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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

Направление подготовки/Специальность **38.03.06 Торговое дело**

Квалификация выпускника **Бакалавр**

Направленность (профиль) **Торговое дело**

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 4 зачетные единицы.

3. Содержание дисциплины, структурированное по темам (разделам)

Раздел 1. 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. Перспективные направления в области информационной безопасности.

Тема 2.3. 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

Лекция 1. 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.

Лекция 2. 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.

Лекция 3. 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.

Лекция 4. 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.

Лекция 5. Тема 2.2 Перспективные направления в области информационной безопасности.

Стеганографические методы защиты информации. Обобщенная модель стегосистемы.

Классификация современных стеганографических методов защиты информации.

Цифровые водяные знаки (ЦВЗ). Области применения и особенности аутентификации сообщений с использованием ЦВЗ.

Методологические и практические проблемы обеспечения информационной безопасности в современном обществе.

Лекция 6. Тема 2.3. 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 Перспективные направления в области информационной безопасности.

Применение стеганографических методов защиты информации.

Тема 2.3. 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.

Тема 2.2 Перспективные направления в области информационной безопасности.

Классификация современных стеганографических методов защиты информации.

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. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Что такое смарт-карты?
34. Какие требования предъявляются к современным криптографическим системам защиты информации?
35. Что такое симметричная криптосистема?
36. Какие виды симметричных криптосистем существуют?
37. Что такое асимметричная криптосистема?

38. Что понимается под односторонней функцией?
39. Как классифицируются криптографические алгоритмы по стойкости?
40. В чем заключается анализ надежности криптосистем?
41. Что такое дифференциальныйкриптоанализ?
42. В чем сущность криптоанализа со связанными ключами?
43. В чем сущность линейногокриптоанализа?
44. Какие атаки изнутри вы знаете?
45. Какая программа называется логической бомбой?
46. Какими способами можно проверить систему безопасности?
47. Что является основными характеристиками технических средств защиты информации?
48. Какие требования предъявляются к автоматизированным системам защиты третьей группы?
49. Какие требования предъявляются к автоматизированным системам защиты второй группы?
50. Какие требования предъявляются к автоматизированным системам защиты первой группы?
51. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52. Какие требования предъявляются к межсетевым экранам?
53. Какие имеются показатели защищенности межсетевых экранов?
54. Какие атаки системы снаружи вы знаете?
55. Какая программа называется вирусом?
56. Какая атака называется атакой отказа в обслуживании?
57. Какие виды вирусов вы знаете?
58. Какие вирусы называются паразитическими?
59. Как распространяются вирусы?
60. Какие методы обнаружения вирусов вы знаете?
61. Какая программа называется монитором обращения?
62. Что представляет собой домен?
63. Как осуществляется защита при помощи ACL-списков?
64. Какой список называется перечнем возможностей?
65. Какие способы защиты перечней возможностей вы знаете?
66. Из чего состоит высоконадежная вычислительная база (TCB)?
67. Какие модели многоуровневой защиты вы знаете?
68. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70. Какие задачи решает система компьютерной безопасности?
71. Какие пути защиты информации в локальной сети существуют?
72. Какие задачи решают технические средства противодействия экономическому шпионажу?

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 – 1)

Код и формулировка компетенции	Индикаторы достижения компетенций
ОПК- 1 - 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 и передачи информации; основные понятия, связанные с компьютерной техникой, компьютерными сетями, программно-информационными системами; основами современного программирования, основные требования информационной безопасности;
	Умеет: работать с современными техническими средствами получения, хранения, обработки и передачи информации; решать стандартные задачи в профессиональной деятельности с использованием информационно-коммуникационных технологий;
	Владеет: навыками использования современных средств коммуникации и технических средств; навыками управления информационными системами и применения информационных систем при решении профессиональных задач.

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

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

Темы докладов-презентаций

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.

