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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

Направление подготовки 37.03.02 Конфликтология

Квалификация выпускника Бакалавр

Направленность (профиль) Конфликтология

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 3 зачетные единицы.

3. Содержание дисциплины, структурированное по темам (разделам)

Раздел 1. Принципы обеспечения защиты информации. Уровни информационной защиты

Тема 1.1 Понятие безопасности
Тема 1.2 Системы безопасности и их дефекты

Раздел 2. Криптографические системы и криптоанализ

Тема 2.1 Основы криптографии
Тема 2.2 Шифрование с секретным ключом
Тема 2.3 Шифрование с открытым ключом
Тема 2.4 Необратимые функции
Тема 2.5 Цифровые подписи

Раздел 3.

Тема 3.1 Аутентификация пользователей
Тема 3.2 Защита паролей в системе UNIX
Тема 3.3 Совершенствование безопасности паролей

Раздел 4.

Тема 4.1 Атаки системы снаружи
Тема 4.2 Атаки системы изнутри
Тема 4.3 Атака системы безопасности

Раздел 5.

Тема 5.1 Механизмы защиты
Тема 5.2 Перечни возможностей
Тема 5.3 Надежные системы

Раздел 6.

Тема 6.1 Метод «песочниц»
Тема 6.2 Интерпретация
Тема 6.3 Программы с подписями
Тема 6.4 Безопасность в системе Java

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. Принципы обеспечения защиты информации. Уровни информационной защиты

Тема 1.1 Понятие безопасности

Тема 1.2 Системы безопасности и их дефекты

Раздел 2. Криптографические системы и криптоанализ

Тема 2.1 Основы криптографии

Тема 2.2 Шифрование с секретным ключом

Тема 2.3 Шифрование с открытым ключом

Тема 2.4 Необратимые функции

Тема 2.5 Цифровые подписи

Раздел 3.

Тема 3.1 Аутентификация пользователей

Тема 3.2 Защита паролей в системе UNIX

Тема 3.3 Совершенствование безопасности паролей

Раздел 4.

Тема 4.1 Атаки системы снаружи

Тема 4.2 Атаки системы изнутри

Тема 4.3 Атака системы безопасности

Раздел 5.

Тема 5.1 Механизмы защиты

Тема 5.2 Перечни возможностей

Тема 5.3 Надежные системы

Раздел 6.

Тема 6.1 Метод «песочниц»

Тема 6.2 Интерпретация

Тема 6.3 Программы с подписями

Тема 6.4 Безопасность в системе Java

Практические занятия

Задание. Разработать концепцию информационной безопасности компании по следующему примерному плану

1. Цели системы информационной безопасности
2. Задачи системы информационной безопасности.

3. Объекты информационной безопасности.
4. Вероятные нарушители.
5. Основные виды угроз информационной безопасности.
6. Классификация угроз.

a. Основные непреднамеренные искусственные угрозы.
b. Основные преднамеренные искусственные угрозы.

7. Мероприятия по обеспечению информационной безопасности.
8. Средства защиты от потенциальных угроз.

Разработайте вариант политики паролей

Предложите ПО для антивирусной защиты (проведя сравнительный анализ цен, возможностей и прочее)

Семинарские занятия

Вопросы для обсуждения

1. Формы защиты интеллектуальной собственности
2. Конфиденциальная информация
3. Классификация и виды информационных ресурсов
4. Информация ограниченного доступа

Примерные темы дискуссий:

1. Основополагающие документы для обеспечения безопасности внутри организации
2. Какие средства используется на инженерных и технических мероприятиях в защите информации
3. Программные средства
4. Криптографические средства
5. Правовое обеспечение безопасности информации
6. Предпосылки появления угроз

5. Методические рекомендации для обеспечения самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов включает усвоение теоретического материала, подготовку к практическим (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. Под информационной безопасностью понимается...

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре.

