Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Райхерт Татьяна Николаевна
Должность: Директор
Дата подписания: 07.03.2022 15:10:00
Уникальный программный ключ:
c914df807d771447164c08ee17f8e2f93dde816b

Министерство просвещения Российской Федерации
Нижнетагильский государственный социально-педагогический институт (филиал)
федерального государственного автономного образовательного учреждения
высшего образования
«Российский государственный профессионально-педагогический университет»

Факультет естествознания, математики и информатики
Кафедра информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.05.04 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования	Бакалавриат
Направление подготовки	09.03.03 Прикладная информатика
Профили	«Прикладная информатика в управлении IT-проектами»
Форма обучения	Очная

Нижний Тагил
2021

Рабочая программа дисциплины «Информационная безопасность». Нижнетагильский государственный социально-педагогический институт (филиал) федерального государственного автономного образовательного учреждения высшего образования «Российский государственный профессионально-педагогический университет», Нижний Тагил, 2021. 9 с.

Настоящая программа составлена в соответствии с требованиями ФГОС ВО по направлению 09.03.03 Прикладная информатика (№ 922 от 19.09.2017)

Автор: канд. пед. наук, доцент, доцент кафедры ИТ _____ Е. С. Васева

Одобрен на заседании кафедры ИТ 24 апреля 2021 г., протокол № 9.

Заведующий кафедрой ИТ _____Мащенко М. В.

Рекомендован к печати методической комиссией ФЕМИ 27 апреля 2021 г., протокол № 6.

Председатель методической комиссии ФЕМИ _____Касимова Н. З.

© Нижнетагильский государственный социально-педагогический институт (филиал) федерального государственного автономного образовательного учреждения высшего образования «Российский государственный профессионально-педагогический университет», 2021.
© Е. С. Васева, 2021.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 4
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 4
3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ 4
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 5
4.1. Объем дисциплины и виды контактной и самостоятельной работы 5
4.2. Учебно-тематический план 5
5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 6
6. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ 7
6.1. Организация самостоятельной работы студентов 7
6.2. Организация текущего контроля и промежуточной аттестации 7
7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ 7
МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 9

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины — формирование компетенций в области обеспечения информационной безопасности в процессе решения профессиональных задач.

Задачи дисциплины:

–раскрыть понятийный аппарат курса и сформировать целостную систему знаний о современных моделях обеспечения безопасности управления информационными ресурсами;

–познакомить студентов с правовыми основами обеспечения информационной безопасности и технологиями обеспечения информационной безопасности средствами систем обеспечения безопасности информации;

–сформировать умения решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности;

–показать основные направления в управлении информационной безопасностью на предприятии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Информационная безопасность является частью учебного плана по направлению подготовки 09.03.03 Прикладная информатика. Дисциплина включена в Блок Б.1 «Дисциплины (модули)» и является составной частью раздела Б1.О. «Обязательная часть». Реализуется кафедрой информационных технологий.

Дисциплина «Информационная безопасность» базируется на компетенциях, полученных при изучении дисциплин «Информатика и программирование», «Информационные системы и технологии», «Теория систем и системный анализ», «Операционные системы» и ряда других дисциплин. Теоретические знания и практические навыки, полученные при изучении дисциплины, могут быть использованы студентами при подготовке курсовых работ и выпускной квалификационной работы.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование и развитие следующих компетенций:

Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной 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	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3. Умеет готовить обзоры, аннотации, рефераты, научные доклады, публикации, и библиографию по научно-исследовательской работе с учетом требований

Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
	информационной безопасности
ПК-8 – Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-8.1. Знает основы информационной безопасности при организации ИТ инфраструктуры
	ПК-8.2. Знает основные возможности и правила для организации ИТ инфраструктуры предприятия
	ПК-8.3.Умеет создать безопасную ИТ инфраструктуру предприятия

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды контактной и самостоятельной работы

Вид работы	Кол-во часов
	Форма обучения
	очная
Общая трудоемкость дисциплины по учебному плану	**108**
Контактная работа, в том числе:	**38**
Лекции	12
Лабораторные занятия	26
Самостоятельная работа, в том числе:	**70**
Самоподготовка к текущему контролю знаний	61
Подготовка к итоговому контролю знаний	9

4.2. Учебно-тематический план

Наименование разделов и тем дисциплины (модуля)	Всего, часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы		
Тема 1. Введение в проблему информационной безопасности	10	2		8	
Тема 2. Угрозы информационной безопасности и методы их реализации	12	2	2	8	тест, отчет по лабораторной работе
Тема 3. Правовые аспекты защиты информации	14	2	4	8	тест, отчет по лабораторной работе
Тема 4. Административный уровень обеспечения информационной безопасности	20	2	6	12	тест, отчет по лабораторной работе
Тема 5. Программно-технический уровень обеспечения информационной безопасности	43	4	14	25	тест, отчет по лабораторной работе
Зачет	9	0	0	9	

Наименование разделов и тем дисциплины (модуля)	Всего, часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы		
Итого	**108**	**12**	**26**	**70**	

4.3. Содержание дисциплины

Тема 1. Введение в проблему информационной безопасности.

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.

Тема 2. Угрозы информационной безопасности и методы их реализации.

Виды возможных нарушений информационной системы. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Тема 3. Правовые аспекты защиты информации.

Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, защиты персональных данных, защиты коммерческой тайны, электронной подписи. Стандарты в области информационной безопасности. Компьютерные преступления.

Тема 4. Административный уровень обеспечения информационной безопасности.

Основные понятия. Концепция безопасности. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Анализ рисков информационной системы предприятия. Стратегии управления рисками. Частная модель угроз информационной безопасности. Управление персоналом.