Тест

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) Принцип комплексного использования СЗИ заключается в
a) организации пропускного режима на предприятие
b) использовании всего арсенала средств защиты
c) защите информации на всех этапах ее обработки
d) защите информации во всех элементах АСОИ
2) Система информационной безопасности включает в себя
a) средства защиты
b) службу информационной безопасности
c) совокупность нормативно-правовых документов
d) систему управления информационной безопасностью
3) Какие преимущества дает построение СИСТЕМЫ ЗИ
a) возможность перераспределения вычислительных ресурсов
b) повышение уровня подготовки персонала АСОИ
c) появление системных свойств
d) упрощение способов решения задач ЗИ
4) Особенности защиты информации в сетях ЭВМ
a) расширение зоны контроля
b) комбинация различных программно-аппаратных средств.
c) большое количество ПЭВМ
d) сложность определения границ сети
5) Каждый узел сети должен иметь
a) универсальную защиту
b) индивидуальную защиту в зависимости от выполняемых функций
c) защиту от НСД
6) Защита сети как единой системы складывается из
a) мер защиты каждого отдельного узла
b) маршрутизации сообщений
c) функций защиты протоколов данной сети
7) Факторы, определяющие качество управления
a) рациональная структура и профессиональная подготовленность СИБ

b) качество исходной информации
c) эффективность средств управления защитой информации
d) отношение руководства к проблемам защиты информации
8) Состав и размеры группы безопасности (СИБ) зависят от
a) структуры конкретного предприятия
b) количества и степени конфиденциальности защищаемой информации
c) качества средств защиты информации
d) наличия финансирования на цели защиты информации
9) 16. Штатный состав службы информационной безопасности
a) не должен иметь обязанностей, связанных с функционированием АС
b) может совмещать функции обслуживания АСОИ и ее защиты
10) Анализ риска проводится после планирования защиты информации
a) да
b) нет
11) Нужно ли учитывать возможность сбоя оборудования при организации защиты информации
a) да
b) нет
12) Влияют ли стихийные бедствия на безопасность информации
a) да
b) нет
13) Хэш-функция осуществляет
a) архивирование документов
b) сжатие документов
14) Значение хэш-функции зависит от
a) применяемого языка
b) структуры документа
c) наличия подписи в документе
15) Хэш-функция должна
a) быть чувствительной к изменениям в тексте
b) обладать свойством необратимости
c) предотвращать несанкционированный доступ к документу

Вариант 4

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

Вариант 5

1) Открытость СЗИ это
a) обеспечение доступа к любым ресурсам
b) возможность включения доп. средств защиты
c) прозрачность СЗИ для пользователей
2) Экономическая эффективность СЗИ определяется
a) предотвращенным ущербом
b) совокупной стоимостью средств защиты информации
c) соотношением затрат на СЗИ и предотвращенным ущербом
3) 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
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) Скрытность управления защитой информации
a) способность воспрепятствовать в выявлении организации ЗИ
b) прозрачность для пользователей системы защиты информации
c) легендирование деятельности организации
8) Оперативность управления защитой информации это способность
a) своевременно реагировать на действия злоумышленников
b) адекватно реагировать на действия злоумышленников
c) реализовывать управленческие решения к заданному сроку.

9) Обоснованность управления защитой информации обеспечивается
a) качеством плана защиты информации
b) всесторонним учетом условий решения поставленной задачи
c) применением моделей, расчетных и информационных задач
d) экспертных систем и опыта в области защиты информации
10) Какие информационные ресурсы относятся к интеллектуальной собственности
a) Перечень должностей организации
b) Профиль научных исследований
c) Список клиентов банка
d) Список сотрудников учреждения
11) Основные этапы анализа риска
a) Определение границ управления информационной безопасностью
b) Разработка модели нарушителя
c) Анализ риска
d) Разработка плана защиты
12) С чего начинается создание системы защиты информации
a) Анализа рынка услуг по защите информации
b) Формирования службы информационной безопасности
c) Определения интеллектуальной собственности организации
13) Аутентификация направлена на установление факта, что
a) информация получена законным получателем
b) информация принята законным пользователем
c) информация не была искажена
14) Аутентификация производится на основании
a) цифровой подписи
b) кодирования информации
c) внутренней структуры документа
15) Какие типы задач решаются в процессе аутентификации
a) аутентификация абонента
b) аутентификация нарушителя
c) аутентификация документа
d) аутентификация принадлежности абонента к заданной группе

Вариант 6

1) Основные направления защиты информации
a) информационное
b) организационно-правовое
c) инженерно-техническое
d) лингвистическое
2) Инженерно-техническое включает в себя
a) аппаратные средства
b) средства сканирования системы обработки информации
c) программные средства
d) средства аутентификации
3) Какие параметры могут быть включены в “профиль” пользователя
a) физиологические характеристики

