ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«ЛЕНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИМЕНИ А.С. ПУШКИНА»**

УТВЕРЖДАЮ

Проректор по учебно-методической

работе

\_\_\_\_\_\_\_\_\_\_\_\_ С.Н.Большаков

РАБОЧАЯ ПРОГРАММА

дисциплины

**Б1.В.01.04 ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ В ЦИФРОВОЙ ЭКОНОМИКЕ**

Направление подготовки **09.04.03 Прикладная информатика**

Направленность (профиль) **Прикладная информатика в цифровой экономике**

(год начала подготовки – 2022)

Санкт-Петербург

2022

**1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ:**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

|  |  |  |
| --- | --- | --- |
| Индекс компетенции | Содержание компетенции  (или ее части) | Индикаторы компетенций (код и содержание) |
| УК-2 | Способен управлять проектом на всех этапах его жизненного цикла | ИУК-2.1. Знает методы управления проектами; этапы жизненного цикла проекта.  ИУК-2.2. Умеет разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ.  ИУК-2.3. Владеет навыками разработки проектов в избранной профессиональной сфере; методами оценки эффективности проекта, а также потребности в ресурсах. |
| УК-3 | Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели | ИУК-3.1. Знает методики формирования команд; методы эффективного руководства коллективами.  ИУК-3.2. Умеет разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту.  ИУК-3.3. Владеет методами организации и управления коллективом, планированием его действий. |
| УК-6 | Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки | ИУК-6.1. Знает основные принципы профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда; способы совершенствования своей деятельности на основе самооценки.  ИУК-6.2. Умеет решать задачи собственного профессионального и личностного развития, включая задачи изменения карьерной траектории; расставлять приоритеты.  ИУК-6.3. Владеет способами управления своей познавательной деятельностью и ее совершенствования на основе самооценки и принципов образования в течение всей жизни. |
| ПК-1 | Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС | ИПК-1.1. Знает методы и инструментальные средства прикладной информатики.  ИПК-1.2. Умеет применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач.  ИПК-1.3. Владеет современными методами и инструментальными средствами прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС. |
| ПК-2 | Способен проектировать архитектуру ИС предприятий и организаций в прикладной области | ИПК-2.1. Знает архитектуру и сервисы ИС предприятий и организаций.  ИПК-2.2. Умеет проектировать архитектуру и сервисы ИС предприятий и организаций в прикладной области.  ИПК-2.3. Владеет способностью проектировать архитектуру и сервисы ИС предприятий и организаций в прикладной области. |
| ПК-3 | Способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств | ИПК-3.1. Знает инновационные инструментальные средства проектирования ИС.  ИПК-3.2. Умеет проектировать информационные процессы и системы, адаптировать современные ИКТ.  ИПК-3.3. Владеет способностью проектировать информационные процессы и системы с использованием инновационных инструментальных средств, адаптировать современные ИКТ к задачам прикладных ИС. |
| ПК-4 | Способен принимать эффективные проектные решения в условиях неопределенности и риска | ИПК-4.1. Знает условия неопределенности и риска проектных решений.  ИПК-4.2. Умеет принимать эффективные проектные решения в условиях неопределенности.  ИПК-4.3. Владеет способностью принимать эффективные проектные решения в условиях неопределенности и риска. |
| ПК-5 | Способен формировать стратегию информатизации прикладных процессов и создания прикладных ИС в соответствии со стратегией развития предприятий | ИПК-5.1. Знает понятия миссии, стратегии предприятия, стратегии информатизации, стратегия развития ИС.  ИПК-5.2. Умеет сопоставлять стратегические цели фирмы с функциональным потенциалом создаваемых ИС.  ИПК-5.3. Владеет навыком отображать стратегические цели предприятия в проектах (моделях) ИС. |
| ПК-6 | Способен управлять информационными ресурсами и ИС | ИПК-6.1. Знает структуру деятельности по управлению сложными объектами, суть понятий информационные ресурсы и информационные системы.  ИПК-6.2. Умеет формулировать управляющие воздействия на информационные ресурсы и информационные системы.  ИПК-6.3. Владеет одним из средств компьютерного мониторинга состояния информационных ресурсов и информационных систем. |
| ПК-7 | Способен управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций | ИПК-7.1. Знает методы и средства управления проектами по информатизации прикладных задач и созданию ИС.  ИПК-7.2. Умеет управлять проектами по информатизации прикладных задач и созданию ИС.  ИПК-7.3. Владеет способами управления проектами по информатизации прикладных задач и созданию ИС. |
| ПК-8 | Способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях | ИПК-8-1. Знает методы научных исследований и инструментария в области проектирования и управления ИС.  ИПК-8-2. Умеет выбирать и использовать методы научных исследований и инструментария в области проектирования и управления ИС.  ИПК-8.3. Владеет способами применения методов научных исследований и инструментария в области проектирования и управления ИС в прикладных областях. |