Тема 5. Программно-технический уровень обеспечения информационной безопасности.

Основные сервисы программно-технического уровня обеспечения информационной безопасности. Идентификация и аутентификация. Парольная аутентификация. Логическое управление доступом. Компьютерные вирусы, классификация. Признаки заражения компьютера вредоносным программным обеспечением. Средства защиты от компьютерных вирусов. Протоколирование и аудит. Криптографические средства защиты. Экранирование.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Обучение по дисциплине «Информационная безопасность» целесообразно построить с использованием компетентностного подхода, в рамках которого образовательный процесс строится с учетом специфики будущей профессиональной деятельности студентов. Лекционные занятия должны стимулировать познавательную ативность студентов, поэтому в ходе лекций необходимо обращение к примерам, взятым из практики, включение проблемных вопросов и ситуаций.

Основными методами, используемыми на практических занятиях, будут: практикум с использованием практико-ориентированных задач, метод проектов, метод проблемных ситуаций.

6. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Организация самостоятельной работы студентов

Самостоятельная работа студентов включает изучение вопросов, вынесенных за рамки аудиторных занятий, расширение и углубление знаний по темам, рассмотренным на лекционных занятиях. При подготовке к практическим занятиям студенты изучают учебные тексты, выполняют тренировочные задания, решают задачи, разрабатывают проекты, готовят доклады, рассматривают способы обеспечения информационной безопасности в информационных системах. Лабораторные работы проверяются преподавателем по отчетам, устные выступления оцениваются в ходе практического занятия.

Тематика лабораторных занятий

1. Анализ угроз информационной безопасности.
2. Анализ основных нормативных документов в области информационной безопасности.
3. Политика информационной безопасности организации. Частная модель угроз
4. Разработка локальных нормативных документов
5. Обеспечение безопасности при работе с документами
6. Возможности защиты информации в операционной системе. Логическое управление доступом
7. Основные признаки присутствия на компьютере вредоносных программ
8. Установка и предварительная настройка антивирусной программы
9. Работа с реестром
10. Протоколирование в ИС
11. Методы криптографии

6.2. Организация текущего контроля и промежуточной аттестации

Текущий контроль усвоения знаний ведется по итогам представления выполненных самостоятельных заданий и защиты отчетов по лабораторным работам; участия в дискуссиях на лекционных занятиях, проверки результатов тестирования.

Текущий контроль учебных достижений студентов может быть проведен с использованием накопительной балльно-рейтинговой системы оценки (НБРС). В этом случае оценке в баллах подлежат как результаты текущих опросов, так и результаты выполнения практических заданий. Для оценки используется шкала баллов, разработанная в соответствии с Положением о НБРС.

Промежуточная аттестация по данной дисциплине проводится в форме зачета с оценкой в 7 семестре.

Примеры вопросов к зачету

1. Проблема информационной безопасности. Основные понятия.
2. Угрозы информационной безопасности.
3. Уровни обеспечения информационной безопасности.
4. Правовое обеспечение информационной безопасности. Основные нормативные документы.
5. ФЗ «О персональных данных».
6. Концепция информационной безопасности предприятия.
7. Политика информационной безопасности предприятия.

8. Анализ рисков информационной системе предприятия.
9. Стратегии управления рисками.
10. Процедурные меры обеспечени информационной безопасности.
11. Основные сервисы программно-технического уровня обеспечения информационной безопасности.
12. Идентификация и аутентификация.
13. Парольная аутентификация.
14. Биометрическая аутентификация.
15. Логическое управление доступом.
16. Компьютерные вирусы, классификация.
17. Признаки заражения компьтера вредоносным программным обеспечением.
18. Средства защиты от компьютерных вирусов.
19. Протоколирование и аудит.
20. Экранирование.
21. Классификация криптографических систем.
22. Симметричные алгоритмы шифрования.
23. Асимметричные алгоритмы шифрования.
24. Криптографические протоколы.
25. Электронная цифровая подпись.
26. Защита информации в сервисах электронных платежей.
27. Криптоанализ и атаки на криптосистемы.
28. Классическая стеганография.
29. Компьютерная стеганография.
30. Удаленные угрозы в вычислительных сетях.
31. Принципы защиты распределенных вычислительных сетей.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Основная литература: *указывается до 5 наименований не старше 5 лет*

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

Дополнительная литература: *указывается до 5 наименований не старше 5 лет*

1. Акмаров, П. Б. Кодирование и защита информации : учебное пособие / П. Б. Акмаров. — Ижевск : Ижевская ГСХА, 2016. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133975 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

2. Бондаренко, И. С. Методы и средства защиты информации : учебное пособие / И. С. Бондаренко, Ю. В. Демчишин. — Москва : МИСИС, 2018. — 32 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/115269 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

3. Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — ISBN 978-5-7641-1008-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/101600 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

4. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441287 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

5. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 96 с. — ISBN 978-5-8114-4040-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114697 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

Программное обеспечение общего и профессионального назначения: LibreOffice, LibreOffice Base, LibreOffice Impress, Kaspersky Endpoint Security – 300, Adobe Reader, браузер Google chrome/Mozilla Firefox, VM VirtualBox.

Информационные системы и платформы:

1. Среда электронного обучения «Русский Moodle» (https://do.ntspi.ru/).
2. Интернет-платформа онлайн-курсов со свободным кодом «Open edX» (https://www.edx.org/).
3. Электронная информационно-образовательная среда РГППУ (https://eios.rsvpu.ru/).
4. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Учебная аудитория для проведения занятий лекционного типа.
2. Учебная аудитория для проведения занятий лабораторного типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами с доступом в интернет, доступом в электронную информационно-образовательною среду, программное обеспечение общего и профессионального назначения.