b) продолжительность сеанса работы
c) время начала (окончания) сеанса работы
d) биометрические характеристики
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) Непосредственная цель управления информационной безопасностью
a) разработка плана защиты и его реализация
b) выработка и реализация своевременных и обоснованных решений
c) организация доступа к критичной информации
d) реализация принятой политики безопасности
8) Основными свойствами управления безопасностью информации являются:
a) Устойчивость
b) Непрерывность
c) Скрытность
d) Оперативность
9) Устойчивость управления обеспечивается
a) надежностью программно-аппаратных средств
b) стойкостью к стихийным бедствиям
c) наличием средств управления
d) защищенностью каналов передачи информации
10) Цель определения границ информационной безопасности
a) Определение основных элементов АСОИ
b) Выявление возможных атак на информационный объект
c) Анализ информационных связей между объектами
11) Какие элементы входят в состав информационной системы
a) Технические средства
b) Информационные ресурсы
c) Технологии обработки информации
d) Операторы системы
12) Основной источник (причина) нарушений информационной безопасности
a) Несовершенство законодательной базы
b) Развитие средств шпионажа
c) Сотрудники организации
d) Усложнение средств вычислительной техники
13) Планирование это

a) Процесс согласования мероприятий по защите информации между отделами и службами

b) Процесс разработки пакета документов по реализации политики безопасности

c) Назначение сроков и ответственных за монтаж и наладку средств защиты информации

14) Какие две группы мероприятий включает план защиты

a) Установка системы защиты

b) Допуск на объект

c) Использование системы защиты

d) Защита от НСД

15) Цель планирования

a) Координация деятельности всех служб и отделов, “причасных” к обеспечению защиты информации

b) Использование всех имеющихся ресурсов

c) Исключение грубых ошибок

d) Разработка плана поставок оборудования

Вариант 7

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) . Какие факторы наиболее опасны для информационной безопасности

a) Внутренние

b) Внешние

11) Цели, которые преследуют злоумышленники

a) Внести изменения в информацию

b) Получить интересующую их информацию

c) Уничтожить материальные ценности

12) Самый высокий ущерб от действий

a) Хакеров

b) Кракеров

c) По неопытности

13) Какие две группы мероприятий включает план защиты

a) Установка системы защиты

b) Допуск на объект

c) Использование системы защиты

d) Защита от НСД

14) Цель планирования

a) Координация деятельности всех служб и отделов, “причасных” к обеспечению защиты информации

b) Использование всех имеющихся ресурсов

c) Исключение грубых ошибок

d) Разработка плана поставок оборудования

15) Виды планирования

a) Перспективное (стратегическое)

b) Текущее (тактическое)

c) оперативное

Вариант 8

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) 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) Управление информационной безопасностью это процесс
a) взаимодействия всех подразделений по защите информации
b) целенаправленного воздействия на объект по заданной программе
c) способ реализации политики безопасности
d) предотвращения нарушений компьютерной безопасности
8) Информационная безопасность и безопасность информации понятия одинаковые
a) да
b) нет
9) Понятие безопасность информации шире, чем понятие информационная безопасность
a) да
b) нет
10) Наиболее часто нарушения информационной безопасности происходят
a) От действий хакеров
b) От действий кракеров
c) По неопытности персонала
11) Что такое сценарий действий по нарушению информационной безопасности
a) Модель нарушителя
b) Совокупность способов проникновения на объект, доступа к информационным ресурсам и использования их в конкурентной борьбе
c) Способы снятия информации с каналов утечки
12) Основные виды технических каналов утечки информации
a) акустический

b) вибрационный
c) электромагнитный
d) визуально-оптический
13) Какие мероприятия плана защиты относятся к разовым
(a) Мероприятия по эксплуатации системы защиты
(b) Контроль за действиями персонала
(c) Определение контролируемой зоны
(d) Анализ системного журнала
14) Какие из перечисленных мероприятий относятся к периодически проводимым
a) Распределение реквизитов разграничения доступа
b) Определение порядка хранения, выдачи и использования документов и носителей конфиденциальной информации
c) Мероприятия по эксплуатации системы защиты
15) Какие из перечисленных мероприятий относятся к проводимым по необходимости
a) Анализ и проверка эффективности СЗИ
b) Мероприятия, осуществляемые при строительстве объекта
c) Мероприятия, проводимые при модернизации СВТ и ПО