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

В) нет правильного ответа

2. Защита информации – это …

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями

пользователей
В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?
А) от компьютеров
Б) от поддерживающей инфраструктуры
В) от информации

4. Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

5. Доступность - это...
А) возможность за приемлемое время получить требуемую информационную услугу.
Б) логическая независимость
В) нет правильного ответа

6. Целостность - это…
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

7. Конфиденциальность - это…
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

8. Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

9. Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

10. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

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

6.1 Планируемые результаты обучения, обеспечивающие достижение планируемых результатов освоения образовательной программы

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	Планируемые результаты обучения по дисциплине
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** основные методы и приемы обеспечения информационной безопасности; методы и средства сбора, обработки, хранения, передачи и накопления информации
	Умеет распознавать опасности и угрозы, возникающие в процессе работы с секретной информацией; применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа информации
	Владеет навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности; навыками обработки конфиденциальной информации, в том числе содержащей государственную тайну, в соответствии со всеми требованиями по защите информации

6.2 Перечень оценочных материалов

Оценочные материалы представляют собой задания для выполнения студентом, 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 учащимися дисциплины, и задания для промежуточной аттестации обучающих, обеспечивающие оценивание промежуточных и окончательных результатов обучения по дисциплине.

Примерные задания для проведения текущего контроля успеваемости

Темы докладов (сообщений)

1. Средства идентификации личности.
2. Классификация датчиков охранной сигнализации.
3. Классификация извещателей.
4. Телевизионные системы наблюдения.
5. Основные средства системы видеоконтроля.
6. Защита личности как носителя информации.
7. Системный подход к защите информации.
8. Параметры системы защиты информации.
9. этапы проектирования системы защиты информации.
10. Потенциальные каналы утечки информации.
11. Этапы разработки мер по предотвращению угроз утечки информации.

Темы рефератов

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Виды угроз безопасности информации.
6. Основные принципы добывания информации.
7. Процедура идентификации, как основа процесса обнаружения объекта.
8. Методы синтеза информации.
9. Методы несанкционированного доступа к информации.

Задания для контрольной работы по вариантам

Вариант 1.

1. Укажите основные свойства VPN
2. Каковы функциональные возможности программы Retina WiFi Scanner
3. 64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности
4. Отметьте потенциально опасные с точки зрения утечек внутренней информации действия
5. Перебор всех слов языка для взлома пароля это
6. Какого типа БД является реестр
7. IDS - это

8. Какие режимы работы имеет программа Iris
9. Используется ли VPN для защиты беспроводных сетей
10. Какие дополнительные меры обеспечения безопасности могут использоваться в беспроводных сетях

Вариант 2

1 Инсайдер - это
2 Сколько root key содержит реестр Windows
3 Решение DeviceLock является
4 Опособ построения одноранговых Wi-Fi сетей называется
5 Какие решения применяются для контроля к внешним устройствам
6 Компьютер проверяет 10 млн. паролей в Сколько примерно ему потребуется, чтобы проверить методом словарной атаки все пароли для языка, содержащего 1 млн слов
7. Сколько групп символов должен минимально содержать надежный пароль
8. Тонкий клиент - это
9. В какой блок файла autorun.inf обычно прописываются вредоносные программы
10. Каково количество популярных паролей, которые остаются неизменными в течение последних 15 лет

Примерные задания для проведения промежуточной аттестации по дисциплине

Список вопросов к зачету с оценкой

ОПК-1 - знать

1. Виды информации по категориям доступа. Общедоступная информация и информация и информация ограниченного доступа. Конфиденциальная информация.
2. Основные нормативно-правовые акты, регулирующие отношения в сфере защиты информации в России.
3. Организационно-правовая структура правового обеспечения защиты информации в России.
4. Порядок лицензирования деятельности по технической защите информации ограниченного доступа.
5. Коммерческая тайна. Правовой порядок установления режима коммерческой тайны.
6. Особенности правовой защиты интеллектуальной собственности. Виды интеллектуальной собственности. Право авторства и авторские (исключительные) права на интеллектуальную собственность.
7. Особенности правовой защиты персональных данных.
8. Принципы и порядок отнесения сведений к государственной тайне. Грифы секретности носителей этих сведений.
9. Порядок допуска и доступа должностных лиц и граждан к сведениям, составляющим государственную тайну.
10. Правовое регулирование отношений по защите информации в информационных и телекоммуникационных сетях, а также в сети Интернет.
11. Правовой порядок установления соответствия параметров объектов информатизации и средств защиты информации требованиям нормативных документов.

Практические задания

ОПК-1 владеть

Задача №1

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

1. Какие правила обеспечения информационной безопасности нарушены?
2. Какие символы должны быть использованы при записи пароля?

Ответ к задаче №2

1. Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем)

2. В качестве пароля должна выбираться последовательность символов, обеспечивающая малую вероятность её угадывания. Пароль должен легко запоминаться.

