгоритмы – моно- и многоалфавитные подстановки.

Классические криптоалгоритмы - перестановки.

Шифрование методом гаммирования.

Современные симметричные системы шифрования. Обобщенная схема симметричного шифрования.

Симметричная система шифрования DES.

Отечественный стандарт симметричного шифрования.

Принцип открытого распространения ключей. Алгоритм Диффи-Хеллмана.

Современные асимметричные системы шифрования. Обобщенная схема асимметричного шифрования.

Асимметричная система шифрования RSA.

Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП.

Электронная цифровая подпись на основе алгоритма RSA.

Отечественный стандарт цифровой подписи ГОСТ Р34.10-2012.

Тема 2.2. Программы, обеспечивающие защиту информации.

Вредоносное программное обеспечение и методы борьбы с ним.

Практические занятия

Тема 1.2. Построение системы защиты информации (СЗИ) в организации.

Анализ угроз информационной безопасности. Построение схем воздействия угроз на информационную систему.

Тема 1.3. Современные методики анализа и управления рисками информационной безопасности.

Построение трехмерной модели “куб безопасности”. Оценка рисков по двум факторам.

Тема 2.1 Криптографическая защита информации.

Применять на практике криптоалгоритмы – моно- и многоалфавитные подстановки, классические криптоалгоритмы - перестановки. Шифрование методом гаммирования.

Уметь пользоваться современными симметричными системами шифрования, а также обобщенной схемой симметричного шифрования, симметричной системой шифрования DES. Отечественным стандартом симметричного шифрования.

Тема 2.2. Программы, обеспечивающие защиту информации.

Практические задачи на применение антивирусных программ.

Семинарские занятия

Тема 1.1 Цели и задачи информационной безопасности.

Место информационной безопасности в национальной безопасности РФ.

Цели и задачи обеспечения информационной безопасности.

Тема 1.2. Построение системы защиты информации (СЗИ) в организации.

Архитектура СЗИ организации и основные требования к средствам защиты.

Анализ угроз информационной безопасности.

Тема 1.3. Современные методики анализа и управления рисками информационной безопасности.

Управление рисками на различных стадиях жизненного цикла информационной системы.

5. Методические рекомендации для обеспечения самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов включает усвоение теоретического материала, подготовку к практическим и семинарским занятиям, выполнение самостоятельных заданий, изучение литературных источников, использование Internet-данных, изучение нормативно-правовой базы, подготовку к текущему контролю знаний, к промежуточной аттестации.

Вопросы для самоконтроля

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?

5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP- сниффинга существуют?
12. Какие модели многоуровневой защиты вы знаете?
13. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
14. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
15. Какие задачи решает система компьютерной безопасности?
16. Какие пути защиты информации в локальной сети существуют?
17. Какие задачи решают технические средства противодействия экономическому шпионажу?
18. Из чего состоит высоконадежная вычислительная база (ТСВ)?
19. Что представляет собой домен?
20. Что включает борьба с атаками на уровне приложений?
21. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
22. В чем заключается распределенное хранение файлов?
23. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
24. Какие уровни информационной защиты существуют, их основные составляющие?
25. В чем заключаются задачи криптографии?
26. Зачем нужны ключи?
27. Какая схема шифрования называется многоалфавитной подстановкой?
28. Какие системы шифрования вы знаете?
29. Что включает в себя защита информации от несанкционированного доступа?
30. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
31. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
32. Какие задачи выполняет подсистема управления доступом?
33. Какие требования предъявляются к подсистеме протоколирования аудита?
34. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
35. В чем заключается контроль участников взаимодействия?
36. Какие функции выполняет служба регистрации и наблюдения?
37. Что такое информационно-опасные сигналы, их основные параметры?
38. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
39. Какой процесс называется аутентификацией пользователя?
40. Какие схемы аутентификации вы знаете?
41. Что такое смарт-карты?
42. Какие требования предъявляются к современным криптографическим системам защиты информации?
43. Что такое симметричная криптосистема?
44. Какие виды симметричных криптосистем существуют?
45. Что такое асимметричная криптосистема?