Вариант 9

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) Способы борьбы с проникновением на объект защиты
a) система охранной сигнализации
b) порядок приема на работу
c) система видеонаблюдения
d) организация проходного режима
5) Политика информационной безопасности это
a) совокупность технических средств защиты информации
b) концептуальный замысел на построение СЗИ
c) организационно-правовые мероприятия по ЗИ
d) планирующий документ по защите информации
6) Информационная безопасность информации достигается обеспечением

a) конфиденциальности
b) доступности
c) комплексирования средств ЗИ
d) целостности информации
7) Учет места и времени действий злоумышленника позволит
a) конкретизировать его возможности по доступу к информационным ресурсам
b) учесть их для повышения качества системы защиты информации
c) выявить точки риска
8) Главное требование к модели нарушителя
a) адаптация к конкретному объекту защиты
b) краткость
c) наглядность
9) Модель нарушителя это
a) одна модель универсального нарушителя
b) совокупность моделей действий нарушителя
c) действия нарушителя по наиболее уязвимым точкам сети
10) Основные составляющие канала утечки информации
a) среда
b) охраняемые границы объекта
c) передатчик
d) приемник
11) Цель оценки вероятности информационного контакта
a) выявление каналов утечки информации
b) изменение параметров характеристик, определяющих величину вероятности установления информационного контакта
c) формирование модели нарушителя
12) К непосредственным потерям относится
a) подрыв репутации
b) замена оборудования
c) ослабление позиций на рынке
13) Что представляет собой план защиты
a) Совокупность технических и программных средств защиты информации
b) План размещения и функциональное предназначение средств защиты
c) Пакет вербально - графических документов по обеспечению информационной безопасности
d) Организационно-методические рекомендации по реализации политики безопасности
14) Основное требование к плану защиты
a) Подробность изложения основных положений
b) Персональная ответственность за каждое направление обеспечения информационной безопасности
c) Качество оформления
15) Когда осуществляется планирование защиты информации
a) По мере поставки средств защиты
b) В процессе выявления атакуемых точек в АСОИ
c) После проведения анализа риска и потерь

Вариант 10

1) Принцип комплексного использования СЗИ заключается в
a) организации пропускного режима на предприятие
b) использовании всего арсенала средств защиты
c) защите информации на всех этапах ее обработки
d) защите информации во всех элементах АСОИ
2) Система информационной безопасности включает в себя
a) средства защиты
b) службу информационной безопасности
c) совокупность нормативно-правовых документов
d) систему управления информационной безопасностью
3) Какие преимущества дает построение СИСТЕМЫ ЗИ
a) возможность перераспределения вычислительных ресурсов
b) повышение уровня подготовки персонала АСОИ
c) появление системных свойств
d) упрощение способов решения задач ЗИ
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) К категории внутренних нарушителей относятся
a) пользователи (операторы) системы
b) хакеры
c) прикладные и системные программисты
d) администраторы
8) Самый опасный вид нарушителя
a) Клиенты
b) Конкуренты
c) Посетители
9) Самой опасной категорией потенциальных нарушителей сети является
a) Программисты
b) Администраторы безопасности
c) Технический персонал
10) К косвенным потерям относится
a) потеря клиентуры

b) восстановление информации в АСОИ

c) снижение банковского доверия

11) Виды стратегий управления рисками

a) уклонение от рисков

b) изменение характера риска

c) уменьшение рисков

d) принятие рисков

12) Как можно поступить в случае недостатка вычислительных ресурсов на нужды защиты информации

a) использовать средства защиты с определенной периодичностью

b) использовать принципы ситуационного управления

c) согласовывать возможности средств защиты с имеющимися ресурсами

13) Что представляет собой план защиты

a) Совокупность технических и программных средств защиты информации

b) План размещения и функциональное предназначение средств защиты

c) Пакет вербально - графических документов по обеспечению информационной безопасности

d) Организационно-методические рекомендации по реализации политики безопасности

14) Основное требование к плану защиты

a) Подробность изложения основных положений

b) Персональная ответственность за каждое направление обеспечения информационной безопасности