Задача №2

Вы - начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?
2. Какое наказание должен понести нарушитель?

Ответ к задаче №3

1. Статья 272. Неправомерный доступ к компьютерной информации.
2. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Задача №3

Вы - руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1. Какая статья уголовного кодекса была нарушена?
2. Какое наказание должен понести нарушитель?

Ответ к задаче №4

1. Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.
2. Создание программ для ЭВМ или внесение изменений в существующие программы,

заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Задача №4

Гражданин П. проник в информационную базу ККБ и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.

1. Являются ли его действия противозаконными?
2. С чем это связано?
3. Какое наказание может ждать гражданина П. за совершенные им действия?

Ответ к задаче №5:

1. Да.

2. Гражданин П. нарушил закон - Гл.28 УК РФ ст. 272 Неправомерный доступ к компьютерной информации.

3. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Задача № 5. С использованием прикладных программных продуктов осуществить поиск и выявление фактов вредоностного влияния на программы, установленные на исследуемом ПК. Опишите данные программы-вредители.

Тестовые задания

ОПК -1 - уметь

Тесты к разделу 1

1) Тест типа 4. «Выберите правильный вариант ответа»:

Уровнем безопасности, соразмерным с риском и величиной ущерба от потери, ненадлежащего использования, модификации или несанкционированного доступа к информации, называется:

Варианты ответа:

a) Адекватная безопасность
b) Полная безопасность
c) Критическая безопасность.

2) Тест типа 4. «Выберите правильный вариант ответа»:

Минимальным набором регуляторов безопасности, необходимых для защиты информационных систем, определяемых из потребностей информационных систем в обеспечении доступности, конфиденциальности и целостности, называется:

Варианты ответа:

a) Базовый уровень безопасности

b) Начальный уровень безопасности

c) Экстремальный уровень безопасности.

3) Тест типа 4. «Выберите правильный вариант ответа»:

Система безопасности, обеспечивающая несколько уровней защиты (низкий, умеренный, высокий) в зависимости от угроз, рисков, доступных технологий, поддерживающих сервисов, времени, кадровых и экономических ресурсов, называется:

Варианты ответа:

a) Калиброванной безопасностью

b) Нормализованной безопасностью

c) Приведенной безопасностью.

4) Тест типа 4. «Выберите правильный вариант ответа»:

Раскрытие информации неавторизованными лицами или нарушение политики безопасности организации, способное повлечь за собой умышленное или неумышленное несанкционированное раскрытие, модификацию, разрушение и/или потерю информации, называется:

Варианты ответа:

a) Компрометацией

b) Несанкционированным доступом

c) Дескридитацией.

5) Тест типа 4. «Выберите правильный вариант ответа»:

Нарушение или угроза неминуемого нарушения политики информационной безопасности, правил добропорядочного поведения или стандартных правил информационной безопасности, называется:

Варианты ответа:

a) Нарушение информационной безопасности

b) Взлом системы безопасности

c) Внедрение в систему безопасности.

Ключ: 1a, 2a, 3 a, 4a, 5 a.

Тесты к разделу 2

1) Тест типа 4. «Выберите правильный вариант ответа»:

Наука, состоящая из двух ветвей: криптографии и криптоанализа, называется:

Варианты ответа:

a) Криптологией

b) Шифрованием

c) Кодированием.

2) Тест типа 4. «Выберите правильный вариант ответа»:

Наука о способах преобразования (шифрования) информации с целью ее защиты от незнакомых пользователей, называется:

Варианты ответа:

a) Криптографией

b) Криптоанализом

c) Криптологией.

3) Тест типа 4. «Выберите правильный вариант ответа»:

Наука (и практика ее применения) о методах и способах вскрытия шифров, называется:

Варианты ответа:

a) Криптоанализом
b) Криптологией
c) Криптографией.

4) Тест типа 4. «Выберите правильный вариант ответа»:

В криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения, называется:

Варианты ответа:

a) Ключом
b) Кодом
c) Отмычкой.

5) Тест типа 4. «Выберите правильный вариант ответа»:

Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется:

Варианты ответа:

a) Воздействием (влиянием)
b) Силой
c) Потерей.

Ключ: 1a, 2a, 3 a, 4a, 5 a.

Тесты к разделу 3

1) Тест типа 4. «Выберите правильный вариант ответа»:

Действия, устройства, процедуры, технологии или другие меры, уменьшающие уязвимость информационной системы, называется:

Варианты ответа:

a) Контрмерами
b) Защитой
c) Противостоянием.

