МИНОБРНАУКИ РОССИИ

Ярославский государственный университет им. П.Г. Демидова

Кафедра цифровых технологий и машинного обучения

УТВЕРЖДАЮ

Декан физического факультета
_____ И.С. Огнев
(подпись)

«23» мая 2023 г.
.

Рабочая программа дисциплины
«Основы информационной безопасности»

Направление подготовки
«11.03.01 Радиотехника»

Направленность (профиль)
«00 Радиотехника»

Форма обучения
очная

Программа одобрена
на заседании кафедры
от «17» апреля 2023 года, протокол № 8

Программа одобрена НМК
физического факультета
протокол № 5 от «25» апреля 2023 года

Ярославль

1. Цели освоения дисциплины

Цель освоения дисциплины – подготовка в области основных принципов и методов информационной безопасности.

Задачи дисциплины:

- ознакомление с основными проблемами защиты информации в информационных системах;
- показ основных методов и средств, используемых при защите систем передачи и обработки информации;
- обучение стандартным приёмам защиты информации в компьютерных системах и локальных сетях.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам по выбору.

Она основывается на знаниях, умениях и навыках, полученных студентами при изучении дисциплин: «Теория вероятностей и математическая статистика», «Дискретная математика»,«Обработка и передача мультимедийной информации», «Операционные системы реального времени».

Она тесно связана с дисциплиной «Информационно-вычислительные сети», а также с рядом дисциплин по выбору.

Знания, умения и навыки, полученные при изучении данной дисциплины, могут использоваться студентами при выполнении выпускной квалификационной работы.

3. Планируемые результаты обучения по дисциплине, соотнесённые с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Профессиональные компетенции		
ПК-1. Способен осуществлять сбор и обработку исходных данных для решения поставленных профессиональных задач в области радиотехники, осуществлять поиск, анализ и выбор методов их решения	ИД_ПК-1.2 Проводит анализ и обоснованный выбор методов решения профессиональных задач в области радиотехники	**Знать:** - основы построения защищенных систем связи; - основные виды угроз для телекоммуникационных систем. **Уметь:** - выявлять и устранять потенциальные уязвимости, с позиций безопасности, информационных систем. **Владеть навыками:** - работы с нормативными документами; - сбора и анализа информации, необходимой для оценки защищенности телекоммуникационных систем.

4. Объём, структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет **3** зачёт. ед., **108** акад. час.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоёмкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)* Формы ЭО и ДОТ *(при наличии)*
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Введение	8		2				5,7	Устный опрос
2	Технологии защиты информации	8		12				15	Устный опрос
3	Стандарты по защите информации	8		10		2		15	Устный опрос
4	Общие критерии оценки защищенности информационных систем	8		10				14	Устный опрос
5	Каналы утечки информации и их анализ	8		6		2		14	Устный опрос
	Промежуточная аттестация	8					0,3		Зачёт
	ИТОГО	***8***		**40**		**4**	**0,3**	**63,7**	**108**
	в том числе с ЭО и ДОТ								

Содержание тем дисциплины

Тема №1

Введение

Предмет, цели, задачи и содержание курса «Основы информационной безопасности». Роль специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

Тема №2

Технологии защиты информации

Основные угрозы информации в компьютерных системах. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах, специфика возникновения угроз в открытых сетях, особенности защиты информации на узлах компьютерной сети, системные вопросы защиты программ и данных. Анализ рисков. Модель противника, возможности противника; параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера. Анализ критических технологий. Политика безопасности для информационных систем. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.

Тема №3

Стандарты по защите информации

Американский стандарт «Оранжевая книга». Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга». Европейский

стандарт по безопасности. Функциональные требования. Вопросы гарантий и эффективности. Стандарты и требования ФСТЭК РФ по технической защите информации. Система лицензирования и сертификации средств защиты. Аттестация защищенных систем. Структуры в РФ, обеспечивающие лицензирование и сертификацию. Нормативная база и ответственность за защиту информации в компьютерных системах.

Тема №4

Общие критерии оценки защищенности информационных систем

Подход к безопасности информационных систем и базовые концепции. Профиль защиты. Функции поддержки политики безопасности. Гарантии безопасности. Требования по безопасности информационных технологий. Оценки защищенности. Компоненты подсистем поддержки политики безопасности. Классы оценки безопасности. Требования к подсистемам аудита. Подсистемы подтверждения подлинности отправки и получения сообщения. Подсистемы разграничения доступа. Подсистемы аутентификации. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы. Подсистемы защиты связи.

Тема №5

Каналы утечки информации и их анализ

Открытые и закрытые каналы передачи информации. Управление конфигурацией. Установка систем сквозного и канального шифрования. Модернизация информационных технологий. Уровни гарантий.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения соответствующей дисциплине используются следующие образовательные технологии:

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекциях и в результате самостоятельной подготовки знаний.

Консультация – занятие перед проведением зачета, на котором проводится консультирование по изученному материалу, формам заданий итогового контроля, ответы на вопросы студентов по дисциплине.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT»http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Скляров Д.В. Искусство защиты и взлома информации. СПб.: БХВ-Петрербург, 2004.
2. Молдовян А.А. и др. Криптография: Учебник для вузов / Молдовян А.А., Молдовян Н.А., Советов Б.Я. СПб.: Лань, 2001.

б) дополнительная литература

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учебный курс - 2-е изд., перераб. и доп. М.: Горячая линия-Телеком, 2002.
2. Сидорин Ю.С. Технические средства защиты информации: учебное пособие. СПб.: СПбГПУ, 2005.
3. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. М.: ДМК, 2002.

