

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 «ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ СЛУЖБОЙ 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	3; 6

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Практическое занятие	18	0,5
Контроль самостоятельной работы	18	0,5
Самостоятельная работа	54	1,5
Форма аттестации: Зачет (6 сем)		
Всего	108	3

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.Ю. Сенцова

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 «Организация и управление службой защиты информации» являются:

-получение знаний в следующих областях: организация и задачи службы информационной безопасности, организационно-технические мероприятия по защите информации, порядок организации работ по защите информации в ведомствах и на предприятиях (порядок проведения охраны предприятия, организация пропускного режима, проведение разработки системы защиты информации, порядок проведения аттестации и лицензирование объекта информатизации др. организационные меры информационной защиты).

2. Место дисциплины в структуре образовательной программы

Дисциплина «Организация и управление службой 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 «Организация и управление службой защиты информации» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Введение в специальность
2. Основы информационной безопасности
3. Самоорганизация и командная работа
4. Теория информации

Дисциплина «Организация и управление службой защиты информации» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Аудит информационной безопасности объектов инфокоммуникаций
2. Основы управления информационной безопасностью
3. Производственная практика (технологическая практика)
4. Работа с конфиденциальной информацией

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ПК-4 Способен организовывать работы по обеспечению информационной безопасности в телекоммуникационных системах

ПК-4.1. Знает правила работы персонала со средствами защиты информации

ПК-4.2. Умеет распределять обязанности и полномочия персонала, обслуживающего защищённую телекоммуникационную систему

ПК-4.3. Владеет навыками сопоставления результатов работы персонала, обслуживающего защищённую телекоммуникационную систему, с целевыми показателями функционирования службы защиты информации

В результате освоения дисциплины обучающийся должен

Знать:

-политику и стратегию информационной безопасности, технологию и способы организации защиты информации и их оптимизацию; понятия и принципы управления; принципы документирования и документооборота; виды документов, требования к их оформлению; правовые и организационные основы документационного обеспечения управленческой и информационно-аналитической деятельности (при решении задач организации службы защиты информации)

Уметь:

-применять на практике принципы политики безопасности; использовать методы количественного представления информации при выполнении комплекса мер по информационной безопасности; применять нормы информационного права, нормативные правовые и методические документы в области защиты информации и обеспечения информационной безопасности.

Владеть:

-навыками анализа, обработки и интерпретации результатов решения задач управления, формирования комплекса мер (правил, процедур, приемов и пр.) для управления информационной безопасностью; навыками организации мероприятий по защите информации в процессах автоматизированной обработки информации; навыками работы с документами ограниченного доступа и обеспечения их защиты.

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 организационные меры по защите информации	6	8	10		10	30	Коллоквиум; Практические занятия
2.	Организация и управление службой безопасности	6	10	8		8	24	
Итого по семестру		6	18	18		18	54	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 организационные меры по защите информации	2	Понятие концепции информационной безопасности.	ПК-4.1 ПК-4.2 ПК-4.3
2.		2	Основные организационно-технические мероприятия по защите информации. Организация работ по защите информации на предприятии.	ПК-4.1 ПК-4.2 ПК-4.3
3.		4	Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.	ПК-4.1 ПК-4.2 ПК-4.3
4.	Организация и управление службой безопасности	2	Организация службы безопасности.	ПК-4.1 ПК-4.2 ПК-4.3
5.		2	Организационно-технические и режимные меры. Организация	ПК-4.1 ПК-4.2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
			доступа и допуска (предоставление, основание отказа, формы допуска).	ПК-4.3
6.		2	Аттестация объектов информатизации. Система лицензирования.	ПК-4.1 ПК-4.2 ПК-4.3
7.		2	Порядок организации и проведения разработок системы защиты информации в ведомствах и на отдельных предприятиях.	ПК-4.1 ПК-4.2 ПК-4.3
8.		2	Организация охраны предприятия. Организация внутриобъектового и пропускного режимов на предприятиях.	ПК-4.1 ПК-4.2 ПК-4.3
	ВСЕГО	18		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Основные организационные меры по защите информации	2	Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации	ПК-4.1 ПК-4.2 ПК-4.3
2.		2	Структурная схема службы защиты информации. Факторы, влияющие на задачи и функции службы защиты информации. Должностной состав сотрудников службы защиты информации	ПК-4.1 ПК-4.2 ПК-4.3
3.		2	Структура и содержание положения о службе защиты информации. Задачи, функции, права и ответственность сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации	ПК-4.1 ПК-4.2 ПК-4.3
4.		2	Организационные задачи службы защиты информации	ПК-4.1 ПК-4.2 ПК-4.3
5.		2	Обеспечение информационной безопасности предприятия службой защиты информации	ПК-4.1 ПК-4.2 ПК-4.3
6.	Организация и управление службой безопасности	2	Состав и содержание управленческих функций. Принципы управления службой защиты информации. Системы методов управления	ПК-4.1 ПК-4.2 ПК-4.3
7.		2	Организация и технология планирования	ПК-4.1 ПК-4.2 ПК-4.3
8.		2	Методы оценки эффективности и качества службы защиты информации	ПК-4.1 ПК-4.2 ПК-4.3
9.		2	Обеспечение персональной ответственности за сохранность носителей информации	ПК-4.1 ПК-4.2 ПК-4.3