46. Что понимается под односторонней функцией?
47. Как классифицируются криптографические алгоритмы по стойкости?
48. В чем заключается анализ надежности криптосистем?
49. Что такое дифференциальный криптоанализ?
50. В чем сущность криптоанализа со связанными ключами?
51. В чем сущность линейного криптоанализа?
52. Какие атаки изнутри вы знаете?
53. Какая программа называется логической бомбой?
54. Какими способами можно проверить систему безопасности?
55. Что является основными характеристиками технических средств защиты информации?
56. Какие требования предъявляются к автоматизированным системам защиты третьей группы?
57. Какие требования предъявляются к автоматизированным системам защиты второй группы?
58. Какие требования предъявляются к автоматизированным системам защиты первой группы?
59. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
60. Какие требования предъявляются к межсетевым экранам?
61. Какие имеются показатели защищенности межсетевых экранов?
62. Какие атаки системы снаружи вы знаете?
63. Какая программа называется вирусом?
64. Какая атака называется атакой отказа в обслуживании?
65. Какие виды вирусов вы знаете?
66. Какие вирусы называются паразитическими?
67. Как распространяются вирусы?
68. Какие методы обнаружения вирусов вы знаете?
69. Какая программа называется монитором обращения?
70. Как осуществляется защита при помощи ACL-списков?
71. Какой список называется перечнем возможностей?
72. Какие способы защиты перечней возможностей вы знаете?

6. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

6.1. Планируемые результаты обучения, соотнесенные с индикаторами достижения компетенций

В процессе изучения дисциплины у обучающихся должны быть сформированы следующие компетенции:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК – 6).

Код и формулировка компетенции	Индикаторы достижения компетенций
ОПК-6 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знает:** методы и средства получения, хранения, обработки, передачи и защиты информации; основные понятия, связанные с информационной безопасностью, современные принципы работы с информацией; основные требования информационной безопасности
	Умеет: решать стандартные задачи в профессиональной деятельности с использованием информационно-коммуникационных технологий; соблюдать основные требования информационной безопасности
	Владеет: навыками практического применения программного обеспечения для решения профессиональных задач, требующих работы с информацией; навыками соблюдения требований информационной безопасности.

6.2. Перечень оценочных материалов

Оценочные материалы представляют собой задания для выполнения обучающимся, позволяющие ему приобрести теоретические знания, практически умения (навыки) и опыт, а также решать задачи, связанные с будущей профессиональной деятельностью. Включают в себя задания для текущего контроля уровня успеваемости, оценивающие ход освоения обучающимися дисциплины, и задания для промежуточной аттестации обучающих, обеспечивающие оценивание промежуточных и окончательных результатов обучения по дисциплине.

Примерные задания для проведения текущего контроля успеваемости

Тестовые задания

Вариант № 1

1) Что входит в понятие “безопасность информации”
a) исключение ознакомления с информацией сотрудников АСОИ
b) предотвращение ознакомления с информацией лиц к ней не допущенных
c) исключение изменений информации
d) исключение утечки информации за счет излучений и наводок
2) Конфиденциальность информации обеспечивается путем
a) содержания критической информации в секрете
b) ограничения доступа в специальные помещения
c) организации мониторинга сети
3) Информационная безопасность информации достигается обеспечением
a) конфиденциальности
b) доступности
c) комплексирования средств ЗИ
d) целостности информации
4) Защита целостности потоков данных осуществляется с использованием
a) дополнительных форм нумерации
b) меток времени
c) повтором сообщений
d) включением дополнительных признаков к сообщению
5) Для обеспечения защиты от анализа трафика могут быть использованы
a) механизм заполнения текста
b) генерация фиктивных сообщений
c) ограничение доступа в выделенные помещения
6) Если сеть централизованная, то защита должна
a) централизованной
b) распределенной
7) При схеме управления защитой информации "длинные руки" полномочия пользователей на каждом компьютере устанавливаются
a) администратором удаленно со своего рабочего места
b) самим пользователем системы
c) пользователем системы после действий администратора безопасности

8) Схема отложенного централизованного управления доступом требует, чтобы компьютеры пользователей на момент изменения полномочий были

a) включены
b) выключены
c) безразлично

9) Для облегчения работы администратора безопасности по контролю за состоянием безопасности АС необходимо предусмотреть следующие возможности

a) селекцию определенных событий из системных журналов
b) ограничение перечня событий, регистрируемых СЗИ
c) семантическое сжатие данных в журналах регистрации
d) автоматическую подготовку отчетных документов

