

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 ОТ РАЗРУШАЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ**»

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	4; 8

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	36	1
Контроль самостоятельной работы	18	0,5
Самостоятельная работа	36	1
Форма аттестации: Зачет (8 сем)		
Всего	108	3

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

Г.И. Салыхиева

Доцент

В.А. Богомолов

СОГЛАСОВАНО

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

Заведующий кафедрой *Согласовано* В.А. Богомолов

УТВЕРЖДЕНО

Начальник центра УМЦ

Утверждаю

Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита от разрушающих программных воздействий» являются:

освоение студентами основных принципов и методов, применяемых при защите компьютерных систем, получение теоретических знаний о функционировании механизмов защиты информации и практических навыков администрирования этих механизмов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита от разрушающих программных воздействий» 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 «Защита от разрушающих программных воздействий» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Безопасность корпоративных информационных систем
2. Безопасность систем баз данных
3. Защита интеллектуальной собственности
4. Защита информационных процессов в компьютерных системах
5. Методы и средства криптографической защиты информации
6. Теоретические основы компьютерной безопасности

Дисциплина «Защита от разрушающих программных воздействий» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Защита операционных систем
2. Комплексная система защиты информации на предприятии

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ПК -1 Способен проводить администрирование подсистем защиты информации в операционных системах, конфигурирование программно-аппаратных средств защиты информации в операционных системах

ПК -1.1. Знает архитектуру и принципы построения операционных систем, виды политик управления доступом и информационными потоками применительно к операционным системам, архитектуру подсистем защиты информации в операционных системах, состав типовых конфигураций программно-аппаратных средств защиты информации

ПК -1.2. Умеет формулировать и настраивать политики безопасности операционных систем, оценивать и противодействовать угрозам безопасности информации операционных систем в том числе и с использованием программно-аппаратных средств защиты

ПК -1.3. Владеет навыками настройки и обновления подсистем защиты информации операционных систем

В результате освоения дисциплины обучающийся должен

Знать:

- принципы работы и структуру современных защищённых операционных систем;
- организацию основных подсистем, реализуемых в рамках операционных систем;
- основные механизмы защиты информации, реализуемые в операционных системах.

Уметь:

- создавать скрипты с использованием командных интерпретаторов Shell и Windows Power Shell
- оптимизировать работу ОС семейств Windows и Linux;
- устанавливать дополнительное программное обеспечение;

- работать с отчуждаемыми носителями информации средствами операционных систем;
- настраивать работу ОС в сетях передачи данных.

Владеть:

- навыками установки операционных систем семейства Windows (Windows 7, Windows 8, Windows 10, Windows Server) и конфигурирования служб;
- навыками установки операционных систем семейства Linux(на примере AltLinux, SuSe, Debian) и конфигурирования демонов;
- навыками настройки и оптимизации работы ОС, достаточными для комфортной работы ОС на аппаратном обеспечении, соответствующем минимальным системным требованиям.

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 3 зачетные единицы, 108 часов.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежуточной аттестации
			Лекция	Практические занятия	Лабораторные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Основные понятия ОС	8	4		8	4	8	Лабораторная работа; Реферат
2.	Подсистемы ОС	8	6		18	8	20	
3.	Особенности реализации механизмов защиты ОС	8	8		10	6	8	
	Итого по семестру	8	18		36	18	36	Зачет