c) Качество оформления

15) Когда осуществляется планирование защиты информации

a) По мере поставки средств защиты

b) В процессе выявления атакуемых точек в АСОИ

c) После проведения анализа риска и потерь

d) После выбора контрмер и средств, обеспечивающих их реализацию

Вариант 11

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) По уровню подготовки нарушитель
a) является специалистом высшей квалификации
b) является специалистом средней квалификации
c) является специалистом низшей квалификации
8) На персонал АСОИ приходится % нарущений
a) 50-60
b) 75-80
c) 30-40
9) К категории внешних нарушителей относятся
a) посетители
b) конкуренты
c) технический персонал
d) преступные организации
10) В чем заключается принцип ситуационного управления вычислительными ресурсами в интересах защиты информации
a) в распределении вычислительных ресурсов в соответствии с возможными потерями и складывающейся обстановкой
b) в равномерном распределении вычислительных ресурсов на отражение всех возможных атак
c) в выделении вычислительных ресурсов на основные виды угроз
11) Главное условие успешности подключения новых средств
a) возможность отражения новых атак
b) совместимость с имеющимися средствами защиты
c) наличие достаточных вычислительных ресурсов
12) Чем определяется сложность оценки эффективности системы защиты информации
a) выбором показателей эффективности
b) взаимосвязью показателей эффективности функционирования системы защиты информации
c) противоречивостью ряда показателей
d) отсутствием методик расчета показателей
13) Что представляет собой план защиты
a) Совокупность технических и программных средств защиты информации
b) План размещения и функциональное предназначение средств защиты

c) Пакет вербально - графических документов по обеспечению информационной безопасности

d) Организационно-методические рекомендации по реализации политики безопасности

14) Основное требование к плану защиты

a) Подробность изложения основных положений

b) Персональная ответственность за каждое направление обеспечения информационной безопасности

c) Качество оформления

15) Когда осуществляется планирование защиты информации

a) По мере поставки средств защиты

b) В процессе выявления атакуемых точек в АСОИ

c) После проведения анализа риска и потерь

d) После выбора контрмер и средств, обеспечивающих их реализацию

Вариант 12

1) Открытость СЗИ это

a) обеспечение доступа к любым ресурсам

b) возможность включения доп. средств защиты

c) прозрачность СЗИ для пользователей

2) Экономическая эффективность СЗИ определяется

a) предотвращенным ущербом

b) совокупной стоимостью средств защиты информации

c) соотношением затрат на СЗИ и предотвращенным ущербом

3) 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

4) В чем преимущества сетевой топологии” звезда”

a) Легкость подключения новых устройств без реконфигурации сети

b) Центральный узел может осуществлять коммутацию каналов, сообщений и пакетов

c) Каждый узел имеет равноправные возможности для передачи сообщения.

5) В чем недостатки сетевой топологии кольцо

a) при добавлении нового узла требуется реконфигурация сети

b) передача сообщения через другие узлы

c) широковещательные передачи невозможны

d) в случае сбоя на центральном узле вся сеть выходит из строя

6) Достоинства топологии “шина”

a) нет центрального узла

b) разрыв шины, изоляция одного устройства не влияют на работу остальных

c) легкость расширения.

7) Основной способ уменьшения конфликтов иерархии

a) установление "обезличенной" власти

b) создание определенного порядка приема на работу

c) продвижение сотрудников по служебной лестнице

8) К чему может привести конфликт “человек-машина”

a) профессиональные отклонения здоровья

b) стрессовые состояния

c) месть

9) Рекомендации по недопущению конфликта “человек-машина”

a) установление рационального режима труда и отдыха операторов

b) чередование различных операций или форм деятельности

c) рациональное распределение функций между человеком и СВТ

10) Какие методы наиболее приемлемы для оценки эффективности систем защиты информации

a) экспертные методы

b) методы сетевого планирования

c) методы многокритериальной оценки эффективности

d) методы линейного и динамического программирования

11) Цель тестирования на проникновение

a) оценка средств обеспечения доступа к информации

b) предоставление гарантий на отсутствие простых путей обхода механизмов защиты

c) анализ возможностей НСД

12) Какой из перечисленных способов нарушения информационной безопасности имеет самый низкий рейтинг

a) подкуп, шантаж, переманивание служащих

b) проникновение в ПЭВМ

c) кража документов

d) съем информации с каналов связи

13) Основные элементы плана защиты информации

a) Положение о защите информации

b) Положение о коммерческой тайне

c) План обеспечения непрерывности работы АСОИ и восстановления информации

d) Договор о порядке обмена электронными документами

14) Элементом какого документа из Плана защиты информации является Перечень сведений, составляющих коммерческую тайну

a) Положение о защите информации

b) Положение о коммерческой тайне

c) План обеспечения непрерывности работы АСОИ и восстановления информации

d) Договор о порядке обмена электронными документами

15) Элементом какого документа из Плана защиты информации является перечень и классификация возможных критическихситуаций

a) Положение о защите информации

b) Положение о коммерческой тайне

c) План обеспечения непрерывности работы АСОИ и восстановления информации

d) Договор о порядке обмена электронными документами

Вариант 13

1) Основные направления защиты информации

a) информационное
b) организационно-правовое
c) инженерно-техническое
d) лингвистическое

2) Инженерно-техническое включает в себя
a) аппаратные средства
b) средства сканирования системы обработки информации
c) программные средства
d) средства аутентификации