10) Реальные возможности нарушителя определяются

a) психологическим состоянием нарушителя
b) состоянием объекта защиты,
c) наличием потенциальных каналов утечки информации,
d) качеством средств защиты информации

11) В качестве показателя эффективности системы защиты информации может быть использованы

a) вероятность обнаружения нарушения
b) своевременность реакции на каждый вид нарушения
c) доказуемость нарушения

12) Для осуществления несанкционированного доступа в информационную систему требуется провести подготовительные действия

a) собрать сведения о системе
b) выполнить пробные попытки вхождения в систему
c) выявить организационную структуру предприятия

13) Программы ЦП характеризуются следующими параметрами

a) криптостойкостью
b) количеством операторов
c) временем работы
d) функциональными возможностями

14) Время работы алгоритма ЦП складывается из времени

a) набора текста
b) генерации ключей
c) проверки подписи
d) постановки подписи

15) С увеличением криптостойкости системы ЦП временные характеристики

a) падают
b) увеличиваются

Вариант № 2

1) Конечная цель защиты информации

a) уменьшение возможных точек атак
b) сведение к минимуму потерь в управлении
c) формирование системы информационной безопасности
d) минимизация риска

2) Основные принципы построения системы защиты информации
a) принцип совместимости средств защиты информации
b) принцип непрерывного совершенствования СЗИ
c) принцип открытости
d) принцип комплексного использования средств защиты
3) Принцип непрерывности совершенствования СЗИ заключается в
a) постоянном контроле функционирования СЗИ
b) выявлении слабых мест в СЗИ
c) анализе рынка услуг в области защиты информации
d) обновлении и дополнении механизма защиты
4) Вероятные угрозы техническому обеспечению
a) изменение конфигурации
b) изменение маршрутизации
c) физический съем информации с каналов
d) искажение входных данных
5) Вероятные угрозы информационному обеспечению
a) Съем и использование выходной информации
b) Подмена протоколов
c) Изменение топологии
d) Перегрузка канала или устройства
6) Вероятные угрозы прикладным программам
a) ознакомление и изменение программ решения
b) изменение прав и полномочий на доступ к ресурсам
c) искажение входных данных
7) Администратор безопасности
a) осуществляет эксплуатацию средств защиты информации
b) обеспечивает непрерывность процесса обработки информации
c) восстанавливает работоспособность компьютерной системы
d) осуществляет допуск в специальные помещения
8) В случае возникновения нарушения в компьютерной системе администратор безопасности
a) изменяет пароли пользователей
b) локализует нарушение
c) определяет причину возникновения нарушения
d) вызывает представителей МВД
9) Источники получения информации для администратора безопасности
a) от пользователей
b) из системного журнала
c) кадровых органов
10) Нарушитель — это лицо, предпринявшее попытку выполнения запрещенных операций
a) по ошибке
b) незнанию
c) осознанно
d) с использованием служебного положения

11) Облик нарушителя по совершению противоправных действий определяется
a) мотивацией и намерениями,
b) совокупностью знаний, умений и навыков (способов) совершения нарушений
c) возможностями технических средств снятия информации
d) умением пользоваться средствами технической разведки
12) Реальные возможности нарушителя определяются
a) психологическим состоянием нарушителя
b) состоянием объекта защиты,
c) наличием потенциальных каналов утечки информации,
d) качеством средств защиты информации
13) Цифровая подпись это
a) полученная хэш-функция
b) хэш-функция, прошедшая математическую обработку
c) электронная версия фактической подписи
14) Цифровая подпись может храниться
a) вместе с документом
b) в отдельном файле
c) в закрытой области памяти
15) Проверка ЦП включает в себя проверку соотношения, связывающего
a) хэш-функцию и подпись под документом
b) подпись под документом и открытый ключ
c) хэш-функцию и открытый ключ
d) хэш-функцию, подпись и открытый ключ