2) Тест типа 4. «Выберите правильный вариант ответа»:

Вредоносное программное обеспечение, нацеленное на компрометацию конфиденциальных данных пользователями, называется:

Варианты ответа:

a) Шпионским программным обеспечением
b) Потайным ходом
c) Ботом.

3) Тест типа 4. «Выберите правильный вариант ответа»:

Требование к информационной системе, являющееся следствием действующего законодательства, миссии и потребностью организации, называется:

Варианты ответа:

d) Требованием безопасности
e) Правилами безопасности
f) Мерами безопасности.

4) Тест типа 4. «Выберите правильный вариант ответа»:

Характеристика информации и/или информационной системы, основанная на оценке потенциального воздействия потери доступности, конфиденциальности и/или целостности этой информации и/или информационной системы на производственную деятельность

организации, ее активов и/или персонала, называется:

Варианты ответа:

a) Категорией безопасности
b) Уровнем защищенности
c) Способом безопасности.

5) Тест типа 4. «Выберите правильный вариант ответа»:

Уровнем воздействия на производственную деятельность организации (включая миссию, функции, образ, репутацию), ее активы (ресурсы) и персонал, являющийся следствием эксплуатации информационной системы и зависящего от потенциального воздействия угрозы и вероятности ее осуществления (реализации), называется:

Варианты ответа:

a) Риском
b) Планом
c) Давлением.

Ключ: 1a, 2a, 3 a, 4a, 5 a.

Тесты к разделу 4

1) Тест типа 4. «Выберите правильный вариант ответа»:

Действием по исправлению уязвимости или устранением угрозы, называется:

Варианты ответа:

a) Лечением
b) Перезагрузкой
c) Переустановкой.

2) Тест типа 4. «Выберите правильный вариант ответа»:

Иерархический показатель степени чувствительности по отношению к определенной угрозе, называется:

Варианты ответа:

a) Уровнем защищенности
b) Степенью безопасности
c) Требованием безопасности.

3) Тест типа 4. «Выберите правильный вариант ответа»:

Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются:

Варианты ответа:

a) Вирусами
b) Червями
c) Руткитами.

4) Тест типа 4. «Выберите правильный вариант ответа»:

Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется:

Варианты ответа:

a) Червем
b) Вирусом
c) Троянской программой.

5) Тест типа 4. «Выберите правильный вариант ответа»:

Набор файлов, устанавливаемых в системе с целью изменения ее стандартной

функциональности вредоносным и скрытым образом, называется:

Варианты ответа:

a) Руткитом
b) Ботом
c) Червем.

Ключ: 1, 2a, 3 a, 4a, 5 a.

Тесты к разделу 5

1) Тест типа 4. «Выберите правильный вариант ответа»:

Определение приоритетов, оценка и реализация контрмер, должным образом уменьшающих риски, называется:

Варианты ответа:

a) Нейтрализацией (уменьшением, ослаблением) рисков
b) Управлением рисков
c) Анализом рисков.

2) Тест типа 4. «Выберите правильный вариант ответа»:

Оставшийся, потенциальный риск после применения всех контрмер, называется:

Варианты ответа:

a) Остаточным риском
b) Минимальным риском
c) Критическим риском.

3) Тест типа 4. «Выберите правильный вариант ответа»:

Возможностью осуществления вредоносного события при отсутствии мер по нейтрализации рисков, называется:

Варианты ответа:

a) Совокупным (суммарным, полным) риском
b) Максимальным риском
c) Диверсией.

4) Тест типа 4. «Выберите правильный вариант ответа»:

Процесс идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

Варианты ответа:

a) Анализом рисков
b) Предупреждением рисков
c) Управление риском.

5) Тест типа 4. «Выберите правильный вариант ответа»:

Процессы, включающие оценку рисков, анализ экономической эффективности, выбор, реализацию и оценку контрмер, а также формальное санкционирование ввода системы в эксплуатацию, называется:

Варианты ответа:

a) Управлением рисками
b) Анализом рисков
c) Нейтрализацией риска.

Ключ: 1a, 2a, 3 a, 4a, 5 a.