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
	ВСЕГО	18		

7. Содержание лабораторных занятий

Проведение лабораторных занятий не предусмотрено учебным планом

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
2.	Структурная схема службы защиты информации. Факторы, влияющие на задачи и функции службы защиты информации. Должностной состав сотрудников службы защиты информации	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
3.	Структура и содержание положения о службе защиты информации. Задачи, функции, права и ответственность сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
4.	Организационные задачи службы защиты информации	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
5.	Обеспечение информационной безопасности предприятия службой защиты информации	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
6.	Состав и содержание управленческих функций. Принципы управления службой защиты информации. Системы методов управления	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
7.	Организация и технология планирования	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
8.	Методы оценки эффективности и качества службы защиты информации	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
9.	Обеспечение персональной ответственности за сохранность носителей информации	6	подготовка к коллоквиуму, подготовка к практическому занятию	ПК-4.1 ПК-4.2 ПК-4.3
	ВСЕГО	54		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
2.	Структурная схема службы защиты информации. Факторы, влияющие на задачи и функции службы защиты	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
	информации. Должностной состав сотрудников службы защиты информации			
3.	Структура и содержание положения о службе защиты информации. Задачи, функции, права и ответственность сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
4.	Организационные задачи службы защиты информации	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
5.	Обеспечение информационной безопасности предприятия службой защиты информации	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
6.	Состав и содержание управленческих функций. Принципы управления службой защиты информации. Системы методов управления	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
7.	Организация и технология планирования	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
8.	Методы оценки эффективности и качества службы защиты информации	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
9.	Обеспечение персональной ответственности за сохранность носителей информации	2	прием коллоквиума, проверка знаний на практическом занятии	ПК-4.1 ПК-4.2 ПК-4.3
	ВСЕГО	18		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Организация и управление службой 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
6-й семестр			
Практические занятия	9	45	72
Коллоквиум	1	15	28
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 «Организация и управление службой защиты информации» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
В. И. Аверченков, М. Ю. Рытов, Служба защиты информации. Организация и управление [Электронный ресурс] Учебное пособие для вузов: Брянск : Брянский государственный технический университет, 2012	http://www.iprbookshop.ru/7008.html Режим доступа: по подписке КНИТУ
В. А. Сердюк, Организация и технологии защиты информации [Прочее] обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: Москва : Издательский дом Высшей школы экономики, 2015	http://biblioclub.ru/index.php?page=book&id=440285 Режим доступа: по подписке КНИТУ
Прокофьев С.Е. Артюхин Р.Е. Панина О.В. Лукичев К.Е., Основы защиты информации в системе государственного и муниципального управления (с практикумом) [Прочее] Учебник: Москва : КноРус, 2022	https://book.ru/book/943134 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
, Организационные и технические методы защиты информации [Учебник] учеб. пособие для студ., обуч. по спец. 21.08.00: Пенза : , 2003	1 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Д. А. Скрипник, Общие вопросы технической защиты информации [Прочее] : Москва : Национальный Открытый Университет «ИНТУИТ», 2016	http://biblioclub.ru/index.php?page=book&id=429070 Режим доступа: по подписке КНИТУ
Н. В. Гришина, Основы информационной безопасности предприятия [Прочее] Учебное пособие: Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	http://znanium.com/catalog/document?id=379717 Режим доступа: по подписке КНИТУ
, Организационно-правовые основы информационной безопасности [Учебник] учебное пособие: Воронеж : ВИ МВД РФ, 2002	2 экз. УНИЦ ФГБОУ ВО «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

11.3. Электронные источники информации

При изучении дисциплины «Организация и управление службой 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/>

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 «Организация и управление службой 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

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
 15. Типовой комплект учебного оборудования «Глобальные компьютерные сети» ,
 16. Типовой комплект учебного оборудования «Корпоративные компьютерные сети» .
- Помещения для самостоятельной работы оснащены компьютерной техникой:
Аудитория Г-407, компьютер/ноутбук 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 «Организация и управление службой защиты информации» составляет 9 ч.

В процессе освоения дисциплины «Организация и управление службой 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).