3) Какие параметры могут быть включены в “профиль” пользователя
a) физиологические характеристики
b) продолжительность сеанса работы
c) время начала (окончания) сеанса работы
d) биометрические характеристики

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) . Чем чреваты конфликты, обусловленные ограниченностью ресурсов (вычислительных или информационных)
a) восполнение информации слухами
b) появление служебных интриг
c) отклонениями в состоянии здоровья

8) Рекомендации по недопущению конфликтов, обусловленных ограниченностью ресурсов
a) подписание контрактов при приеме на работу
b) грамотная мотивация
c) формирование общей миссии организации

9) Виды конфликтов иерархии:
a) "равный-равный"
b) "высший-низший"
c) отделов автоматизации и защиты информации
d) формальной и неформальной структур руководства

10) Среднестатистические потери в результате компьютерных преступлений составляют
a) 1 2000 000 $
b) 500 000 $
c) 60 000 $

d) 300 000 $

11) Что можно сделать с оставшимся в результате создания системы информационной безопасности риском

a) проявлять наибольшее внимание к возможным атакам

b) застраховать риск

c) распределять ресурсы защиты на появляющиеся во времени риски

d) принять меры по ликвидации последствий возможных нападений

12) Какие риски в банках страхуются западными компаниями

a) ввод мошеннически подготовленных или видоизмененных данных, или команд в компьютерные сети банка, системы перевода средств или связи с клиентами, в том числе во время передачи данных;

b) умышленное уничтожение или кража, воровство электронных данных и их носителей;

c) вирусные атаки;

d) осуществление платежей на основании сфальсифицированных поручений клиентов, передаваемых по системам электронной, тестированной телексной, факси-мильной или телефонной связи.

13) Элементом какого документа из плана защиты информации является Инструкция администратора безопасности

a) Положение о защите информации

b) Положение о коммерческой тайне

c) План обеспечения непрерывности работы АСОИ и восстановления информации

d) Договор о порядке обмена электронными документами

14) Элементом какого документа из плана защиты информации является Порядок проведения конфиденциальных переговоров

a) Положение о защите информации

b) Положение о коммерческой тайне

c) План обеспечения непрерывности работы АСОИ и восстановления информации

d) Договор о порядке обмена электронными документами

15) Элементом какого документа из плана защиты информации является Порядок подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов

a) Положение о защите информации

b) Положение о коммерческой тайне

c) План обеспечения непрерывности работы АСОИ и восстановления информации

d) Договор о порядке обмена электронными документами

Вариант 14

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) Особенности защиты информации в сетях ЭВМ
a) расширение зоны контроля
b) комбинация различных программно-аппаратных средств.
c) большое количество ПЭВМ
d) сложность определения границ сети
5) Каждый узел сети должен иметь
a) универсальную защиту
b) индивидуальную защиту в зависимости от выполняемых функций
c) защиту от НСД
6) Защита сети как единой системы складывается из
a) мер защиты каждого отдельного узла
b) маршрутизации сообщений
c) функций защиты протоколов данной сети
7) Известными способами сбора сведений являются*:*
a) подбор соучастников
b) анализ периодических изданий, ведомственных бюллетеней
c) перехват сообщений электронной почты, подслушивание разговоров
d) организация краж.
8) К чему приводят ограничения, связанные с требованиями режима
a) нахождение в специальных помещениях
b) ограничение свободы перемещения и публикаций
c) увеличение времени работы
9) Основной способ уменьшения конфликтов, вызванных требованиями режима
a) стимулирование
b) воспитательная работа
c) снятие напряжения
10) Что можно сделать с оставшимся в результате создания системы информационной безопасности риском
a) проявлять наибольшее внимание к возможным атакам
b) застраховать риск
c) распределять ресурсы защиты на появляющиеся во времени риски
d) принять меры по ликвидации последствий возможных нападений
11) Какие риски в банках страхуются западными компаниями
a) ввод мошеннически подготовленных или видоизмененных данных, или команд в компьютерные сети банка, системы перевода средств или связи с клиентами, в том числе во время передачи данных;
b) умышленное уничтожение или кража, воровство электронных данных и их носителей;
c) вирусные атаки;

d) осуществление платежей на основании сфальсифицированных поручений клиентов, передаваемых по системам электронной, тестированной телексной, факсимильной или телефонной связи.