Тесты к разделу 6

1) Тест типа 4. «Выберите правильный вариант ответа»:

Шифр реализует следующее преобразование открытого текста: каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу, то есть после буквы «я» следует буква «а», называется:

Варианты ответа:

a) Шифр Цезаря
b) Шифр Сократа
c) Шифр Менделеева.

2) Тест типа 4. «Выберите правильный вариант ответа»:

Уровень риска, который считается доступным для достижения желаемого результата, называется:

Варианты ответа:

a) Терпимостью по отношению к риску
b) Независимостью
c) Устойчивостью.

3) Тест типа 4. «Выберите правильный вариант ответа»:

Создание абсолютно надежной, недоступной для других каналов связи между абонентами или использование общественного канала связи, но при этом скрывая сам факт передачи информации или использование общественного канала связи, не передавая по нему нужную информацию в так называемом преобразованном виде, чтобы восстановить ее мог только адресат, любая из этих возможностей называется:

Варианты ответа:

a) Тайной передачей информации
b) Скрытой информацией
c) Кодированием.

4) Тест типа 4. «Выберите правильный вариант ответа»:

Телекоммуникационная или информационная система, передающая, обрабатывающая и/или хранящая информацию, потери, ненадлежащие использованию и/или несанкционированный доступ, к которым могут негативно воздействовать на миссию организации, называется:

Варианты ответа:

a) Системой, критичной для выполнения миссии организации (критичная система)
b) Неустойчивой системой
c) Замкнутой системой.

5) Тест типа 4. «Выберите правильный вариант ответа»:

Совокупность внешних процедур, условий и объектов, воздействующих на разработку, эксплуатацию и сопровождение информационных систем, называется:

Варианты ответа:

a) Окружением (средой)
b) Обществом
c) Переферией.

Ключ: 1a, 2a, 3 a, 4a, 5 a.

Итоговый тест

1) Тест типа 4. «Выберите правильный вариант ответа»:

Уровнем безопасности, соразмерным с риском и величиной ущерба от потери,

ненадлежащего использования, модификации или несанкционированного доступа к информации, называется:

Варианты ответа:

a) Адекватная безопасность
b) Полная безопасность
c) Критическая безопасность.

2) Тест типа 4. «Выберите правильный вариант ответа»:

Минимальным набором регуляторов безопасности, необходимых для защиты информационных систем, определяемых из потребностей информационных систем в обеспечении доступности, конфиденциальности и целостности, называется:

Варианты ответа:

a) Базовый уровень безопасности
b) Начальный уровень безопасности
c) Экстремальный уровень безопасности.

3) Тест типа 4. «Выберите правильный вариант ответа»:

Система безопасности, обеспечивающая несколько уровней защиты (низкий, умеренный, высокий) в зависимости от угроз, рисков, доступных технологий, поддерживающих сервисов, времени, кадровых и экономических ресурсов, называется:

Варианты ответа:

a) Калиброванной безопасностью
b) Нормализованной безопасностью
c) Приведенной безопасностью.

4) Тест типа 4. «Выберите правильный вариант ответа»:

Наука, состоящая из двух ветвей: криптографии и криптоанализа, называется:

Варианты ответа:

a) Криптологией
b) Шифрованием
c) Кодированием.

5) Тест типа 4. «Выберите правильный вариант ответа»:

Наука о способах преобразования (шифрования) информации с целью ее защиты от незнакомых пользователей, называется:

Варианты ответа:

a) Криптографией
b) Криптоанализом
c) Криптологией.

6) Тест типа 4. «Выберите правильный вариант ответа»:

Наука (и практика ее применения) о методах и способах вскрытия шифров, называется:

Варианты ответа:

a) Криптоанализом
b) Криптологией
c) Криптографией.

7) Тест типа 4. «Выберите правильный вариант ответа»:

Действия, устройства, процедуры, технологии или другие меры, уменьшающие уязвимость информационной системы, называется:

Варианты ответа:

a) Контрмерами

b) Защитой
c) Противостоянием.

8) Тест типа 4. «Выберите правильный вариант ответа»:

Вредоносное программное обеспечение, нацеленное на компрометацию конфиденциальных данных пользователями, называется:

Варианты ответа:

a) Шпионским программным обеспечением
b) Потайным ходом
c) Ботом.

9) Тест типа 4. «Выберите правильный вариант ответа»:

Требование к информационной системе, являющееся следствием действующего законодательства, миссии и потребностью организации, называется:

Варианты ответа:

a) Требованием безопасности
b) Правилами безопасности
c) Мерами безопасности.