**2. Место дисциплины в структуре ОП:**

Цель дисциплины: формирование у обучающихся компетенции в области эффективного противодействия киберугрозам цифровой экономики.

Задачи дисциплины:

* знакомство обучающихся с видами киберугроз для цифровой экономики;
* изучение способов обеспечения кибербезопасности в условиях развития цифровой экономики, обеспечения устойчивости и безопасности цифровизации российской экономики;
* рассмотрение подходов к обеспечению безопасности данных.

Дисциплина относится к части, формируемой участниками образовательных отношений, модуль Программирование и информационные системы в цифровой экономике.

Освоение дисциплины и сформированные при этом компетенции необходимы в последующей деятельности.

**3. Объем дисциплины и виды учебной работы:**

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 академических часов *(1 зачетная единица соответствует 36 академическим часам).*

Очная форма обучения

|  |  |  |
| --- | --- | --- |
| Вид учебной работы | Трудоемкость в акад.час | |
|  |  | Практическая подготовка |
| **Контактная работа (аудиторные занятия) (всего):** | 32 | |
| в том числе: |  | |
| Лекции | 16 | - |
| Лабораторные работы / Практические занятия (в т.ч. зачет) | 16/- | 4/- |
| **Самостоятельная работа (всего)** | 76 | |
| **Вид промежуточной аттестации (экзамен):** | - | |
| контактная работа | - | |
| самостоятельная работа по подготовке к экзамену | - | |
| **Общая трудоемкость дисциплины (в час. /з.е.)** | 108/3 | |

Заочная форма обучения

|  |  |  |
| --- | --- | --- |
| Вид учебной работы | Трудоемкость в акад.час | |
|  |  | Практическая подготовка |
| **Контактная работа (аудиторные занятия) (всего):** | 16 | |
| в том числе: |  | |
| Лекции | 4 | - |
| Лабораторные работы/ Практические занятия | 12/- | 4/- |
| **Самостоятельная работа (всего)** | 88 | |
| **Вид промежуточной аттестации (зачет):** | 4 | |
| контактная работа | 0,25 | |
| самостоятельная работа по подготовке к зачету | 3,75 | |
| **Вид промежуточной аттестации (экзамен):** | - | |
| контактная работа | - | |
| самостоятельная работа по подготовке к экзамену | - | |
| **Общая трудоемкость дисциплины (в час. /з.е.)** | 108/3 | |

**4.СОДЕРЖАНИЕ ДИСЦИПЛИНЫ:**

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей**).**

**4.1 Блоки (разделы) дисциплины.**

|  |  |
| --- | --- |
| № | Наименование блока (раздела) дисциплины |
| 1 | Задачи кибербезопасности в цифровой экономике. |
| 2 | Киберпреступность и способы её предотвращения. |
| 3 | Специфика технологии защищенного документооборота. |
| 4 | Анализ режимов работы кибернетических систем. |
| 5 | Принципы построения системы кибербезопасности. |

**4.2. Примерная тематика курсовых работ (проектов):**

Курсовая работа по дисциплине не предусмотрена учебным планом.

