МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

**УТВЕРЖДАЮ**
Проректор по учебной работе
Д.Ш. Султанова
«07» июня 2021 г.

Рабочая программа дисциплины в виде электронного документа выгружена из информационной системы управления университетом и соответствует оригиналу
Простая электронная подпись, ID подписи: 1060
Подписал Проректор по учебной работе Д.Ш. Султанова
Дата 07.06.2021

# РАБОЧАЯ ПРОГРАММА
по дисциплине **«КОНФИГУРИРОВАНИЕ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»**

| | |
|---|---|
| Специальность: | 10.05.05 Безопасность информационных технологий в правоохранительной сфере |
| Специализация: | Технологии защиты информации в правоохранительной сфере |
| Квалификация выпускника: | Специалист по защите информации |
| Форма обучения: | Очная |
| Институт: | Инженерный химико-технологический институт |
| Факультет: | Факультет экологической, технологической и информационной безопасности |
| Кафедра-разработчик: | Кафедра «Информационная безопасность» |
| Курс; семестр | 5; 9 |

| Вид нагрузки | Часы | Зачётные единицы |
|---|---|---|
| Лекция | 18 | 0,5 |
| Лабораторная работа | 27 | 0,75 |
| Контроль самостоятельной работы | 63 | 1,75 |
| Самостоятельная работа | 72 | 2 |
| Форма аттестации: Дифференцированный зачет (9 сем) | | |
| Всего | 180 | 5 |

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1461 от 22.11.2020) по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере для специализации «Технологии защиты информации в правоохранительной сфере» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Старший преподаватель В.И. Нурулин

---

**С О Г Л А С О В А Н О**

Рабочая программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность», протокол от 26.05.2021 г. № 10.

Заведующий кафедрой ***Согласовано*** В.А. Богомолов

**У Т В Е Р Ж Д Е Н О**

Начальник центра УМЦ ***Утверждаю*** Л.А. Китаева

**1. Цели освоения дисциплины**

Целями освоения дисциплины «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» являются:

а) знакомство с основными понятиями в корпоративных информационных системах;

б) получение теоретических знаний по безопасности корпоративных информационных систем;

в) получение навыков защиты корпоративных информационных систем.

**2. Место дисциплины в структуре образовательной программы**

Дисциплина «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» относится к формируемой участниками образовательных отношений части ООП и формирует у обучающихся по специализации «Технологии защиты информации в правоохранительной сфере» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Информатика
2. Средства и системы технического обеспечения обработки, хранения и передачи информации

Дисциплина «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Контроль безопасности в компьютерных сетях

**3. Компетенции обучающегося, формируемые в результате освоения дисциплины**

**ПК -2 Способен обеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем**

ПК -2.1. Знает принципы построения компьютерных сетей, порядок реализации методов и средств межсетевого экранирования, источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению, принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

ПК -2.2. Умеет оценивать угрозы безопасности информации в компьютерных сетях, настраивать правила фильтрации пакетов в компьютерных сетях, оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях, обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях

ПК -2.3. Владеет навыками применения программно-аппаратных средств защиты информации в компьютерных сетях и управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях

**В результате освоения дисциплины обучающийся должен**

**Знать:**

- как обеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем;
- принципы построения компьютерных сетей, порядок реализации методов и средств

межсетевого экранирования, источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению, принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- как оценивать угрозы безопасности информации в компьютерных сетях, настраивать правила фильтрации пакетов в компьютерных сетях, оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях, обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях;
- навыки применения программно-аппаратных средств защиты информации в компьютерных сетях и управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях

**Уметь:**

- обеспечитьобеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем;
- строить компьютерные сети, порядок реализации методов и средств межсетевого экранирования, источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению, принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- оценивать угрозы безопасности информации в компьютерных сетях, настраивать правила фильтрации пакетов в компьютерных сетях, оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях, обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях;
- применять программно-аппаратные средства защиты информации в компьютерных сетях и управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях

**Владеть:**

- обеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем;
- навыки построения компьютерных сетей, порядок реализации методов и средств межсетевого

экранирования, источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению, принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

- навыки оценивать угрозы безопасности информации в компьютерных сетях, настраивать правила фильтрации пакетов в компьютерных сетях, оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях, обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях;

- навыками применения программно-аппаратных средств защиты информации в компьютерных сетях и управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях

## 4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 5 зачетных единиц, 180 часов.

| № п/п | Раздел дисциплины | Семе-стр | Виды учебной работы (в часах) | | | | | Оценочные средства для проведения текущей и промежу-точной аттестации |
|---|---|---|---|---|---|---|---|---|
| | | | Лекция | Практические занятия | Лабора-торные | КСР | СРС | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1. | Конфигурирование компьютерных систем и программного обеспечения | 9 | 8 | | 19 | 57 | 66 | Лабораторная работа |
| 2. | Обеспечение безопасности компьютерных систем и программного обеспечения | 9 | 10 | | 8 | 6 | 6 | |
| | **Итого по семестру** | **9** | **18** | | **27** | **63** | **72** | **Дифференцированный зачет** |

## 5. Содержание лекционных занятий по темам

| № п/п | Раздел дисциплины | Часы | Тема лекционного занятия | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 1. | Конфигурирование компьютерных систем и программного обеспечения | 2 | Технология аутентификации и обеспечение безопасностиоперационных систем. Технологии межсетевых экранов | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 2. | | 2 | Принцип криптографической защиты инфомации | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 3. | | 2 | Построение и организация комплексной системы защиты информации | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 4. | | 2 | Мэжсетевые экраны. VPN. | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |

| № п/п | Раздел дисциплины | Часы | Тема лекционного занятия | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 5. | Обеспечение безопасности компьютерных систем и программного обеспечения | 2 | Технологии применения комплексной системы защиты информации в телекоммуникационных системах | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 6. | | 2 | Вредоносные программы: классификация, методы обнаружения | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 7. | | 6 | Распределенные информационные системы. | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| | **ВСЕГО** | **18** | | |

## 6. Содержание практических/семинарских занятий

Проведение практических/семинарских занятий не предусмотрено учебным планом

## 7. Содержание лабораторных занятий

| № п/п | Раздел дисциплины | Часы | Тема занятия | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 6 |
| 1. | Конфигурирование компьютерных систем и программного обеспечения | 12 | Законодательный уровень информационной безопасности | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 2. | | 3 | Защита информации в распределенных компьютеных сетях | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 3. | | 2 | Технические средства комплексной системы защиты информации | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 4. | | 2 | VPN | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 5. | Обеспечение безопасности компьютерных систем и программного обеспечения | 4 | Основные методы обеспечения качества функционирования | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 6. | | 2 | Анализ и управление политикой иформационной безопасности на объекте с использованием системы "Кондор" | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 7. | | 2 | Вредоносные программы: классификация, методы обнаружения | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| | **ВСЕГО** | **27** | | |

## 8. Самостоятельная работа

| № п/п | Темы, выносимые на самостоятельную работу | Часы | Форма СРС | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 5 | 6 |
| 1. | Основные методы внедрения и анализа функционирования программного обеспечения | 11 | подготовка к лабораторной работе | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 2. | Загрузка и установка программного обеспечения | 10 | подготовка к лабораторной работе | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |

| № п/п | Темы, выносимые на самостоятельную работу | Часы | Форма СРС | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 5 | 6 |
| 3. | схемы сетевой защиты на базе МЭ, ее основные варианты архетиктуры | 12 | подготовка к лабораторной работе | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 4. | Мэжсетевые экраны. VPN. | 33 | подготовка к лабораторной работе | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 5. | Аудит комплексной защиты | 2 | подготовка к лабораторной работе | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 6. | Методы и средства защиты компьютерных систем | 2 | подготовка к лабораторной работе | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 7. | Вредоносные программы: классификация, методы обнаружения | 2 | подготовка к лабораторной работе | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| | **ВСЕГО** | **72** | | |