в) ресурсы сети «Интернет»:

Сайты по вопросам информационной безопасности: http://www.itsec.ru, http://bugtraq.ru/, http://www.securitylab.ru/, http://iso27000.ru/

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в аудитории для практических занятий (семинаров) больше либо равно списочному составу группы обучающихся.

Автор:
Профессор кафедры
цифровых технологий и
машинного обучения, д. т. н. А.Л. Приоров

Приложение № 1 к рабочей программе дисциплины
«Основы информационной безопасности»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Устный опрос

1. CRC-алгоритмы обнаружения ошибок в транзакциях USB пакетов.
2. Безопасность беспроводных сетей стандарта 802.11.
3. Безопасностьсоединения bluetooth-устройств.
4. Протокол EAP.
5. Обзор технологии EDGE: основные принципы обеспечения безопасности.
6. Безопасностьтехнологии GPRS.
7. Технология безопасности в SIM-картах.
8. Методы защиты информации в мобильной связи 3-го поколения.
9. Технология GPRS и безопасность передачи данных.
10. Шифрование, основанное на местоположении: Использование GPS для повышения степени защиты данных.
11. Смарт-карты. Защита и безопасность.
12. Алгоритмы шифрования в сетях GSM.
13. Способы защиты CD от нелегального копирования.
14. Различные технологии защиты для цифрового видео.
15. Защита авторских прав в DVD и DivX.
16. Электронные ключи — комплексное решение проблемы пиратского копирования компьютерных программ.
17. Современная стеганография: принципы, основные носители и методы противодействия.
18. Безопасность TCP/IP.
19. Протоколраспределениякючей Kerberos.
20. Сетевые средства управления доступом.
21. Блочные симметричные шифры в SSL.
22. Безопасность электронной почты.
23. Атаки, основанные на переполнении буфера и контрмеры по их предотвращению.
24. Сравнение хеш-функций MD5 и SHA-1.
25. Сравнение алгоритмов Blowfish и DES.
26. Принципы построения систем биометрической аутентификации.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачёту

1. CRC-алгоритмы обнаружения ошибок в транзакциях USB пакетов.
2. Безопасность беспроводных сетей стандарта 802.11.
3. Безопасность соединения bluetooth-устройств.
4. Протокол EAP.
5. Обзор технологии EDGE: основные принципы обеспечения безопасности.
6. Безопасностьтехнологии GPRS.
7. Технология безопасности в SIM-картах.
8. Методы защиты информации в мобильной связи 3-го поколения.
9. Технология GPRS и безопасность передачи данных.
10. Шифрование, основанное на местоположении.
11. Использование GPS для повышения степени защиты данных.
12. Смарт-карты. Защита и безопасность.
13. Алгоритмы шифрования в сетях GSM.
14. Способы защиты CD от нелегального копирования.
15. Различные технологии защиты для цифрового видео.
16. Защита авторских прав в DVD и DivX.
17. Электронные ключи – комплексное решение проблемы пиратского копирования компьютерных программ.
18. Современная стеганография: принципы, основные носители и методы противодействия.
19. Безопасность TCP/IP.
20. Протокол распределения ключей Kerberos.
21. Сетевые средства управления доступом.
22. Блочные симметричные шифры в SSL.
23. Безопасность электронной почты.
24. Атаки, основанные на переполнении буфера и контрмеры по их предотвращению.
25. Сравнение хеш-функций MD5 и SHA-1.
26. Сравнение алгоритмов Blowfish и DES.
27. Принципы построения систем биометрической аутентификации.
28. Виды данных, используемые при построении систем биометрической аутентификации.

Критерии оценивания ответов на вопросы билета

Критерий	Пороговый уровень (на «удовлетворительно»)	Продвинутый уровень (на «хорошо»)	Высокий уровень (на «отлично»)
Соответствие ответа вопросу	Хотя бы частичное (не относящееся к вопросу не подлежит проверке)	Полное	Полное
Наличие примеров	Имеются отдельные примеры	Много примеров	Есть практически ко всем утверждениям
Содержание ответа	Понятийные вопросы изложены с классификациями, проблемные с постановкой проблемы и изложением различных точек зрения. Имеются ошибки или пробелы.	Ответ почти пол-ный, без ошибок,не хватает отдель-ных элементов и тонкостей	Исчерпываю-щий полный ответ

2. Описание процедуры выставления оценки

Изучение дисциплины заканчивается зачётом. Для подготовки ответа на вопрос билета отводится не менее 40 минут.

Оценка «зачтено» выставляется, если ответ на вопрос билета дан не ниже, чем на пороговом уровне.

Оценка «не зачтено» выставляется, если ответ на вопрос билета дан ниже, чем на пороговом уровне.

Приложение № 2 к рабочей программе дисциплины
«Основы информационной безопасности»

Методические указания для студентов по освоению дисциплины

Основной формой усвоения учебного материала по дисциплине «Основы информационной безопасности» является самостоятельная работа студента, причём в достаточно большом объеме. По всем темам предусмотрены задания самостоятельной работы, на которых происходит закрепление изученного материала и отработка необходимых навыков.

Изучение дисциплины заканчивается зачетом. Оценка выставляется на основании уровня сформированности указанных компетенций, который оценивается как средняя оценка по совокупности параметров: оценки за самостоятельные задания и ответы на вопросы билета.

Освоить вопросы данной дисциплины самостоятельно студенту достаточно сложно. Посещение всех предусмотренных лекций и практических занятий является совершенно необходимым. Без упорных и регулярных самостоятельных занятий в течение семестра сдать зачёт практически невозможно.