

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 «КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ»

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
Практическое занятие	36	1
Контроль самостоятельной работы	18	0,5
Самостоятельная работа	45	1,25
Форма аттестации: Экзамен (8 сем)	27	0,75
Всего	144	4

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

СОГЛАСОВАНО

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

УТВЕРЖДЕНО

Начальник центра УМЦ

Утверждаю

Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Комплексная система защиты информации» являются:

- а) формирование компетентности в области инженерных подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности предприятия и его информационной инфраструктуры;
- б) развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- в) привитие стремления к поиску оптимальных, простых и надежных решений;
- г) выработка навыков разработки систем защиты информации предприятия на основе оценки угроз безопасности информации, способов моделирования, технологии организации, кадрового, технологического и нормативно-методического обеспечения, методах оценки эффективности СЗИ;
- д) расширение кругозора.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Комплексная система защиты информации» относится к формируемой участниками образовательных отношений 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 «Комплексная система защиты информации» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Защита информационных процессов в телекоммуникациях
2. Методы и средства криптографической защиты информации
3. Программно-аппаратные средства защиты информации

Дисциплина «Комплексная система защиты информации» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Аудит информационной безопасности объектов инфокоммуникаций
2. Проектирование защищенных телекоммуникационных систем
3. Производственная практика (технологическая практика)

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ПК-2 Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности

ПК-2.1. Знает критерии безопасности обработки информации в телекоммуникационных системах

ПК-2.2. Умеет выполнять мероприятия для реализации политики информационной безопасности

ПК-2.3. Владеет навыками определения состава и порядка настройки технических средств для управления телекоммуникационными системами и средствами их защиты от НСД

ПК-3 Способен выполнять работы по обеспечению информационной безопасности телекоммуникационных систем на всех этапах их жизненного цикла

ПК-3.1. Знает план мероприятий по внедрению решений и средств для обеспечения информационной безопасности в соответствии с требованиями реализуемой политики безопасности

ПК-3.2. Умеет восстанавливать работоспособность телекоммуникационных систем после инцидентов информационной безопасности

ПК-3.3. Владеет навыками проведения операции вывода защищённых телекоммуникационных систем из эксплуатации

В результате освоения дисциплины обучающийся должен

Знать:

- первичные исходные данные для проектирования подсистем и средств обеспечения

информационной безопасности;

-теоретические аспекты комплексной системы защиты информации;

Уметь:

-использовать соответствующие методы обеспечения информационной безопасности выбранных объектов;

-классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

Владеть:

-навыками работы с методами и моделями оценки эффективности КСЗИ;

-навыками разработки документации для решения задач информационной безопасности;

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ 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.	Теоретические основы построения комплексной системы построения системы защиты информации	8	5	16		2	5	Практические занятия; Реферат; Экзамен
2.	Первые шаги перед построением комплексной системы защиты на предприятии	8	3	12		4	10	
3.	Проектирование и внедрение комплексной системы защиты информации	8	10	8		12	30	
Итого по семестру		8	18	36		18	45	Экзамен

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Теоретические основы построения комплексной системы построения системы защиты информации	3	Основные термины и определения. Сущность и задачи комплексной системы защиты информации	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.		2	Организационно-правовые аспекты защиты информации в	ПК-2.1 ПК-2.2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
			АС	ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Первые шаги перед построением комплексной системы защиты на предприятии	1	Прием и увольнение персонала с позиции безопасности	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.		1	Аудит защищённой АС	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
5.		1	Определение и нормативное закрепление состава защищаемой информации	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
6.	Проектирование и внедрение комплексной системы защиты информации	2	Проектирование и развёртывание защищённых корпоративных систем	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
7.		2	Моделирование угроз системе и действий нарушителя	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
8.		1	Основные компоненты комплексной системы обеспечения информационной безопасности в организации	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
9.		1	Создание политики безопасности организации	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
10.		2	Оценка соответствия системы защиты информации	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
11.		2	Особенности построения систем защиты информации различного уровня конфиденциальности	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	18		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Теоретические основы построения комплексной системы построения системы защиты информации	6	Изучение требований к классам защищённости автоматизированных систем	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.		6	Изучение требований к классам защищённости информационных систем, обрабатывающих персональные данные.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.		4	Изучение требований к классам защищённости государственных информационных систем.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.	Первые шаги перед построением комплексной системы защиты на предприятии	4	Подготовка резюме на позицию специалиста по информационной безопасности	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
5.		4	Инвентаризация и категорирование информационных ресурсов.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
6.		4	Анализ защищённости системы. Форензика	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
7.	Проектирование и внедрение комплексной системы защиты информации	4	Разработка спецификации средств защиты информации	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
8.		4	Подготовка заявки на получение лицензий	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	36		