10) Тест типа 4. «Выберите правильный вариант ответа»:

Действием по исправлению уязвимости или устранением угрозы, называется:

Варианты ответа:

a) Лечением
b) Перезагрузкой
c) Переустановкой.

11) Тест типа 4. «Выберите правильный вариант ответа»:

Иерархический показатель степени чувствительности по отношению к определенной угрозе, называется:

Варианты ответа:

a) Уровнем защищенности
b) Степенью безопасности
c) Требованием безопасности.

12) Тест типа 4. «Выберите правильный вариант ответа»:

Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются:

Варианты ответа:

a) Вирусами
b) Червями
c) Руткитами.

13) Тест типа 4. «Выберите правильный вариант ответа»:

Определение приоритетов, оценка и реализация контрмер, должным образом уменьшающих риски, называется:

Варианты ответа:

a) Нейтрализацией (уменьшением, ослаблением) рисков
b) Управлением рисков
c) Анализом рисков.

14) Тест типа 4. «Выберите правильный вариант ответа»:

Оставшийся, потенциальный риск после применения всех контрмер, называется:

Варианты ответа:

a) Остаточным риском
b) Минимальным риском
c) Критическим риском.

15) Тест типа 4. «Выберите правильный вариант ответа»:

Возможностью осуществления вредоносного события при отсутствии мер по нейтрализации рисков, называется:

Варианты ответа:

a) Совокупным (суммарным, полным) риском
b) Максимальным риском
c) Диверсией.

16) Тест типа 4. «Выберите правильный вариант ответа»:

Шифр реализует следующее преобразование открытого текста: каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу, то есть после буквы «я» следует буква «а», называется:

Варианты ответа:

a) Шифр Цезаря
b) Шифр Сократа
c) Шифр Менделеева.

17) Тест типа 4. «Выберите правильный вариант ответа»:

Уровень риска, который считается доступным для достижения желаемого результата, называется:

Варианты ответа:

a) Терпимостью по отношению к риску
b) Независимостью
c) Устойчивостью.

18) Тест типа 4. «Выберите правильный вариант ответа»:

Создание абсолютно надежной, недоступной для других каналов связи между абонентами или использование общественного канала связи, но при этом скрывая сам факт передачи информации или использование общественного канала связи, не передавая по нему нужную информацию в так называемом преобразованном виде, чтобы восстановить ее мог только адресат, любая из этих возможностей называется:

Варианты ответа:

a) Тайной передачей информации
b) Скрытой информацией
c) Кодированием.

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».

Зачет с оценкой. Критерии выставления оценок

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

«неудовлетворительно».

Оценка «отлично» при приеме зачета с оценкой 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 зачета с оценкой 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 зачета с оценкой 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 зачета с оценкой 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;

• не владения 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 с использованием шкалы, включающей оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», 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 / 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 978-5-44753946-7. - DOI 10.23681/276557. - Текст : электронный.

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 : Ефремов, И.В. Информационные технологии в сфере безопасности: практикум / И.В. Ефремов,

2. 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.

Нормативно-правовые акты:

1. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"
2. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"
3. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

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

1. Электронная библиотечная система «Университетская библиотека онлайн» https://biblioclub.ru /
2. Электронная библиотечная система «IPR BOOKS» www.iprbookshop.ru
3. Справочная правовая система «КонсультантПлюс»

9. Лицензионное программное обеспечение

- Notepad++ 7.5.8
- MS Windows 7 Профессиональная
- MS Windows 10 Pro
- Moodle 3.8.2.

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:

- учебные аудитории для проведения занятий лекционного типа (укомплектованные специализированной мебелью и оборудованные техническими средствами обучения, служащими для представления учебной информации большой аудитории, а также имеющие наборы демонстрационного оборудования и учебнонаглядных пособий, обеспечивающих тематические иллюстрации, соответствующие рабочим программам дисциплин);
- учебные аудитории для проведения занятий семинарского типа (с типовым оборудованием, обеспечивающим применение современных информационных технологий, и наглядными пособиями);
- компьютерные классы с демонстрационно-обучающими и обучающе-контролирующими возможностями, доступом к базам данных и Интернет;
- учебные аудитории для групповых и индивидуальных консультаций;
- учебные аудитории для текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы обучающихся (оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации);
- библиотека (имеющая читальные залы и рабочие места для обучающихся, 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.