**4.3. Перечень занятий, проводимых в активной и интерактивной формах, обеспечивающих развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств. Практическая подготовка\*.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование блока (раздела) дисциплины** | **Занятия, проводимые в активной и интерактивной формах** | | **Практическая подготовка\*** |
| **Форма проведения занятия** | **Наименование видов занятий** |
| 1. | Задачи кибербезопасности в цифровой экономике | лекционное занятие  лабораторное занятие | лекция-дискуссия  разбор конкретных ситуаций |  |
| 2. | Киберпреступность и способы её предотвращения | лекционное занятие  лабораторное занятие | лекция-дискуссия  разбор конкретных ситуаций |  |
| 3. | Специфика технологии защищенного документооборота | лекционное занятие  лабораторное занятие | лекция-дискуссия  разбор конкретных ситуаций |  |
| 4. | Анализ режимов работы кибернетических систем | лекционное занятие  лабораторное занятие | лекция-дискуссия  разбор конкретных ситуаций |  |
| 5. | Принципы построения системы кибербезопасности | лекционное занятие  лабораторное занятие | лекция-дискуссия  разбор конкретных ситуаций | Формирование модели угроз безопасности информации для заданной информационной системы |

**\***Практическая подготовка при реализации учебных предметов, курсов, дисциплин (модулей) организуется путем проведения практических занятий, практикумов, лабораторных работ и иных аналогичных видов учебной деятельности, **предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.**

**5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине:**

**5.1 Темы конспектов**

Тема 1. Задачи кибербезопасности в цифровой экономике.

Тема 2. Киберпреступность и способы её предотвращения.

Тема 3 Специфика технологии защищенного документооборота.

Тема 4 Анализ режимов работы кибернетических систем.

Тема 5 Принципы построения системы кибербезопасности.

**5.2 Темы для творческой самостоятельной работы обучающегося**

Темы для творческой самостоятельной работы студента формулируются обучающимся самостоятельно, исходя из перечня тем занятий текущего семестра.

**5.3. Темы рефератов**

* 1. ИКТ-системы для сложных инфраструктур: от технологий безопасности к решениям безопасности.
  2. Безопасность, стабильность и отказоустойчивость инфраструктуры глобального Интернета.
  3. Проблемы противодействия угрозам вмешательства во внутренние дела суверенных государств через социальные медиа.
  4. Защита критически важной инфраструктуры: многоуровневый подход.
  5. Перспективы применения международных правовых норм в киберпространстве.
  6. Адаптация международного права безопасности к информационному пространству.
  7. Защита критически важной инфраструктуры в киберпространстве.
  8. Перспективы применения Big Data для обеспечения безопасности критических информационных систем.
  9. Уголовная ответственность в сфере компьютерной безопасности.
  10. Стадии и стратегии управления безопасностью и риском.
  11. Сравнение концепций стратегии национальной/информационной безопасности России и США.
  12. Сравнение концепций стратегии национальной/информационной безопасности России и Китая.
  13. Подходы к защите персональных данных различными группами информационных сервисов: facebook+whatsapp+Instagram.
  14. Подходы к защите персональных данных различными группами информационных сервисов: Вконтакте, Одноклассники.
  15. Подходы к защите пользовательских данных IT-гигантом Google.
  16. Подходы к защите пользовательских данных IT-гигантом Yandex (в рамках стратегии национальной безопасности РФ).
  17. Феномен WeChat и подходы к данным пользователей.
  18. Шифрование данных в WhatsApp.
  19. Шифрование данных в Telegram.
  20. Социальная инженерия.
  21. Цифровой аватар: грани опасности для граждан.
  22. Защита цифровой личности.
  23. Стеганография - защита ценных бумаг.
  24. Уголовное преследование в РФ по направлению ИБ.
  25. Самые "громкие" бэкдоры.

**5.4. Вопросы для подготовки к практическим занятиям (лабораторным работам):**

*Лабораторная работа №1. Контроль и разграничения доступа в информационных системах*

1. Идентификация - процедура определения тождественности \_\_\_\_\_\_\_ одному из зарегистрированных в системе идентификаторов.

2. Аутентификация - процедура установления \_\_\_\_\_\_\_\_\_ предъявляемого субъектом идентификатора.

3. Процедура аутентификации может являться условием прохождения процедуры идентификации и предшествовать процедуре \_\_\_\_\_\_\_\_\_.

4. Процедура аутентификации, основанная на предъявлении пользователем уникального объекта, связанного с \_\_\_\_\_\_\_\_\_\_, основана на факторе, условно обозначаемом как «Я имею».

5. Многоразовый \_\_\_\_\_\_\_\_\_, используемый для нескольких сеансов аутентификации, может создаваться самим пользователем.