7. Содержание лабораторных занятий

Проведение лабораторных занятий не предусмотрено учебным планом

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Основные термины и определения. Сущность и задачи комплексной системы защиты информации	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
				ПК-3.1 ПК-3.2 ПК-3.3
2.	Аудит защищённой АС	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Определение и нормативное закрепление состава защищаемой информации	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.	Проектирование и развёртывание защищённых корпоративных систем	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
5.	Моделирование угроз системе и действий нарушителя	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
6.	Основные компоненты комплексной системы обеспечения информационной безопасности в организации	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
7.	Создание политики безопасности организации	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
8.	Оценка соответствия системы защиты информации	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
9.	Особенности построения систем защиты информации различного уровня конфиденциальности	5	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	45		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Основные термины и определения. Сущность и задачи комплексной системы защиты информации	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
				ПК-3.3
2.	Аудит защищённой АС	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Определение и нормативное закрепление состава защищаемой информации	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.	Проектирование и развёртывание защищённых корпоративных систем	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
5.	Моделирование угроз системе и действий нарушителя	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
6.	Основные компоненты комплексной системы обеспечения информационной безопасности в организации	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
7.	Создание политики безопасности организации	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
8.	Оценка соответствия системы защиты информации	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
9.	Особенности построения систем защиты информации различного уровня конфиденциальности	2	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	18		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Комплексная система защиты информации» 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			
Практические занятия	8	32	48
Реферат	1	4	12
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 «Комплексная система защиты информации» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
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 Режим доступа: по подписке КНИТУ
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»
А. А. Петренко, С. А. Петренко, Аудит безопасности Intranet [Электронный ресурс] : Москва : ДМК Пресс, 2010	https://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1113 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

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, С.А. Клейменов, А.М. Петраков, Информационная безопасность и защита информации [Учебник] учеб. пособие для студ. вузов, обуч. по спец. 230201 "Информацион. системы и технологии": М. : Академия, 2008	10 экз. УНИЦ ФГБОУ ВО «КНИТУ»
В. И. Аверченков, Аудит информационной	http://www.iprbookshop.ru/6991.html

безопасности [Электронный ресурс] Учебное пособие для вузов: Брянск : Брянский государственный технический университет, 2012	Режим доступа: по подписке КНИТУ
А.Ф. Кемалов, Р.А. Кемалов, Т.Ф. Ганиева, Теоретические и прикладные основы разработки поточной схемы и расчета товарного баланса нефтеперерабатывающего завода [Учебник] учеб. пособие: Казань : , 2010	28 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Т.Ф. Ганиева, Р.А. Кемалов, А.Ф. Кемалов, Теоретические и прикладные основы разработки поточной схемы и расчета товарного баланса нефтеперерабатывающего завода [Электронный ресурс] учеб. пособие: Казань : , 2010	http://ft.kstu.ru/ft/978-5-7882-1015-5-Kemalov_Kemalov_Ganieva-TIPORPSIRTBNZ.pdf Доступ с IP адресов 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
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»
С. Н. Никифоров, Защита информации [Электронный ресурс] Учебное пособие: Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015	http://www.iprbookshop.ru/74365.html Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Комплексная система защиты информации» 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 «Комплексная система защиты информации»:

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

Офисные и деловые программы: 1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях

Офисные и деловые программы: Константа: Управление процессами.

Дополнительное ПО доступное по бесплатной подписке от Microsoft

Офисные и деловые программы: Microsoft Office 365 Версия для студентов
Офисные и деловые программы: Microsoft Office 365 Версия для преподавателей
ПО для коллективной работы Microsoft Teams

Moodle 3.10

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:

1. Ноутбук на базе процессора AMD Dual-Core E-350
2. Проектор мультимедийный EB-W10, экран для проектора.
3. Экран проекционный настенный.

Помещения для самостоятельной работы оснащены компьютерной техникой:

компьютер преподавателя

11 компьютеров студента тип AMD A4-6300

кондиционер SystemAir Sysplit Wall Smart

Проектор Acer H5360BD с доской интерактивной, экран

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

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Комплексная система защиты информации» составляет 9 ч.

В процессе освоения дисциплины «Комплексная система защиты информации» 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);

