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 ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»**

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; 7

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	45	1,25
Контроль самостоятельной работы	81	2,25
Самостоятельная работа	81	2,25
Форма аттестации: Зачет (7 сем), Экзамен (7 сем)	27	0,75
Всего	252	7

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:

Доцент	К.В. Иванов
Старший преподаватель	Г.И. Саляхиева

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 «Защита информационных процессов в компьютерных системах» являются:

а) ознакомление с основными понятиями, используемыми при защите информации в компьютерных системах;

б) представление об основных проблемах защиты информации в компьютерных системах;

в) обучение студентов методам защиты информации в компьютерных системах для построения защищенных информационных технологий;

г) получение навыков практической работы по использованию средств защиты информационных процессов в компьютерных системах.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информационных процессов в компьютерных системах» 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 информационных процессов в компьютерных системах» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Безопасность корпоративных информационных систем
2. Инженерно-техническая защита информации

Дисциплина «Защита информационных процессов в компьютерных системах» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Защита операционных систем
2. Защита от разрушающих программных воздействий
3. Комплексная система защиты информации на предприятии
4. Основы проектной деятельности
5. Основы управления информационной безопасностью

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:

- технологию построения защищенных компьютерных систем.
- методы оценок защищенности компьютерных систем.
- основные положения РД ФСТЭК России (Гостехкомиссии).
- основные положения TCSEC, ITSEC.
- основные подходы к оценке защищенности в "общих критериях оценки защищенности информационных технологий".

Уметь:

- оценивать защищенность компьютерных систем.
- анализировать риски в компьютерных системах.

Владеть:

- навыками установки и настройки средств компьютерной безопасности; навыками применения программных средств компьютерной безопасности; навыками реализации решений типовых задач обеспечения компьютерной безопасности.

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 7 зачетных единиц, 252 часа.

№ 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.	Информационные технологии и их поддержка	7	4		10	22	27	Лабораторная работа; Реферат; Экзамен
2.	Технология защиты информации	7	6		15	18	18	
3.	Американские и европейские стандарты по защите информации	7	4		10	18	18	
4.	Общие критерии оценки защищенности информационных технологий - Common Criteria (CC)	7	4		10	23	18	
	Итого по семестру	**7**	**18**		**45**	**81**	**81**	**Зачет, Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Информационные технологии и их поддержка	2	Информационные технологии и информационные системы	ПК -2.1 ПК -2.2 ПК -2.3

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
2.		2	Проектирование и разработка информационных технологий	ПК -2.1 ПК -2.2 ПК -2.3
3.	Технология защиты информации	2	Основные угрозы информации в компьютерных системах	ПК -2.1 ПК -2.2 ПК -2.3
4.		2	Политика безопасности для компьютерных систем	ПК -2.1 ПК -2.2 ПК -2.3
5.		2	Государственная политика в области безопасности компьютерных систем	ПК -2.1 ПК -2.2 ПК -2.3
6.	Американские и европейские стандарты по защите информации	2	"Оранжевая книга"	ПК -2.1 ПК -2.2 ПК -2.3
7.		2	ITSEC	ПК -2.1 ПК -2.2 ПК -2.3
8.	Общие критерии оценки защищенности информационных технологий - Common Criteria (CC)	2	Подход к безопасности компьютерных систем в CC и базовые концепции. Классы в CC	ПК -2.1 ПК -2.2 ПК -2.3
9.		2	Каналы утечки и их анализ по CC. Безопасное функционирование по CC	ПК -2.1 ПК -2.2 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.	Информационные технологии и их поддержка	5	Поиск в Интернет сайтов и материалов, связанных с обеспечением безопасности в компьютерных системах.	ПК -2.1 ПК -2.2 ПК -2.3
2.		5	Стандарты и методология создания и эксплуатации ИС	ПК -2.1 ПК -2.2 ПК -2.3
3.	Технология защиты информации	5	Сравнение функций безопасности одной из операционных систем с требованиями РД Гостехкомиссии	ПК -2.1 ПК -2.2 ПК -2.3
4.		5	Определение основных угроз информационной безопасности в компьютерных системах	ПК -2.1 ПК -2.2 ПК -2.3
5.		5	Количественная оценка стойкости парольной защиты.	ПК -2.1 ПК -2.2 ПК -2.3
6.	Американские и европейские стандарты по защите информации	5	Поиск в Интернет сайтов и материалов, связанных с обеспечением безопасности в компьютерных системах	ПК -2.1 ПК -2.2 ПК -2.3
7.		5	Обеспечение информационной безопасности в ведущих зарубежных странах	ПК -2.1 ПК -2.2 ПК -2.3
8.	Общие критерии оценки защищенности информационных технологий - Common	5	Классификация защищенности компьютерной системы по требованиям	ПК -2.1 ПК -2.2