Вариант № 3

1) Процесс защиты информации может быть
a) децентрализованным
b) иерархическим
c) централизованным
2) Система защиты информации может быть
a) децентрализованной
b) иерархической
c) централизованной
3) Принцип” предвидеть и предотвратить” требует наличия
a) средств прогнозирования
b) средств мониторинга сети
c) систем поддержки принятия решений
d) систем видеонаблюдения
4) Характерные особенности корпоративной сети по сравнению с локальной
a) высокая скорость передачи данных
b) неопределенный круг пользователей
c) большая протяженность линий связи
5) Уязвимые места корпоративной сети
a) каналы связи
b) ретрансляторы
c) шлюзы

d) модемы

6) Основные виды обеспечения корпоративной сети

a) информационное

b) техническое

c) методическое

d) программное

7) Главное требование к администратору безопасности

a) коммуникабельность

b) деловая активность

c) высокая профессиональная подготовленность

d) знание основ психологии

8) Основной показатель эффективности управления защитой информации

a) скрытность управления

b) величина цикла управления

c) безошибочность действий администратора

d) качество планирующих документов

9) Основные этапы управления

a) сбор и анализ информации от объектов защиты

b) обработка информации

c) принятие решения и выработка управляющих воздействий

d) реализация управляющих воздействий и контроль исполнения

10) На какой из аспектов защиты информации влияют ошибки в программном обеспечении

a) Конфиденциальность

b) Целостность

c) Доступность

11) Исходя и из каких обстоятельств ранжируются риски

(a) В зависимости от ущерба

(b) В зависимости от времени реакции на них

(c) В зависимости от степени конфиденциальности решаемой задачи

12) Меняются ли ранги рисков в зависимости от ситуации

a) да

b) нет

13) В общепринятую модель аутентификации входят

a) арбитр

b) приемник

c) передатчик

d) противник

14) Аутентификация служит для защиты от

a) маскарада

b) НСД

c) разрушения архивов

d) проникновения в спец. помещения

15) Система аутентификации характеризуется

a) наличием средств сканирования сети

b) временем реакции на нарушение

c) требуемыми вычислительными ресурсами
d) криптостойкостью

Темы доклада-презентации

1. Основные понятия и определения информационной безопасности. Виды информации ограниченного доступа.
2. Цели и задачи защиты информации.
3. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем.
4. Основные направления и способы защиты информации.
5. Понятия идентификации и аутентификации.
6. Требования к парольной защите.
7. Основные направления технической защиты информации.
8. Понятие технического канала утечки информации.
9. Угрозы утечки информации по техническим каналам.
10. Характеристики объектов информатизации.
11. Побочные электромагнитные излучения и наводки.
12. Классификация технических каналов утечки информации.
13. Понятие политики безопасности организации.
14. Сертификация средств защиты информации.
15. Категорирование информационных объектов по степени важности и конфиденциальности защищаемой информации.

Темы рефератов

1. Понятие информационной безопасности
2. Системы информационной безопасности и их дефекты
3. Основы криптографии
4. Шифрование с секретным ключом
5. Шифрование с открытым ключом
6. Цифровые подписи как элемент информационной безопасности
7. Аутентификация пользователей
8. Защита паролей в операционной системе (по выбору студента)
9. Совершенствование безопасности паролей
10. Атака системы безопасности
11. Атаки системы снаружи
12. Атаки системы изнутри
13. Механизмы защиты информации на предприятии
14. Факторы надежности системы информационной безопасности
15. Метод «песочниц»
16. Программы с подписями

