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 **«ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»**

| | |
|---|---|
| Направление подготовки: | 10.03.01 Информационная безопасность |
| Профиль: | Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности) |
| Квалификация выпускника: | Бакалавр |
| Форма обучения: | Очно-заочная |
| Институт: | Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия" |
| Факультет: | Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия" |
| Кафедра-разработчик: | Казанский межвузовский инженерный центр "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет" |
| Курс; семестр | 4; 8 |

| Вид нагрузки | Часы | Зачётные единицы |
|---|---|---|
| Лекция | 18 | 0,5 |
| Лабораторная работа | 36 | 1 |
| Контроль самостоятельной работы | 45 | 1,25 |
| Самостоятельная работа | 81 | 2,25 |
| Форма аттестации: Дифференцированный зачет (8 сем) | | |
| Всего | 180 | 5 |

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1427 от 17.11.2020) по направлению подготовки 10.03.01 Информационная безопасность для профиля «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент А.С. Балыбердин

---

**С О Г Л А С О В А Н О**

Рабочая программа рассмотрена и одобрена на заседании Казанского межвузовского инженерного центра "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет", протокол от 19.05.2021 г. № 6.

Директор ***Согласовано*** А.Ф. Махоткин

**У Т В Е Р Ж Д Е Н О**

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

**1. Цели освоения дисциплины**

Целями освоения дисциплины «Защита информации от утечки по техническим каналам» являются:

- изучение современных методов и средств инженерно-технической защиты информации;
- формирование умений применения методов и средств инженерно-технической защиты информации.
- освоение принципов и методологии инженерно-технической защиты информации;
- знакомство с возможностями и порядком применения инженерно-технических средств защиты информации;
- формирование первоначальных навыков проектирования систем инженерно-технической защиты информации.

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

Дисциплина «Защита информации от утечки по техническим каналам» относится к обязательной части ООП и формирует у обучающихся по профилю «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Защита информации от утечки по техническим каналам» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Информатика
2. Информационные технологии в информационной безопасности
3. Основы информационной безопасности
4. Сети и системы передачи информации
5. Теория информации

Дисциплина «Защита информации от утечки по техническим каналам» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Комплексная система защиты информации
2. Основы управления информационной безопасностью
3. Подготовка к процедуре защиты и защита выпускной квалификационной работы
4. Производственная практика (преддипломная практика)
5. Производственная практика (Эксплуатационная практика)

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

**ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;**

ОПК-9.1. Знает современные достижения науки и техники в области защиты информации, современные принципы рационального выбора средств защиты в зависимости от вида объекта защиты, системный подход к выполнению и организации

ОПК-9.2. Умеет проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ОПК-9.3. Владеет навыками эффективного применения средств криптографической защиты информации, средств технической защиты информации, сетей и систем передачи информации при решении задач профессиональной деятельности

**В результате освоения дисциплины обучающийся должен**

**Знать:**

основы теории информационной безопасности, классификацию и основное содержание нормативных документов в данной области

**Уметь:**

проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

выбирать режимы работы программно-аппаратных средств криптографической и технической защиты информации в операционных системах, настраивает правила фильтрации пакетов в компьютерных сетях

**Владеть:**

навыками по реализации технологий, направленных на обеспечение информационной безопасности

## 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. | Методы, способы и средства технической защиты информации | 8 | 8 | | 16 | 22 | 39 | Лабораторная работа; Реферат |
| 2. | Организация технической защиты информации | 8 | 10 | | 20 | 23 | 42 | |
| | **Итого по семестру** | **8** | **18** | | **36** | **45** | **81** | **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. | Методы, способы и средства технической защиты информации | 4 | Концепция технической защиты информации | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 2. | | 4 | Способы технической охраны | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 3. | Организация технической защиты информации | 6 | Организационные и технические меры технической защиты информации в государственных и коммерческих структурах | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 4. | | 4 | Системный подход к технической защите информации | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| | **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. | Методы, способы и средства технической защиты информации | 8 | Средства перехвата информации в оптическом диапазоне волн | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 2. | | 8 | Средства перехвата информации в каналах, образованных средствами вычислительной техники | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 3. | Организация технической защиты информации | 10 | Моделирование объекта защиты | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 4. | | 10 | Моделирование технических каналов утечки информации | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| | **ВСЕГО** | **36** | | |