6. Персональное средство аутентификации («токен») предназначено для организации процедуры аутентификации на основе фактора «Я \_\_\_\_\_\_\_».

7. Процедура аутентификации на основе признаков, относящихся ко внешнему виду или особенностям действий субъекта, называется \_\_\_\_\_\_\_\_\_\_\_\_ аутентификацией.

8. В дискреционной модели разграничения доступа устанавливаются права доступа для каждой пары \_\_\_\_\_\_\_ и объекта.

9. В мандатной модели разграничения доступа уровни доступа субъектов сравниваются с метками \_\_\_\_\_\_\_\_\_\_\_ объектов.

10. В \_\_\_\_\_\_\_\_ модели разграничения доступа добавление нового субъекта сводится к присвоению ему подходящей совокупности прав доступа субъекта к объектам информационной системы.

11. Основной и вспомогательный персонал организации, технический персонал провайдеров услуг относятся к категории \_\_\_\_\_\_\_\_\_\_ источников угроз безопасности.

12. В соответствии с Методикой определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., разработчики программных средств, конкурирующие организации, бывшие работники - \_\_\_\_\_\_\_\_\_ нарушителя, соответствующие внешнему типу нарушителя.

13. В соответствии с Методикой определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ - воздействие нарушителя на пользователей, администраторов информационной системы или обслуживающий персонал.

*Лабораторная работа №2. Криптографические методы защиты информации*

1. \_\_\_\_\_\_\_ шифр - шифр, обрабатывающий за каждое применение операции зашифрования группу символов открытого текста фиксированной длины.

2. В современных блочных шифрах к преобразованиям зашифрования и расшифрования добавляется преобразование \_\_\_\_\_\_\_\_\_\_\_ ключа.

3. Одной из особенностей сети Фейстеля является разделение блока открытого текста, обрабатываемого за одно применение операции зашифрования, на два (левый и правый) или более \_\_\_\_\_\_\_\_\_.

4. В SP-сети P-блоки реализуют операцию \_\_\_\_\_\_\_\_ над шифруемым блоком открытого текста.

5. При добавлении в систему симметричного шифрования с n абонентами нового абонента потребуется выработать и распределить между абонентами \_\_\_ ключей для обеспечения конфиденциальности связи между любыми двумия абонентами.

6. Получив сообщение C=5 в криптографической системе RSA с N=55, Алиса, применив секретный ключ d=23, может получить окрытый текст M=\_\_\_\_.

7. В схемах электронной цифровой подписи владелец на основе секретного ключа может зашифровать (подписать) сообщение, а любой желающий может на основе открытого ключа владельца расшифровать сообщение, т. е. \_\_\_\_\_\_\_\_\_\_ корректность подписи.

8. Пара аргументов, для которых значения функции хэширования совпадают, называются \_\_\_\_\_\_\_\_.

9. Понятие (n, t)-пороговой схемы используется в криптографических протоколах \_\_\_\_\_\_\_\_ секрета и означает, что среди n участников группы восстановить секретное значение может любая подгруппа, включающая не менее чем t участников, а никакие t-1 участников группы не могут этого сделать.

10. Под квантовой криптографией обычно понимается реализация схем передачи между абонентами \_\_\_\_\_\_\_ последовательности, которая затем может быть использована в качестве ключа симметричной системы шифрования.

11. Основной и вспомогательный персонал организации, технический персонал провайдеров услуг относятся к категории \_\_\_\_\_\_\_\_\_\_ источников угроз безопасности.

12. В соответствии с Методикой определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., разработчики программных средств, конкурирующие организации, бывшие работники - \_\_\_\_\_\_\_\_\_ нарушителя, соответствующие внешнему типу нарушителя.

13. В соответствии с Методикой определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ - воздействие нарушителя на пользователей, администраторов информационной системы или обслуживающий персонал.

*Лабораторная работа №3. Стенографическая защита информации*

1. Применение невидимых чернил в сочетании с видимым текстом является примером маскирования секретного \_\_\_\_\_\_\_ в другом сообщении.

2. Под сообщением в стеганографии обычно понимается передаваемая \_\_\_\_\_\_\_ информация.

3. Информация, используемая для сокрытия секретного сообщения, называется стеганографическим \_\_\_\_\_\_\_\_\_\_\_\_.