17. Безопасность в системе Java

Примерные задания для проведения промежуточной аттестации по дисциплине

Список вопросов к зачету

ОПК-6 - знать

1. Основные понятия и определения информационной безопасности. Виды информации ограниченного доступа.
2. Цели и задачи защиты информации.
3. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем.
4. Основные направления и способы защиты информации.
5. Понятия идентификации и аутентификации.
6. Требования к парольной защите.
7. Основные направления технической защиты информации.
8. Понятие технического канала утечки информации.
9. Угрозы утечки информации по техническим каналам.
10. Характеристики объектов информатизации.
11. Побочные электромагнитные излучения и наводки.
12. Классификация технических каналов утечки информации.
13. Понятие политики безопасности организации.
14. Сертификация средств защиты информации.
15. Категорирование информационных объектов по степени важности и конфиденциальности защищаемой информации.
16. Аттестация объектов по выполнению требований обеспечения безопасности информации.
17. Основные разделы документов, характеризующих политику безопасности организации.
18. Задачи технических средств защиты информации.
19. Пассивные и активные средства и способы защиты информации.
20. Методы выявления закладочных устройств.
21. Устройства защиты телефонных переговоров. Генераторы пространственного зашумления.
22. Генераторы акустического и виброакустического зашумления.
23. Сетевые фильтры.
24. Подавители диктофонов.
25. Виды и типы аппаратных и программных средств защиты информации.
26. Специальные регистры для хранения реквизитов защиты.
27. Генераторы кодов.
28. Устройства измерения индивидуальных характеристик человека с целью его идентификации.
29. Устройства шифрования информации.
30. Классификация программных средств защиты информации.
31. Программы внешней защиты.
32. Программы внутренней защиты. Программы ядра системы безопасности.

33. Интегральная безопасность информационных систем.
34. Комплексная защита объектов.
35. Механические системы защиты.
36. Системы оповещения.
37. Системы опознавания.
38. Основы физической защиты объектов.
39. Интегральный комплекс физической защиты объектов.
40. Технические средства физической защиты.

Тест

ОПК-6- уметь

1. Какие технические каналы утечки информации Вы знаете
a) телевизионный
b) электромагнитный
c) визуально-оптический
d) акустический
2. Чем достигается нестандартность СЗИ организации
a) разнообразием используемых средств
b) отличием отдельных элементов СЗИ от СЗИ других объектов
c) содержанием политики безопасности в секрете
d) закупкой средств у разных организаций
3. Каждый пользователь должен иметь
a) минимальный набор привилегий по функциональным задачам
b) возможность доступа ко всей информации по каждой задаче
c) доступ к информации по его запросу
4. Характерные особенности корпоративной сети по сравнению с локальной
a) высокая скорость передачи данных
b) неопределенный круг пользователей
c) большая протяженность линий связи
5. Уязвимые места корпоративной сети
a) каналы связи
b) ретрансляторы
c) шлюзы
d) модемы
6. Основные виды обеспечения корпоративной сети
a) информационное
b) техническое
c) методическое
d) программное
7. Информационная безопасность и безопасность информации понятия одинаковые
a) да
b) нет
8. Понятие безопасность информации шире, чем понятие информационная безопасность
a) да
b) нет

9. Основная (опосредованная) цель управления информационной безопасностью

a) реализация потенциальных возможностей системы защиты

b) реализация потенциальных возможностей автоматизированной системы обработки информации

c) предотвращение НСД к информационным ресурсам

d) недопущение искажения и уничтожения информации

10. Основные направления защиты информации:

a) информационное

b) организационно-правовое

c) инженерно-техническое

d) лингвистическое

11. Экономическая эффективность СЗИ определяется

a) предотвращенным ущербом

b) совокупной стоимостью средств защиты информации

c) соотношением затрат на СЗИ и предотвращенным ущербом

12. Универсальность средств защиты характеризуется

a) независимостью языка представления информации

b) непротиворечивостью средств защиты информации

c) независимостью от формы представления информации

d) независимостью от вида носителя

13. Система защиты информации может быть

a) децентрализованной

b) иерархической

c) централизованной

14. Конечная цель защиты информации

a) уменьшение возможных точек атак

b) сведение к минимуму потерь в управлении

c) формирование системы информационной безопасности

d) минимизация риска

15. Понятие безопасность информации шире, чем понятие информационная безопасность

a) да

b) нет

16. Наиболее часто нарушения информационной безопасности происходят

a) От действий хакеров

b) От действий кракеров

c) По неопытности персонала

17. Что входит в понятие “безопасность информации”

a) исключение ознакомления с информацией сотрудников АСОИ

b) предотвращение ознакомления с информацией лиц к ней не допущенных

c) исключение изменений информации

d) исключение утечки информации за счет излучений и наводок

18. Конфиденциальность информации обеспечивается путем

a) содержания критической информации в секрете

b) ограничения доступа в специальные помещения

c) организации мониторинга сети

Перечень оценочных средств во взаимосвязи с планируемыми результатами обучения по дисциплине