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
	Criteria (CC)		безопасности информации в системе общих критериев	ПК -2.3
9.		5	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**45**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Информационные технологии и информационные системы	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
2.	Проектирование и разработка информационных технологий	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
3.	Основные угрозы информации в компьютерных системах	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
4.	Политика безопасности для компьютерных систем	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
5.	Государственная политика в области безопасности компьютерных систем	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
6.	"Оранжевая книга"	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
7.	ITSEC	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
8.	Подход к безопасности компьютерных систем в CC и базовые концепции. Классы в CC	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
9.	9 Каналы утечки и их анализ по CC. Безопасное функционирование по CC	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3
	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.	Информационные технологии и информационные системы	7	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
2.	Проектирование и разработка информационных технологий	7	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
3.	Основные угрозы информации в компьютерных системах	8	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
4.	Политика безопасности для компьютерных систем	9	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
				ПК -2.3
5.	Государственная политика в области безопасности компьютерных систем	9	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
6.	"Оранжевая книга"	9	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
7.	ITSEC	9	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
8.	Подход к безопасности компьютерных систем в СС и базовые концепции. Классы в СС	9	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
9.	Каналы утечки и их анализ по СС. Безопасное функционирование по СС	14	прием лабораторной работы, прием экзамена, проверка реферата	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**81**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Защита информационных процессов в компьютерных системах» 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
7-й семестр			
Лабораторная работа	9	27	45
Реферат	1	9	15
Экзамен	1	24	40
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 информационных процессов в компьютерных системах» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
В. И. Аверченков, Аудит информационной безопасности [Электронный ресурс] Учебное пособие для вузов: Брянск : Брянский государственный технический университет, 2012	http://www.iprbookshop.ru/6991.html Режим доступа: по подписке КНИТУ
А. А. Бирюков, Информационная безопасность: защита и нападение	https://e.lanbook.com/book/93278 Режим доступа: по подписке КНИТУ

[Электронный ресурс] : Москва : ДМК Пресс, 2017	
В. Ф. Шаньгин, Информационная безопасность [Электронный ресурс] : Москва : ДМК Пресс, 2014	http://e.lanbook.com/books/element.php?pl1_id=50578 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 Режим доступа: по подписке КНИТУ
А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников, Информационная безопасность [Лабораторные работы] лабор. практикум : учеб. пособие: М. : Кнорус, 2013	1 экз. УНИЦ ФГБОУ ВО «КНИТУ»
А. В. Кувыклин, М. В. Рудановский, М. Ю. Рытов [и др.], Аудит информационной безопасности органов исполнительной власти [Электронный ресурс] Учебное пособие: Брянск : Брянский государственный технический университет, 2012	http://www.iprbookshop.ru/6992.html Режим доступа: по подписке КНИТУ
В. В. Лисяк, Разработка информационных систем [Прочее] учебное пособие: Ростов-на-Дону|Таганрог : Южный федеральный университет, 2019	http://biblioclub.ru/index.php?page=book&id=577875 Режим доступа: по подписке КНИТУ
А. В. Артемов, Информационная безопасность [Прочее] курс лекций: Орел : МАБИВ, 2014	http://biblioclub.ru/index.php?page=book&id=428605 Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Защита информационных процессов в компьютерных системах» 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 «Защита информационных процессов в компьютерных системах»:

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

В качестве материально-технического обеспечения дисциплины могут быть использованы мультимедийные средства; презентации или кинофильмов; демонстрационные приборы.

При изучении дисциплины используются следующие учебно-методические материалы для обеспечения самостоятельной работы:
1. Лекции проводятся в мультимедийной аудитории, материал лекций предоставляется обучающимся в форме презентаций.
2. Для самостоятельной работы студентам выдаётся курс лекций по дисциплине, задания на подготовку к практическим занятиям.
3. По завершении изучения темы выдаются пробные тестовые задания для самостоятельной проверки уровня знаний студента.
4.Содержание лекций, задания на практические занятия, контрольные тесты выложены на сайте образовательной среды ФГБОУ ВО КНИТУ «MOODLE»
5. Для подготовки к зачёту обучающимся предоставляется перечень вопросов для подготовки.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Защита информационных процессов в компьютерных системах» составляет 27 ч.

В процессе освоения дисциплины «Защита информационных процессов в компьютерных системах» используются следующие образовательные технологии:
1. работа в малых группах;
2. использование элементов системы дистанционного обучения (система дистанционного обучения Moodle).