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Основные понятия ОС	2	Введение в операционные системы	ПК -1.1 ПК -1.2 ПК -1.3
2.		2	Основные понятия, используемые в операционных системах	ПК -1.1 ПК -1.2 ПК -1.3
3.	Подсистемы ОС	2	Управление задачами. Процессы и потоки	ПК -1.1 ПК -1.2 ПК -1.3
4.		2	Управление памятью	ПК -1.1 ПК -1.2 ПК -1.3
5.		2	Управление данными	ПК -1.1 ПК -1.2 ПК -1.3
6.	Особенности реализации механизмов защиты ОС	2	Конфигурирование сетевой подсистемы	ПК -1.1 ПК -1.2 ПК -1.3
7.		2	Особенности ОС семейства Linux.	ПК -1.1 ПК -1.2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
				ПК -1.3
8.		2	Особенности ОС семейства Windows	ПК -1.1 ПК -1.2 ПК -1.3
9.		2	Особенности популярных мобильных ОС	ПК -1.1 ПК -1.2 ПК -1.3
	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.	Основные понятия ОС	4	Установка и настройка ОС	ПК -1.1 ПК -1.2 ПК -1.3
2.		4	Конфигурирование ОС	ПК -1.1 ПК -1.2 ПК -1.3
3.	Подсистемы ОС	6	Изучение интерфейсов командной строки в ОС	ПК -1.1 ПК -1.2 ПК -1.3
4.		6	Конфигурирование сетевой подсистемы с использованием средств защиты информации	ПК -1.1 ПК -1.2 ПК -1.3
5.		6	Методы оптимизации и повышения производительности ОС семейства Linux	ПК -1.1 ПК -1.2 ПК -1.3
6.	Особенности реализации механизмов защиты ОС	5	Методы оптимизации и повышения производительности ОС Windows	ПК -1.1 ПК -1.2 ПК -1.3
7.		5	Обзор механизмов защиты информации ОС Android и ОС IOS	ПК -1.1 ПК -1.2 ПК -1.3
	ВСЕГО	36		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Введение в операционные системы	4	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
2.	Основные понятия, используемые в операционных системах	4	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
3.	Управление задачами. Процессы и потоки.	5	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
4.	Управление памятью	5	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
				ПК -1.3
5.	Управление данными	5	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
6.	Конфигурирование сетевой подсистемы	5	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
7.	Особенности ОС семейства Linux	3	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
8.	Особенности популярных мобильных ОС	2	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
9.	Особенности популярных мобильных ОС	3	написание реферата, подготовка к лабораторной работе	ПК -1.1 ПК -1.2 ПК -1.3
	ВСЕГО	36		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Введение в операционные системы	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
2.	Основные понятия, используемые в операционных системах	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
3.	Управление задачами. Процессы и потоки.	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
4.	Управление памятью	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
5.	Управление данными	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
6.	Конфигурирование сетевой подсистемы	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
7.	Особенности ОС семейства Linux	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
8.	Особенности ОС семейства Windows	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
9.	Особенности популярных мобильных ОС	2	прием лабораторной работы, проверка реферата	ПК -1.1 ПК -1.2 ПК -1.3
	ВСЕГО	18		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Защита от разрушающих программных воздействий» 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			
Реферат	1	11	16
Лабораторная работа	7	49	84
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 от разрушающих программных воздействий» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
В.П. Мельников, С.А. Клейменов, А.М. Петраков, Информационная безопасность и защита информации [Учебник] учеб. пособие для студ. вузов, обуч. по спец. 230201 "Информационные системы и технологии": М. : Академия, 2006	50 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Е.К. Баранова, А.В. Бабаш, Информационная безопасность и защита информации [Прочее] Учебное пособие: Москва : Издательский Центр РИОР, 2020	http://znaniyum.com/go.php?id=1114032 Режим доступа: по подписке КНИТУ
А. А. Бирюков, Информационная безопасность: защита и нападение [Электронный ресурс] : Москва : ДМК Пресс, 2017	https://e.lanbook.com/book/93278 Режим доступа: по подписке КНИТУ
Э. Таненбаум, Компьютерные сети [Прочее] : М. [и др.] : Питер, 2005	26 экз. УНИЦ ФГБОУ ВО «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 Режим доступа: по подписке КНИТУ
В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе, Защита информации [Учебник] учебник для подгот. бакалавров по напр. 230100 "Информатика и вычислит. техника": М. : Академия, 2014	10 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Э. Таненбаум, Современные операционные системы [Прочее] : М. [и др.] : Питер, 2006	9 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Н. В. Тюльпинова,, Защита интеллектуальной собственности и компьютерной информации [Прочее] учебное пособие для магистров: Саратов : Вузовское образование, 2020	http://www.iprbookshop.ru/88755.html 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 Режим доступа: по подписке КНИТУ
К. А. Коньков,, Основы операционных систем. Устройство и функционирование ОС Windows [Прочее] учебное пособие: Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/97565.html Режим доступа: по подписке КНИТУ
В. О. Сафонов, Основы современных операционных систем [Электронный ресурс] : Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/62818.html Режим доступа: по подписке КНИТУ
В. Ю. Суходольский, Ю. М. Шапаренко, П. П. Бескид, Проектирование защищенных информационных систем. Часть 1. Конструкторское проектирование. Защита от физических полей [Электронный ресурс] Учебное пособие: Санкт-Петербург : Российский государственный гидрометеорологический университет, 2008	http://www.iprbookshop.ru/17960.html Режим доступа: по подписке КНИТУ
В. Карпов, К. Коньков, Основы операционных систем [Прочее] практикум: Москва : Национальный Открытый Университет «ИНТУИТ», 2016	http://biblioclub.ru/index.php?page=book&id=429022 Режим доступа: по подписке КНИТУ
В.В. Лисяк, Разработка информационных систем [Прочее] Учебное пособие: Ростов-на-Дону : Издательство Южного федерального университета (ЮФУ), 2019	http://znanium.com/go.php?id=1088133 Режим доступа: по подписке КНИТУ
А. С. Широков, Ю. П. Качановский, Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс] Методические указания к проведению лабораторной работы по курсу «Информатика»: Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2014	http://www.iprbookshop.ru/55120.html Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Защита от разрушающих программных воздействий» 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/>

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 «Защита от разрушающих программных воздействий»:

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

- MS Office 2010-2016 Standard от 08.11.2016 No 16/2189/Б

- notepad++ <https://notepad-plus-plus.org/resources/>

фисные и деловые программы: ABBYY FineReader 9.0 проф от 19.11.2008 № AF90-3S1V01-102;

Офисные и деловые программы: MS Office 2007 Russian от 16.10.2008 лицензия № 44684779;

ПО для коллективной работы Microsoft Teams

Научное ПО: Mathcad Education

Научное ПО: Mathematica Standard

Научное ПО: Scilab

ПО имеющее лимит по сроку использования (закупленное ВУЗом)

Научное ПО: STATISTICA Academic До августа 2021 Научное ПО: Hyperworks До декабря 2020 V05-102;

Учебные аудитории для проведения учебных занятий оснащены презентационной техникой (проектор, экран, компьютер) и техническими средствами обучения: компьютер с доступом в Интернет, доска интерактивная Webster TS 810, М-проектор BENQ MX880UST, М-проектор Optoma EX7155e

Помещения для самостоятельной работы оснащены компьютерной техникой: ПК: Intel Core2 Duo2.6Gz/3M/клавиатура, монитор LCD19``, мышь; ПК: Intel Core2 Duo2.6Gz/3Md, монитор LCD19``. ТМГ, сет. фильтр.

с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ. Допускается замена оборудования его виртуальными аналогами.

1. Д229 - компьютерный класс
2. Д507 а - компьютерный класс
- 3 . доска настенная
4. стол преподавателя
5. стулья и парты ученические

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Защита от разрушающих программных воздействий» составляет 18 ч.

В процессе освоения дисциплины «Защита от разрушающих программных воздействий» используются следующие образовательные технологии:

1. работа в малых группах;
2. использование элементов системы дистанционного обучения (система дистанционного обучения Moodle).