Код и формулировка компетенции	Планируемые результаты обучения по дисциплине	Оценочные средства
ОПК-6 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**З н а е** методы и средства получения, хранения, обработки, передачи и защиты информации; основные понятия, связанные с информационной безопасностью, современные принципы работы с информацией; основные требования информационной безопасности	**Список вопросов:** 1. Основные понятия и определения информационной безопасности. Виды информации ограниченного доступа. 2. Цели и задачи защиты информации. 3. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем. 4. Основные направления и способы защиты информации. 5. Понятия идентификации и аутентификации. 6. Требования к парольной защите. 7. Основные направления технической защиты информации. 8. Понятие технического канала утечки информации. 9. Угрозы утечки информации по техническим каналам. 10. Характеристики объектов информатизации. 11. Побочные электромагнитные излучения и наводки. 12. Классификация технических каналов утечки информации. 13. Понятие политики безопасности организации. 14. Сертификация средств защиты информации. 15. Категорирование информационных объектов по степени важности и конфиденциальности защищаемой информации. 16. Аттестация объектов по выполнению требований обеспечения безопасности информации. 17. Основные разделы документов, характеризующих политику безопасности организации. 18. Задачи технических средств защиты информации. 19. Пассивные и активные средства и способы защиты информации. 20. Методы выявления закладочных устройств. 21. Устройства защиты телефонных переговоров. Генераторы пространственного зашумления. 22. Генераторы акустического и виброакустического зашумления.

		23. Сетевые фильтры. 24. Подавители диктофонов. 25. Виды и типы аппаратных и программных средств защиты информации. 26. Специальные регистры для хранения реквизитов защиты. 27. Генераторы кодов. 28. Устройства измерения индивидуальных характеристик человека с целью его идентификации. 29. Устройства шифрования информации. 30. Классификация программных средств защиты информации. 31. Программы внешней защиты. 32. Программы внутренней защиты. Программы ядра системы безопасности. 33. Интегральная безопасность информационных систем. 34. Комплексная защита объектов. 35. Механические системы защиты. 36. Системы оповещения. 37. Системы опознавания. 38. Основы физической защиты объектов. 39. Интегральный комплекс физической защиты объектов. 40. Технические средства физической защиты.
	Умеет: решать стандартные задачи в профессиональной деятельности с использованием информационно-коммуникационных технологий; соблюдать основные требования информационной безопасности	**Тесты:** 1. Какие технические каналы утечки информации Вы знаете a) телевизионный b) электромагнитный c) визуально-оптический d) акустический 2. Чем достигается нестандартность СЗИ организации a) разнообразием используемых средств b) отличием отдельных элементов СЗИ от СЗИ других объектов c) содержанием политики безопасности в секрете d) закупкой средств у разных организаций 3. Каждый пользователь должен иметь a) минимальный набор привилегий по функциональным задачам b) возможность доступа ко всей информации по каждой задаче c) доступ к информации по его запросу 4. Характерные особенности корпоративной сети по сравнению с локальной a) высокая скорость передачи данных b) неопределенный круг пользователей c) большая протяженность линий связи 5. Уязвимые места корпоративной сети a) каналы связи b) ретрансляторы

		c) шлюзы d) модемы 6. Основные виды обеспечения корпоративной сети a) информационное b) техническое c) методическое d) программное 7. Информационная безопасность и безопасность информации понятия одинаковые a) да b) нет 8. Понятие безопасность информации шире, чем понятие информационная безопасность a) да b) нет 9. Основная (опосредованная) цель управления информационной безопасностью a) реализация потенциальных возможностей системы защиты b) реализация потенциальных возможностей автоматизированной системы обработки информации c) предотвращение НСД к информационным ресурсам d) недопущение искажения и уничтожения информации 19. Основные направления защиты информации: a) информационное b) организационно-правовое c) инженерно-техническое d) лингвистическое 20. Экономическая эффективность СЗИ определяется a) предотвращенным ущербом b) совокупной стоимостью средств защиты информации c) соотношением затрат на СЗИ и предотвращенным ущербом 21. Универсальность средств защиты характеризуется a) независимостью языка представления информации b) непротиворечивостью средств защиты информации c) независимостью от формы представления информации d) независимостью от вида носителя 22. Система защиты информации может быть a) децентрализованной b) иерархической c) централизованной 23. Конечная цель защиты информации a) уменьшение возможных точек атак b) сведение к минимуму потерь в