12) Какие мероприятия являются определяющими в обеспечении информационной безопасности

a) финансирование
b) организационные мероприятия
c) программно-аппаратные
d) правовые

13) Элементом какого документа из плана защиты информации является Инструкция пользователю по соблюдению режима информационной безопасности

a) Положение о защите информации
b) Положение о коммерческой тайне
c) План обеспечения непрерывности работы АСОИ и восстановления информации
d) Договор о порядке обмена электронными документами

14) Элементом какого документа из плана защиты информации является Материалы обоснования предложений экспертной комиссии по включению сведений в развернутый перечень

a) Положение о защите информации
b) Положение о коммерческой тайне
c) План обеспечения непрерывности работы АСОИ и восстановления информации
d) Договор о порядке обмена электронными документами

15) Является ли План защиты элементом управления системой информационной безопасности

a) да
b) нет

Ключи ответов

Вариант 1

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b,c,d	a	a,c,d	a,b,d	a,b	a	a	c	a,c,d	b,c,d	a,b	a,b	a,c,d	b,c,d	a

Вариант 2

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b	b,d	a,b,d	a,c	b,d	a,c,d	a,b,c	b,c	a,b	a,b,c	a,b	b,c,d	b	a,b	d

Вариант 3

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b,c,d	a,b,d	a,b	a,b,d	b	a,c	a,b,c	a,b,d	a,b,d	b	a	a	b	b	a,b

Вариант 4

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	c	a,b,c	a,c	b,c	a,b	a,b,c	c	b	a,c,d	b	a	a	a,b,c	a,c	b,c,d

Вариант 5

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b,c,d	a	a,c,d	a,b,d	a,b	a	a	c	a,c,d	b,c,d	a,b	a,b	a,c,d	b,c,d	a

Вариант 6

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b	b,d	a,b,d	a,c	b,d	a,c,d	a,b,c	b,c	a,b	a,b,c	a,b	b,c,d	b	a,b	d

Вариант 7

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b,c,d	a,b,d	a,b	a,b,d	b	a,c	a,b,c	a,b,d	a,b,d	b	a	a	b	b	a,b

Вариант 8

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	c	a,b,c	a,c	b,c	a,b	a,b,c	c	b	a,c,d	b	a	a	a,b,c	a,c	b,c,d

Вариант 9

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b,c,d	a	a,c,d	a,b,d	a,b	a	a	c	a,c,d	b,c,d	a,b	a,b	a,c,d	b,c,d	a

Вариант 10

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b	b,d	a,b,d	a,c	b,d	a,c,d	a,b,c	b,c	a,b	a,b,c	a,b	b,c,d	b	a,b	d

Вариант 11

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b,c,d	a,b,d	a,b	a,b,d	b	a,c	a,b,c	a,b,d	a,b,d	b	a	a	b	b	a,b

Вариант 12

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Номер ответа	c	a,b,c	a,c	b,c	a,b	a,b,c	c	b	a,c,d	b	a	a	a,b,c	a,c	b,c,d

Вариант 13

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b,c,d	a	a,c,d	a,b,d	a,b	a	a	c	a,c,d	b,c,d	a,b	a,b	a,c,d	b,c,d	a

Вариант14

Номер задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Номер ответа	b	b,d	a,b,d	a,c	b,d	a,c,d	a,b,c	b,c	a,b	a,b,c	a,b	b,c,d	b	a,b	d

Примерные задания для проведения промежуточной аттестации по дисциплине

Список экзаменационных 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 диктафонов.

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.

6.3. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Для оценивания результатов промежуточной аттестации применяется шкала оценивания, включающая следующие оценки: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Экзамен. Критерии выставления оценок

На экзамен выносятся вопросы, охватывающие все содержание учебной дисциплины.

Знания обучающихся оцениваются путем выставления по результатам ответа обучающегося итоговой оценки «отлично», либо «хорошо», либо «удовлетворительно», либо «неудовлетворительно».

Оценка «отлично» при приеме экзамена выставляется в случае:

- полного, правильного и уверенного изложения обучающимся учебного материала по каждому из вопросов билета;
- уверенного владения обучающимся понятийно-категориальным аппаратом учебной дисциплины;
- 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 в вопросах билета;
- приведения обучающимся надлежащей аргументации, наличия у обучающегося логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;
- лаконичного и правильного ответа обучающегося на дополнительные вопросы преподавателя.