## 8. Самостоятельная работа

| № п/п | Темы, выносимые на самостоятельную работу | Часы | Форма СРС | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 5 | 6 |
| 1. | Средства перехвата информации в оптическом диапазоне волн | 20 | написание реферата, подготовка к лабораторной работе | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 2. | Средства перехвата информации в каналах, образованных средствами вычислительной техники | 19 | написание реферата, подготовка к лабораторной работе | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 3. | Моделирование объекта защиты | 22 | написание реферата, подготовка к лабораторной работе | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 4. | Моделирование технических каналов утечки информации | 20 | написание реферата, подготовка к лабораторной работе | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| | **ВСЕГО** | **81** | | |

### 8.1 Контроль самостоятельной работы

| № п/п | Темы, выносимые на самостоятельную работу | Часы | Форма КСР | Индикаторы достижения компетенции |
|---|---|---|---|---|
| 1 | 2 | 3 | 5 | 6 |
| 1. | Средства перехвата информации в оптическом диапазоне волн | 11 | прием лабораторной работы, проверка реферата | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 2. | Средства перехвата информации в каналах, образованных средствами вычислительной техники | 11 | прием лабораторной работы, проверка реферата | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 3. | Моделирование объекта защиты | 11 | прием лабораторной работы, проверка реферата | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| 4. | Моделирование технических каналов утечки информации | 12 | прием лабораторной работы, проверка реферата | ОПК-9.1<br>ОПК-9.2<br>ОПК-9.3 |
| | **ВСЕГО** | **45** | | |

## 9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Защита информации от утечки по техническим каналам» 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 |
|---|---|---|---|
| **8-й семестр** | | | |
| Лабораторная работа | 4 | 52 | 80 |
| Реферат | 1 | 8 | 20 |
| **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 «Защита информации от утечки по техническим каналам» в качестве основных источников информации рекомендуется использовать следующую литературу:

| Основные источники информации | Количество экземпляров |
|---|---|
| А. В. Зенков, Информационная безопасность и защита информации [Прочее] Учебное пособие для вузов: Москва : Юрайт, 2021 | https://urait.ru/bcode/477968<br>Режим доступа: по подписке КНИТУ |
| А.П. Жук, Е.П. Жук, Защита информации [Прочее] Учебное пособие: Москва : Издательский Центр РИОР, 2021 | http://znanium.com/catalog/document?id=367588<br>Режим доступа: по подписке КНИТУ |
| П. Б. Хорев, Программно-аппаратная защита информации [Прочее] Учебное пособие: Москва : ООО "Научно-издательский центр ИНФРА-М", 2020 | http://new.znanium.com/go.php?id=1035570<br>Режим доступа: по подписке КНИТУ |

### 11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

| Дополнительные источники информации | Количество экземпляров |
|---|---|
| Москвитин Г.И., Комплексная защита информации в организации [Прочее] Монография: Москва : Русайнс, 2020 | https://www.book.ru/book/934814<br>Режим доступа: по подписке КНИТУ |
| И.С. Клименко, Информационная безопасность и защита информации: модели и методы управления [Прочее] Монография: Москва : ООО "Научно-издательский центр ИНФРА-М", 2020 | http://new.znanium.com/go.php?id=1018665<br>Режим доступа: по подписке КНИТУ |
| В.Ф. Шаньгин, Комплексная защита информации в корпоративных системах [Прочее] Учебное пособие: Москва : Издательский Дом "ФОРУМ", 2020 | http://znanium.com/go.php?id=1093695<br>Режим доступа: по подписке КНИТУ |
| Е.К. Баранова, А.В. Бабаш, Информационная безопасность и защита информации [Прочее] Учебное пособие: Москва : Издательский Центр РИОР, 2020 | http://znanium.com/go.php?id=1114032<br>Режим доступа: по подписке КНИТУ |
| А. А. Внуков, Основы информационной безопасности: защита информации [Прочее] | https://urait.ru/bcode/467356<br>Режим доступа: по подписке КНИТУ |

| | |
|---|---|
| Учебное пособие Для СПО: Москва : Юрайт, 2020 | |

**11.3. Электронные источники информации**

При изучении дисциплины «Защита информации от утечки по техническим каналам» 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 IPR SMART: 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
Wiley Online Library: https://onlinelibrary.wiley.com/
Springer Nature: https://link.springer.com/
zbMath : https://zbmath.org/

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 «Защита информации от утечки по техническим каналам»:

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

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:
Аудитория 351-А;
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
14. компьютер/ноутбук
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:
Аудитория Г-407,
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 «Защита информации от утечки по техническим каналам» составляет 9 ч.

В процессе освоения дисциплины «Защита информации от утечки по техническим каналам» используются следующие образовательные технологии:
• творческие задания;
• работа в малых группах;
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• изучение и закрепление нового материала на интерактивной лекции (лекция-беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций, лекция с заранее запланированными ошибками, лекция- пресс-конференция, мини-лекция);