4. Даже не имея достоверной информации о наличии передаваемого секретного сообщения, нарушитель может предпринять попытку реализации угрозы \_\_\_\_\_\_\_ скрытого сообщения, изменяя структуру контейнера, но не изменяя его смысловое содержание.

5. В так называемой «модели заключенных» предполагается, что канал связи, по которому происходит передача сообщений (стегоканал), контролирует \_\_\_\_\_\_\_\_\_, который может полностью контролировать обмен сообщениями между абонентами.

6. Реализуя атаку разрушения сообщения, нарушитель модифицирует \_\_\_\_\_\_\_\_\_\_, стремясь разрушить сообщение, если оно присутствует..

7. Направление стеганографии, основанное на использовании в качестве контейнеров структур системного ПО, служебной информации операционной или файловой системы, называется \_\_\_\_\_\_\_\_\_\_\_ стеганографией..

8. Пользовательские файлы, например графические или звуковые, используются в качестве контейнеров в направлении стеганографии, называемом \_\_\_\_\_\_\_\_\_\_ стеганографией.

9. Хрупкие цифровые водяные знаки предназначены для контроля \_\_\_\_\_\_\_\_\_ информации.

10. Для идентификации некоторых дорогостоящих объектов (таких как автомобили и запчасти) применяют стеганографический метод передачи идентификационной информации, являющийся современных воплощением технологии \_\_\_\_\_\_\_\_, применявшейся для скрытой передачи информации разведчиками.

*Лабораторная работа №4. Программно-технические меры защиты информации*

1. Сервис безопасности - набор функций, реализуемых \_\_\_\_\_\_\_\_ защиты информации для обеспечения защищенности системы.

2. Согласно определению из УК РФ, вредоносная программа - программа, заведомо предназначенная для \_\_\_\_\_\_\_\_\_\_\_\_ уничтожения, блокирования, модифцикации компьютерной информации или нейтрализации средств защиты компьютерной информации.

3. Вредоносные программы, реализующие несанкционированные действия, направленные на нарушение безопасности информационной системы, без создания собственных копий, называются \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ .

4. Вредоносные программы, относящиеся к типам «вирус» или «червь» обладают способностью к \_\_\_\_\_\_\_\_\_\_\_\_, то есть созданию собственных копий в пределах одного узла сети или на узлах, ранее не подвергнувшихся заражению.

5. Альтернативой сигнатурному анализу при обнаружении вредоносных программ является анализ \_\_\_\_\_\_\_\_ программы.

6. При выборе средств \_\_\_\_\_\_\_\_\_\_\_ защиты рекомендуется учитывать тесты лабораторий, проводящих различные тесты таких средств, основываясь на результатах тестов, соответствующих условиям работы защищаемой системы.

7. Функция, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области, называется \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_.

8. Межсетевое экранирование не защищает систему от загрузки пользователями \_\_\_\_\_\_\_\_\_\_\_ программного обеспечения.

9. Среди дополнительных задач DLP-систем может рассматриваться блокирование передачи не только \_\_\_\_\_\_\_\_\_, но и просто нежелательной информации.

10. Протоколированием называется фиксирование информации о \_\_\_\_\_\_\_\_\_\_, происходящих в информационной системе.

*Лабораторная работа №5. Системы обнаружения и предотвращения компьютерных атак*

1. Сервис безопасности - набор функций, реализуемых \_\_\_\_\_\_\_\_ защиты информации для обеспечения защищенности системы.

2. Согласно определению из УК РФ, вредоносная программа - программа, заведомо предназначенная для \_\_\_\_\_\_\_\_\_\_\_\_ уничтожения, блокирования, модифцикации компьютерной информации или нейтрализации средств защиты компьютерной информации.

3. Вредоносные программы, реализующие несанкционированные действия, направленные на нарушение безопасности информационной системы, без создания собственных копий, называются \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ .

4. Вредоносные программы, относящиеся к типам «вирус» или «червь» обладают способностью к \_\_\_\_\_\_\_\_\_\_\_\_, то есть созданию собственных копий в пределах одного узла сети или на узлах, ранее не подвергнувшихся заражению.

5. Альтернативой сигнатурному анализу при обнаружении вредоносных программ является анализ \_\_\_\_\_\_\_\_ программы.

