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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты компьютерной информации

(наименование дисциплины)

Направление подготовки
09.03.04 Программная инженерия

Квалификация выпускника
Бакалавр

Направленность (профиль)
Проектирование программного обеспечения

2023 г.

1. Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций

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

ОПК -3 – способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Индикатор достижения компетенции	***Планируемые результаты обучения***
ИД-1 (ОПК-3) подбирать инструменты для решения задачи защиты информации	***знает***
	РО-1 ИД-1 (ОПК-3) роль и место информационных технологий при разработке и использовании информационных систем; принципы, методы и средства защиты компьютерной информации
	умеет
	РО-2 ИД-1 (ОПК-3) проводит аудит рисков информационной безопасности **РО-3 ИД-1 (ОПК-3)** использует в практической деятельности организации информацию, полученную в ходе аудита
	владеет
	РО-4 ИД-1 (ОПК-3) установка и использование средств информационной безопасности

2. Объем дисциплины в зачетных единицах

Объем дисциплины составляет 4 зачетные единицы.

3. Содержание дисциплины

Программа учебного курса по информационной безопасности имеет высокую актуальность и отражает важные способы работы с цифровыми ресурсами. В первую очередь информационная безопасность в РФ – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Разделы учебной дисциплины отражают широкий перечень вопросов, касающейся кибербезопасности: правовые, организационно-технические, экономические. Отдельно обсуждаются варианты угроз в сфере защиты информации с которыми сталкивается любая компания в нынешних реалиях. Методологию защиты информации конкретной организации отражает Концепция защиты информации – это система взглядов на сущность, цели, принципы и организацию защиты информации в этой организации.

Раздел 1. Место информационной безопасности в национальной безопасности РФ.

Тема 1.1 Цели и задачи информационной безопасности.

Понятие информации. Фазы обращения информации в информационных системах.

Место информационной безопасности в национальной безопасности РФ.

Цели и задачи обеспечения информационной безопасности.

Составляющие информационной безопасности.

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

Виды и источники угроз информационной безопасности РФ.

Структура государственной системы обеспечения информационной безопасности РФ.

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

Архитектура СЗИ организации и основные требования к средствам защиты.

Функциональное построение СЗИ организации и назначение основных подразделений.

Элементарные модели СЗИ организации. Семирубежная модель защиты.

Последовательность и содержание основных этапов проектирования СЗИ организации.

Содержание процесса эксплуатации СЗИ организации.

Анализ угроз информационной безопасности.

Внутренние и внешние источники угроз информационной безопасности.

Схема воздействия угроз на информационную систему.

Перечень основных формальных и неформальных средств защиты информации.

Стратегии защиты информации на объекте информатизации.

Основы защиты информации в телекоммуникационных сетях.

Роль персонала в обеспечении информационной безопасности предприятия.

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

Управление рисками на различных стадиях жизненного цикла информационной системы.

Трехмерная модель “куб безопасности”.

Анализ информационных рисков, угроз и уязвимостей системы.

Оценка рисков по двум факторам.

Анализ информационных рисков, угроз и уязвимостей системы.

Оценка рисков по трем факторам.

Программное обеспечение для анализа рисков информационной безопасности.

Раздел 2. Информационная безопасность, как основа стабильности организации.

Тема 2.1 Криптографическая защита информации.

Классические криптоалгоритмы – моно- и многоалфавитные подстановки.

Классические криптоалгоритмы - перестановки.

Шифрование методом гаммирования.

Современные симметричные системы шифрования. Обобщенная схема симметричного шифрования.

Симметричная система шифрования DES.

Отечественный стандарт симметричного шифрования.

Принцип открытого распространения ключей. Алгоритм Диффи-Хеллмана.

Современные асимметричные системы шифрования. Обобщенная схема асимметричного шифрования.

Асимметричная система шифрования RSA.

Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП.

Электронная цифровая подпись на основе алгоритма RSA.

Отечественный стандарт цифровой подписи ГОСТ Р34.10-2012.

Тема 2.2. 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.

Тема 2.3. Программы, обеспечивающие защиту информации.

Вредоносное программное обеспечение и методы борьбы с ним.

4. Методические рекомендации по организации изучения учебной дисциплины, включая самостоятельную работу обучающихся

Изучение дисциплины включает контактную работу обучающихся с педагогическими работниками, а также коммерческими организациями, привлекаемыми 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.

Вопросы для самоконтроля/Задания для самоконтроля/Вопросы и задания 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 (ТСВ)?

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?

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

Основная:

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102070.html

2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.

Дополнительная:

1. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97562.html

2. Моргунов, А.В. Информационная безопасность : учебно-методическое пособие : [16+] / А.В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726

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

1. http://biblioclub.ru/ – электронная библиотечная система «Университетская библиотека Онлайн»
2. http://www.iprbookshop.ru/ – электронная библиотечная система IPR BOOKS
3. http://www.yurist.ru
4. http://www.garant.ru – ГАРАНТ: [Информационно-правовой портал]
5. Справочная правовая система Консультант Бизнес: Версия Проф

Профессиональные базы данных в составе СПС Консультант:

- Законодательство Санкт-Петербурга и Ленинградской области
- Международное право

7. Лицензионное программное обеспечение

1. Офисный пакет Libre Office;
2. Интернет-браузер Mozilla Firefox;
3. Dr.Web Desktop Security Suite (Комплексная защита)
4. Moodle 3.8.2.

8. 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 учебно-наглядных 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);

- специальные помещения для проведения занятий по дисциплине (в т.ч. лаборатории, оснащенные лабораторным оборудованием, в зависимости от степени сложности);
- 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.