		управлении c) формирование системы информационной безопасности d) минимизация риска 24. Понятие безопасность информации шире, чем понятие информационная безопасность a) да b) нет 25. Наиболее часто нарушения информационной безопасности происходят a) От действий хакеров b) От действий кракеров c) По неопытности персонала 26. Что входит в понятие “безопасность информации” a) исключение ознакомления с информацией сотрудников АСОИ b) предотвращение ознакомления с информацией лиц к ней не допущенных c) исключение изменений информации d) исключение утечки информации за счет излучений и наводок 27. Конфиденциальность информации обеспечивается путем a) содержания критической информации в секрете b) ограничения доступа в специальные помещения c) организации мониторинга сети
	Владеет: навыками практического применения программного обеспечения для решения профессиональных задач, требующих работы с информацией; навыками соблюдения требований информационной безопасности.	**Выполнение практических заданий по темам (разделам):** **Раздел 1. Защита информации. Место информационной безопасности в национальной безопасности РФ.** Тема 1.1 Цели и задачи информационной безопасности. Тема 1.2. Построение системы защиты информации (СЗИ) в организации. Тема 1.3. Современные методики анализа и управления рисками информационной безопасности. **Раздел 2. Информационная безопасность, как основа стабильности организации.** Тема 2.1 Криптографическая защита информации. Тема 2.2. Программы, обеспечивающие защиту информации.

6.3. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Для оценивания результатов промежуточной аттестации применяется шкала оценивания, включающая следующие оценки: «зачтено», «не зачтено».

Зачет. Критерии выставления оценок

Допуск к зачету осуществляется на основании посещаемости обучающимся аудиторных занятий и успешном освоении материалов лекций и семинаров.

Знания обучающихся оцениваются путем выставления по результатам ответа обучающегося итоговой оценки «зачтено», либо «не зачтено».

Оценка «зачтено» при приеме зачета выставляется в случае:

- полного и правильного изложения обучающимся учебного материала по каждому из вопросов;
- самостоятельной подготовки обучающегося к ответу в установленные для этого сроки, исключающей использование нормативных источников, основной и дополнительной литературы, конспектов лекций и иного вспомогательного материала, кроме случаев специального указания или разрешения преподавателя;
- владения обучающимся понятийно-категориальным аппаратом;
- логически последовательного, взаимосвязанного и правильно структурированного изложения обучающимся учебного материала, умения устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь;
- приведения обучающимся надлежащей аргументации, наличия у обучающегося логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам;
- лаконичного и правильного ответа обучающегося на дополнительные вопросы преподавателя.

Оценка «зачтено» может быть выставлена также при соблюдении вышеперечисленных требований в основном, без существенных ошибок и пробелов при изложении обучающимся учебного материала, приведении ссылок на нормативно-правовые акты, а также на их отдельные принципиально значимые положения.

Оценка «не зачтено» при приеме зачета выставляется в случае:

- отказа обучающегося от ответа по билету с указанием, либо без указания причин;
- невозможности изложения обучающимся учебного материала по одному или всем вопросам;
- допущения обучающимся существенных ошибок при изложении учебного материала по одному или всем вопросам;
- не владения обучающимся понятийно-категориальным аппаратом;
- невозможность обучающегося дать ответы на дополнительные вопросы преподавателя.

Любой из указанных недостатков может служить основанием для выставления обучающемуся оценки «не зачтено».

Дополнительные вопросы могут быть заданы обучающимся в случаях:

- необходимости конкретизации информации по вопросам с целью проверки глубины знаний отвечающего по связанным между собой темам и проблемам;
- необходимости проверки знаний отвечающего по основным темам и проблемам курса при недостаточной полноте его ответа по вопросам билета.

В случае, когда промежуточная аттестация проводиться в форме тестирования:

«Зачтено» обучающиеся получают в том случае, если верные ответы составляют от 50% до 100% от общего количества

«Не зачтено» обучающиеся получают в том случае, если верные ответы на тест составляют менее 50 %.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276557 – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.