6. При выборе средств \_\_\_\_\_\_\_\_\_\_\_ защиты рекомендуется учитывать тесты лабораторий, проводящих различные тесты таких средств, основываясь на результатах тестов, соответствующих условиям работы защищаемой системы.

7. Функция, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области, называется \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_.

8. Межсетевое экранирование не защищает систему от загрузки пользователями \_\_\_\_\_\_\_\_\_\_\_ программного обеспечения.

9. Среди дополнительных задач DLP-систем может рассматриваться блокирование передачи не только \_\_\_\_\_\_\_\_\_, но и просто нежелательной информации.

10. Протоколированием называется фиксирование информации о \_\_\_\_\_\_\_\_\_\_, происходящих в информационной системе.

**6 Оценочные средства для текущего контроля успеваемости:**

**6.1. Текущий контроль**

|  |  |  |
| --- | --- | --- |
| №п/п | № и наименование блока (раздела) дисциплины | Форма текущего контроля |
| 1 | Разделы 1-5 | Проверка наличия конспектов.  Устный опрос, тест |
| 2 | Разделы 3-5 | Защита отчета по результатам выполнения лабораторных работ. |

**6.2. Примеры оценочных средств для текущего контроля успеваемости**

***Темы конспектов.***

Представлены в разделе 5.1.

***Перечень практических заданий.***

Представлены в п. 5.4.

***Примеры тестовых заданий.***

1. Под политикой безопасности организации, согласно ГОСТ Р ИСО/МЭК 15408-1 – 2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», понимается

Выберите один вариант из перечисленных

* Совокупность правил и директив, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию
* Совокупность правил, процедур или руководящих принципов в области безопасности для некоторой организации
* Совокупность правил, решений руководства, обеспечивающих адекватный уровень безопасности информации в организации
* Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых организацией

2. Политика безопасности по своей сути относится к категории

Выберите один вариант из перечисленных

* Административных мер защиты информации
* Организационно-технических мер защиты информации
* Нормативных мер защиты информации
* Морально-этических мер защиты информации

3. Целью разработки политики безопасности организации является обеспечение

Выберите один вариант из перечисленных

* Соблюдения требований законов и иных норм в области информационной безопасности
* Управления и поддержки высшим руководством информационной безопасности
* Непрерывности деятельности организации и включения информационной безопасности в бизнес-процессы организации
* Соблюдения в рамках организации адекватного уровня информационной безопасности

4. Цели и принципы информационной безопасности формулируются в политике безопасности организации в соответствии с:

Выберите один вариант из перечисленных

* Требованиями действующего законодательства и иных нормативных актов
* Требованиями обязательств организации
* Целями функционирования организации
* Актуальными угрозами и возможностями нарушителей безопасности информации

5. Одной из основных рекомендаций по рассмотрению организационных аспектов информационной безопасности в политике безопасности организации является назначение ответственного лица, чьей обязанностью будет

Выберите один вариант из перечисленных

* Контроль действий других пользователей
* Контроль работоспособности действующих решений руководства организации
* Учет случаев нарушения действующих решений руководства организации
* Консультирование других пользователей

6. Укажите все аспекты распределения обязанностей между сотрудниками организации, формулируемые в политике безопасности организации:

Выберите все подходящие варианты из перечисленных

* Обязанности каждого сотрудника
* Возможность делегирования обязанностей при сохранении ответственности
* Круг обязанностей каждого руководителя
* Возможность делегирования ответственности за соблюдение политики безопасности
* Возможность делегирования обязанностей и ответственности за соблюдение политики безопасности
* Обязанности руководства организации в целом
* Круг обязанностей каждого отдела организации

7. Укажите все вопросы, которые рекомендуется решать в рамках управления активами:

Выберите все подходящие варианты из перечисленных

* Владение активами
* Использование активов
* Приобретение и ликвидация активов
* Оценка активов
* Классификация информации
* Оценка рисков

8. При формулировании вопросов управления активами в политике безопасности для активов, связанных со средствами обработки информации, назначается владелец по следующему принципу:

Выберите один вариант из перечисленных

* Для каждого актива высшего уровня важности – конкретное лицо
* Для каждого актива – конкретное лицо
* Для каждого актива высшего уровня важности – конкретное лицо или определенная часть организации
* Для каждого актива – конкретное лицо или определенная часть организации