Оценка «хорошо» при приеме экзамена выставляется в случае:

• недостаточной полноты изложения обучающимся учебного материала по отдельным (одному или двум) вопросам билета при условии полного, правильного и уверенного изложения учебного материала по, как минимум, одному вопросу билета;

• допущения обучающимся незначительных ошибок и неточностей при изложении учебного материала по отдельным (одному или двум) вопросам билета;

• допущения обучающимся незначительных ошибок и неточностей при использовании в ходе ответа отдельных понятий и категорий дисциплины;

• нарушения обучающимся логической последовательности, взаимосвязи и структуры изложения учебного материала по отдельным вопросам билета, недостаточного умения обучающегося устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

• приведения обучающимся слабой аргументации, наличия у обучающегося недостаточно логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;

• допущения обучающимся незначительных ошибок и неточностей при ответе на дополнительные вопросы преподавателя.

Любой из указанных недостатков или их определенная совокупность могут служить основанием для выставления обучающемуся оценки «хорошо».

Оценка «удовлетворительно» при приеме экзамена выставляется в случае:

• невозможности изложения обучающимся учебного материала по любому из вопросов билета при условии полного, правильного и уверенного изложения учебного материала по как минимум одному из вопросов билета;

• допущения обучающимся существенных ошибок при изложении учебного материала по отдельным (одному или двум) вопросам билета;

• допущении обучающимся ошибок при использовании в ходе ответа основных понятий и категорий учебной дисциплины;

• существенного нарушения обучающимся или отсутствия у обучающегося логической последовательности, взаимосвязи и структуры изложения учебного материала, неумения обучающегося устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

• отсутствия у обучающегося аргументации, логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;

• невозможности обучающегося дать ответы на дополнительные вопросы преподавателя.

Любой из указанных недостатков или их определенная совокупность могут служить основанием для выставления обучающемуся оценки «удовлетворительно».

Оценка «неудовлетворительно» при приеме экзамена выставляется в случае:

• отказа обучающегося от ответа по билету с указанием, либо без указания причин;

• невозможности изложения обучающимся учебного материала по двум или всем вопросам билета;

• допущения обучающимся существенных ошибок при изложении учебного материала по двум или всем вопросам билета;

• скрытное или явное использование обучающимся при подготовке к ответу нормативных источников, основной и дополнительной литературы, конспектов лекций и

иного вспомогательного материала, кроме случаев специального указания или разрешения преподавателя;

- невладения обучающимся понятиями и категориями данной дисциплины;
- невозможность обучающегося дать ответы на дополнительные вопросы преподавателя;

Любой из указанных недостатков или их совокупность могут служить основанием для выставления обучающемуся оценки «неудовлетворительно».

Обучающийся имеет право отказаться от ответа по выбранному билету с указанием, либо без указания причин и взять другой билет. При этом с учетом приведенных выше критериев оценка обучающемуся должна быть выставлена на один балл ниже заслуживаемой им.

Дополнительные вопросы могут быть заданы обучающемуся в случае:

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

При проведении промежуточной аттестации в форме тестирования, оценивание результата проводится следующим образом:

«**Отлично**» - получают обучающиеся в том случае, если верные ответы составляют от 80% до 100% от общего количества

«**Хорошо**» - получают обучающиеся в том случае, если верные ответы составляют от 71 до 79% от общего количества;

«**Удовлетворительно**»- получают обучающиеся в том случае, если верные ответы составляют 50 –70 % правильных ответов;

«**Неудовлетворительно**» - работа, содержащая менее 50% правильных ответов.

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. – М.-Берлин: Директ-Медиа, 2015 г. 253 с. - https://biblioclub.ru/index.php?page=book&id=276557

Дополнительная литература:

2. Аверченков В. И. Аудит информационной безопасности: учебное пособие для вузов. – М.: Флинта, 2016 г. - 269 с. https://lib.biblioclub.ru/book_93245_Audit_informatsionnoi_bezopasnosti_uchebnoe_posobie_dlya_vuzov /

3. Ефремов И., Солопова В. Информационные технологии в сфере безопасности : практикум: практикум. – Оренбург: ОГУ, 2013 г. - 116 с. https://lib.biblioclub.ru/book_259178_informatsionnyie_tehnologii_v_sfere_bezopasnosti /

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

1. ЭБС «Университетская библиотека онлайн» https://biblioclub.ru /
2. ЭБС IPR BOOKS - www.iprbookshop.ru
3. СПС «Консультант Плюс»

9. Лицензионное программное обеспечение

- Notepad++ 7.5.8
- Visual Studio Community 2017
- MS Windows 7 Профессиональная
- MS Windows 10 Pro

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

В зависимости от вида проводимых занятий 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.