### 8.1 Контроль самостоятельной работы

| № п/п | Темы, выносимые на самостоятельную работу | Часы | Форма КСР | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 5 | 6 |
| 1. | Алгоритмы шифрования, цифровой подписи | 4 | прием лабораторной работы | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 2. | Биометрическая аутентификация, аутентификация на основе пин-КОДА | 4 | прием лабораторной работы | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 3. | классификация угроз безопасности, пути реализации угроз | 17 | прием лабораторной работы | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 4. | Мэжсетевые экраны. VPN. | 32 | прием лабораторной работы | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 5. | Основные методы обеспечения качества функционирования | 2 | прием лабораторной работы | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 6. | Методы и средства защиты компьютерных систем | 2 | прием лабораторной работы | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| 7. | Вредоносные программы: классификация, методы обнаружения | 2 | прием лабораторной работы | ПК -2.1<br>ПК -2.2<br>ПК -2.3 |
| | **ВСЕГО** | **63** | | |

### 9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» используется рейтинговая система. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО КНИТУ.

Рейтинговая оценка формируется на основании текущего и промежуточного контроля. За контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

| Оценочные средства | Кол-во | Мин.баллов | Макс.баллов |
|---|---|---|---|
| **9-й семестр** | | | |
| Лабораторная работа | 7 | 60 | 100 |

| | | | |
|---|---|---|---|
| **Итого** | | **60** | **100** |

## 10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации и итоговой аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

## 11. Информационно-методическое обеспечение дисциплины

### 11.1. Основная литература

При изучении дисциплины «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» в качестве основных источников информации рекомендуется использовать следующую литературу:

| Основные источники информации | Количество экземпляров |
|---|---|
| С. В. Родин, Г. В. Перминов, А. В. Скрыпников [и др.], Безопасность систем баз данных [Электронный ресурс] Учебное пособие: Воронеж : Воронежский государственный университет инженерных технологий, 2015 | http://www.iprbookshop.ru/50628.html<br>Режим доступа: по подписке КНИТУ |
| В. А. Астапчук, П. В. Терещенко, Корпоративные информационные системы: требования при проектировании [Прочее] Учебное пособие для вузов: Москва : Юрайт, 2020 | https://urait.ru/bcode/453261<br>Режим доступа: по подписке КНИТУ |
| А. В. Курбесов, Корпоративные информационные системы [Прочее] учебное пособие: Ростов-на-Дону : Издательско-полиграфический комплекс РГЭУ (РИНХ), 2018 | http://biblioclub.ru/index.php?page=book&id=567042<br>Режим доступа: по подписке КНИТУ |
| А. Ю. Никитаева, Корпоративные информационные системы [Прочее] Учебное пособие: Таганрог : Издательство ТТИ ЮФУ, 2017 | http://znanium.com/go.php?id=996036<br>Режим доступа: по подписке КНИТУ |

### 11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

| Дополнительные источники информации | Количество экземпляров |
|---|---|
| В. Кияев, О. Граничин, Безопасность информационных систем [Прочее] курс: Москва : Национальный Открытый Университет «ИНТУИТ», 2016 | http://biblioclub.ru/index.php?page=book&id=429032<br>Режим доступа: по подписке КНИТУ |
| А. В. Никулин,, В. В. Артюшенко,, Компьютерные сети и телекоммуникации [Прочее] учебно-методическое пособие по русскому языку как иностранному: Новосибирск : Новосибирский государственный технический университет, 2020 | http://www.iprbookshop.ru/99345.html<br>Режим доступа: по подписке КНИТУ |
| В. В. Артюшенко,, А. В. Никулин,, Компьютерные сети и телекоммуникации [Прочее] учебно-методическое пособие по русскому языку как иностранному: Новосибирск : Новосибирский государственный технический университет, | http://www.iprbookshop.ru/99345.html<br>Режим доступа: по подписке КНИТУ |