9. Укажите все виды угроз, на снижение вероятности которых должны быть прямо направлены мероприятия по управлению персоналом

Выберите все подходящие варианты из перечисленных

* Хищение средств обработки информации
* Сетевые атаки
* Утечка информации по техническим каналам
* Внедрение в информационную систему организации вредоносных программ
* Имущественный ущерб путем мошеннических действий
* Использование средств обработки информации в личных целях

10. На снижение вероятности угроз со стороны нарушителя вида «Бывшие работники» направлено формулирование вопросов

Выберите один вариант из перечисленных

* Прекращения прав доступа сотрудников
* Обучения и тренинга сотрудников
* Поддержания осведомленности сотрудников об угрозах информационной безопасности
* Применения дисциплинарных мер за нарушение политики безопасности
* Контроля соблюдения требований политики безопасности руководством всех уровней

11. Укажите все аспекты, являющиеся целями рассмотрения в политике безопасности организации вопроса физической безопасности

Выберите все подходящие варианты из перечисленных

* Предотвращение неавторизованного физического доступа в помещения организации
* Предотвращение неавторизованного воздействия на информацию организации
* Предотвращение повреждения оборудования организации
* Предотвращение неавторизованного воздействия на персонал организации
* Предотвращение повреждения программного обеспечения организации

12. Укажите все аспекты, которые должны быть сформулированы в разделе политики безопасности организации, посвященном физической безопасности

Выберите все подходящие варианты из перечисленных

* Вопросы защиты оборудования организации от сбоев поддерживающей инфраструктуры;
* Принципы управления рисками при использовании оборудования вне помещений организации
* Принципы перемещения имущества организации
* Политика управления доступом на территорию объекта информатизации, порядок ее обеспечения физическими мерами
* Вопросы регистрации и снятия с учета сотрудников организации, предоставления им прав доступа на территорию объекта информатизации и прекращения таких прав
* Вопросы проверки кандидатов на доступ на территорию объекта информатизации в соответствии с требованиями обязательств и аспектов деятельности организации

13. Укажите аспекты управления доступом, которые рекомендуется организовать в виде формальных процедур

Выберите все подходящие варианты из перечисленных

* Предоставление и прекращение привилегий пользователей в системе
* Управление распределением пользовательских паролей
* Обеспечение физических мер управления доступом
* Периодический пересмотр предоставленных пользователям прав в ИС
* Предоставление пользователям доступа к сетевым услугам

14. Целью рассмотрения в политике безопасности организации вопросов эксплуатации информационных систем является обеспечение при эксплуатации ИС

Выберите один вариант из перечисленных

* Уверенности в постоянном поддержании уровня безопасности
* Обеспечения надлежащего уровня безопасности
* Уверенности в обеспечении надлежащего уровня безопасности
* Обеспечения уверенности в поддерживаемом уровне безопасности

15. Одной из основных рекомендаций по рассмотрению в политике безопасности организации вопросов эксплуатации информационных систем является согласование требований безопасности

Выберите один вариант из перечисленных

* Непосредственно перед началом эксплуатации информационной системы
* По результатам некоторого периода эксплуатации информационной системы
* До разработки информационной системы
* По результатам внедрения новых компонентов информационной системы

16. Одной из основных рекомендаций по вопросам управления инцидентами информационной безопасности является:

Выберите один вариант из перечисленных

* Передача расследования инцидентов на более высокий уровень
* Передача расследования инцидентов на более низкий уровень
* Расследование инцидентов на уровне, на котором был совершен инцидент
* Расследование инцидентов на уровне, на котором был выявлен инцидент

17. Укажите все источники требований, исключение нарушений которых является целью рассмотрения в политике безопасности организации вопроса соответствия требованиям обязательств организации

Выберите все подходящие варианты из перечисленных

* Действующие законы
* Государственные стандарты
* Международные стандарты
* Подзаконные нормативно-правовые акты
* Договорные обязательства организации
* Отраслевые стандарты
* Цели деятельности организации

18. Укажите все процессы, при которых, согласно рекомендации по обеспечению соответствия требованиям обязательств организации, должны учитываться требования безопасности:

Выберите все подходящие варианты из перечисленных

* Проектирование ИС
* Реализация ИС
* Внедрение ИС
* Функционирование ИС
* Использование ИС