2. Основы информационной культуры личности : учебно-методический комплекс дисциплины по направлению подготовки 510306 (071900.62) «Библиотечно-информационная деятельность», квалификация (степень) выпускника «бакалавр» / составители Н. И. Гендина, Г. А. Стародубова, Л. Н. Рябцева. — Кемерово : Кемеровский государственный институт культуры, 2015. — 212 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/55802.html — Режим доступа: для авторизир. пользователей.

Дополнительная литература:

1. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. – 3-е изд., стер. – Москва : Флинта, 2016. – 269 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93245 – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.

2. Ефремов, И.В. Информационные технологии в сфере безопасности: практикум / И.В. Ефремов, В.А. Солопова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». – Оренбург : ОГУ, 2013. – 116 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=259178 – Текст : электронный.

3. Лазарева, Л.И. Информационная культура социального педагога: структура, правила подготовки и оформления результатов самостоятельной учебной и профессиональной деятельности / Л.И. Лазарева ; Министерство культуры Российской Федерации, ФГБОУ ВПО «Кемеровский государственный университет культуры и искусств», Институт социально-культурных технологий, Кафедра социальной педагогики. – Кемерово : КемГУКИ, 2014. – 183 с. : табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=275373 – Текст : электронный.

3. Сергеева, Ю.С. Библиотечное дело и библиотековедение / Ю.С. Сергеева. – Москва : Приор-издат, 2009. – 171 с. – (Конспект лекций. В помощь студенту). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=72786 – Текст :

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", информационных справочных систем и профессиональных баз данных, необходимых для освоения дисциплины

1. http://biblioclub.ru/ – электронная библиотечная система «Университетская библиотека Онлайн»
2. http://www.iprbookshop.ru/ – электронная библиотечная система IPR BOOKS
3. Справочная правовая система Консультант Бизнес: Версия Проф

Справочно-поисковые системы:

Российская государственная библиотека. – Режим доступа: https://www.rsl.ru/

Российская национальная библиотека. – Режим доступа: http://nlr.ru

Государственная публичная научно-техническая библиотека (ГПНТБ) России. – Режим доступа: http://www.gpntb.ru/

Библиотека Конгресса США. – Режим доступа: http://loc.gov

Британская библиотека. – Режим доступа: http://blpc.bl.uk

Центральная государственная публичная библиотека им. В.В. Маяковского. – Режим http://www.pl.spb.ru/

Президентская библиотека им. Б.Н. Ельцина – Режим доступа: https://www.prlib.ru/

Информационное агентство «Интегрум-Техно». – Режим доступа: https://integrum.ru/

Профессиональные ресурсы и базы данных:

Государственный научно-исследовательский институт информационных технологий и телекоммуникаций http://www.informika.ru/

Поисковая система Google. – Режим доступа: https://www.google.ru/

Поисковая система Yandex. – Режим доступа: https://yandex.ru/

Федеральный портал «Российское образование» http://edu.ru/

9. Лицензионное программное обеспечение

- Notepad++ 7.5.8
- Dr.Web Desktop Security Suite (Комплексная защита)
- MS Windows 7 Профессиональная
- MS Windows 10 Pro
- MS Office 2010
- VS Office 2013
- MS Office 2016

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

В зависимости от вида проводимых учебных занятий и форм осуществления образовательной деятельности по соответствующей образовательной программе используется следующее материально-техническое обеспечение дисциплины:

- лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном и имеющие выход в Интернет);
- специализированные помещения для проведения практических занятий по дисциплине – компьютерные классы с демонстрационно-обучающими и обучающе-контролирующими возможностями, доступом к базам данных и Интернет;
- помещения для проведения семинарских и практических занятий (с типовым оборудованием, обеспечивающим применение современных информационных технологий и наглядными пособиями);
- библиотека (имеющая читальные залы и рабочие места для студентов, оснащенные компьютерами с доступом к базам данных и Интернет).

Для инвалидов и лиц с ограниченными возможностями здоровья форма проведения занятий по дисциплине устанавливается образовательной организацией с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья. При определении формы проведения занятий с обучающимся-инвалидом образовательная организация должна учитывать рекомендации, данные по результатам медико-социальной экспертизы, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда. При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности. При необходимости обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.