| | |
|---|---|
| 2020 | |
| А. В. Кузин, Д.А. Кузин, Компьютерные сети [Прочее] Учебное пособие: Москва : Издательство "ФОРУМ", 2020 | http://znanium.com/go.php?id=1088380 Режим доступа: по подписке КНИТУ |
| М. В. Дибров, Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 [Прочее] Учебник и практикум Для СПО: Москва : Юрайт, 2020 | https://urait.ru/bcode/452574 Режим доступа: по подписке КНИТУ |
| М. В. Дибров, Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 [Прочее] Учебник и практикум Для СПО: Москва : Юрайт, 2020 | https://urait.ru/bcode/453065 Режим доступа: по подписке КНИТУ |
| Ибе Оливер, Компьютерные сети и службы удаленного доступа [Электронный ресурс] : Саратов : Профобразование, 2019 | http://www.iprbookshop.ru/87999.html Режим доступа: по подписке КНИТУ |

**11.3. Электронные источники информации**

При изучении дисциплины «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» предусмотрено использование электронных источников информации:

1. Электронный каталог УНИЦ КНИТУ: Режим доступа: http://ruslan.kstu.ru/
2. ЭБС «Лань»:Режим доступа: https://e.lanbook.com
3. Образовательная платформа «Юрайт»: Режим доступа: https://urait.ru/
4. ЭБС «Znanium.com»: Режим доступа: http://znanium.com/
5. ЭБС Университетская библиотека онлайн: Режим доступа: http://biblioclub.ru/
6. ЭБС IPRbooks: Режим доступа: http://www.iprbookshop.ru/
7. ЭБС BOOK.ru : Режим доступа: https://www.book.ru/
8. Научная электронная библиотека https://elibrary.ru/

**УНИЦ**
***Согласовано***

**11.4. Профессиональные базы данных и информационные справочные системы**

Базы данных
Scopus Доступ свободный: www.scopus.com
Web of Science Доступ свободный: apps.webofknowledge.com

Информационные справочные системы
Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru
Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

**12. Материально-техническое обеспечение дисциплины**

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое в учебном процессе при освоении дисциплины «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения»:

Офисные и деловые программы: ABBYY FineReader 9.0 проф;
Офисные и деловые программы: MS Office 2007 Russian;
Офисные и деловые программы: MS Office 2007 Professional Russian;
Офисные и деловые программы: MS Office 2010-2016 Standard

Архиватор 7 Zip
Блокнот Notepad
Яндекс Браузер

1. Виртуальные машины VirtualBOX (GNU GENERAL PUBLIC LICENSE)
2. Симулятор сетей GNS3 (GNU GENERAL PUBLIC LICENSE)
3. Операционная система Linux (Fedora, Ubuntu). (GNU GENERAL PUBLIC LICENSE)
4. RADIUS сервер (GNU GENERAL PUBLIC LICENSE)
5. Sendmail - SMTP сервер (Sendmail License)
6. POP3 сервер (BSD License)
7. IMAP4 сервер (BSD License)
8. NTP сервер (BSD License)
9. Межсетевой экран iptables (GNU GENERAL PUBLIC LICENSE)
10. Межсетевой экран Firewalld (GNU GENERAL PUBLIC LICENSE)
11. Сканер сетевой безопасности nmap (GNU GENERAL PUBLIC LICENSE)
12. Система обнаружения атак snort (GNU GENERAL PUBLIC LICENSE)
13. Система синхронизации данных rsync

Учебные аудитории для проведения учебных занятий оснащены оборудованием:
1. Аудитория П-7;
техническими средствами обучения:
1. Типовой комплект учебного оборудования «Глобальные компьютерные сети» ,
2. Типовой комплект учебного оборудования «Корпоративные компьютерные сети» .

Помещения для самостоятельной работы оснащены компьютерной техникой:
1. Аудитория И1-107,
с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

**13. Образовательные технологии**

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» составляет 9 ч.

В процессе освоения дисциплины «Конфигурирование и обеспечение безопасности компьютерных систем и программного обеспечения» используются следующие образовательные технологии:

• творческие задания;
• работа в малых группах;
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• системы дистанционного обучения.