19. Обучение сотрудников принципам работы с учетом требований политики безопасности относится к этапу

Выберите один вариант из перечисленных

* Эксплуатации
* Первоначального планирования
* Аудита и контроля
* Внедрения
* Разработки

20. Жизненный цикл политики безопасности предполагает контроль за соблюдением содержащихся в ней требований

Выберите один вариант из перечисленных

* Только в случае выявления и расследования инцидентов информационной безопасности
* Только при плановой аттестации сотрудников
* На постоянной основе
* В ходе периодических проверок

**7. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование | Авторы | Место издания | Год издания | Наличие | |
| печатные издания | ЭБС (адрес в сети Интернет) |
| 1. | Информационная безопасность и защита информации: учебное пособие для вузов | Зенков А.В. | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/497002> |
| 2. | Преступления в сфере информационной безопасности: учебное пособие для вузов | Корабельников С.М. | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/496492> |
| 3. | Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов | Полякова Т.А., Стрельцов А.А. | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/498844> |
| 4. | Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие | Казарин О.В.,  Шубинский И.Б. | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/495524> |
| 5. | Кибербезопасность в условиях электронного банкинга: практическое пособие | Бердюгин А.А., Дудка А.Б., Конявская С.В. | М.: Прометей | 2020 |  | [https://biblioclub.ru](https://biblioclub.ru/index.php?page=book&id=610688) |
| 6. | Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения | Белоус А.И. | Москва : Техносфера | 2021 |  | [https://biblioclub.ru](https://biblioclub.ru/index.php?page=book&id=610688) |
| 7. | Информационная безопасность и защита информации: теория и практика: учебное пособие | Ищейнов В.Я. | М., Берлин: Директ-Медиа | 2020 |  | [https://biblioclub.ru](https://biblioclub.ru/index.php?page=book&id=610688) |
| 8. | Основы информационной безопасности: учебное пособие | Гультяева Т.А. | Новосибирск: НГТУ | 2018 |  | [https://biblioclub.ru](https://biblioclub.ru/index.php?page=book&id=610688) |
| 9. | Управление информационной безопасностью: учебное пособие | Шилов А.К. | Ростов-на-Дону: ЮФУ | 2018 |  | [https://biblioclub.ru](https://biblioclub.ru/index.php?page=book&id=610688) |

**8. Ресурсы информационно-телекоммуникационной сети «Интернет»:**

1. «НЭБ». Национальная электронная библиотека. – Режим доступа: [http://нэб.рф/](http://www.biblioclub.ru/)

2. «eLibrary». Научная электронная библиотека. – Режим доступа: [https://elibrary.ru](https://elibrary.ru/)

3. «КиберЛенинка». Научная электронная библиотека. – Режим доступа: <https://cyberleninka.ru/>

4. ЭБС «Университетская библиотека онлайн». – Режим доступа: [http://www.biblioclub.ru/](http://www.knigafund.ru/)

5. Российская государственная библиотека. – Режим доступа: <http://www.rsl.ru/>

**9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ:**

В ходе осуществления образовательного процесса используются следующие информационные технологии:

- средства визуального отображения и представления информации (LibreOffice) для создания визуальных презентаций как преподавателем (при проведении занятий) так и обучаемым при подготовке докладов для семинарского занятия.

- средства телекоммуникационного общения (электронная почта и т.п.) преподавателя и обучаемого.

- использование обучаемым возможностей информационно-телекоммуникационной сети «Интернет» при осуществлении самостоятельной работы.

**9.1. Требования к программному обеспечению учебного процесса**

Для успешного освоения дисциплины, обучающийся использует следующие программные средства:

* Windows 10 x64
* MicrosoftOffice 2016
* LibreOffice
* Firefox
* GIMP

**9.2. Информационно-справочные системы (при необходимости):**

Не используются

**10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий.

Для изучения дисциплины используется следующее оборудование: аудитория, укомплектованная мебелью для обучающихся и преподавателя, доской, ПК с выходом в интернет, мультимедийным проектором и экраном.

Для самостоятельной работы обучающихся используется аудитория, укомплектованная специализированной мебелью и техническими средствами (ПК с выходом в интернет и обеспечением доступа в электронно-информационно-образовательную среду организации).