

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 «**ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**»

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, 8

Вид нагрузки	Часы	Зачётные единицы
Лекция	36	1
Лабораторная работа	63	1,75
Контроль самостоятельной работы	63	1,75
Самостоятельная работа	63	1,75
Форма аттестации: Зачет (7 сем), Курсовая работа (8 сем), Экзамен (8 сем)	27	0,75
Всего	252	7

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

К.В. Иванов

---

### **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 «Основы управления информационной безопасностью» являются:

- а) изучение методов и средств управления информационной безопасностью (ИБ) в организации,
- б) изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

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

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части ООП и формирует у обучающихся по специализации «Технологии защиты информации в правоохранительной сфере» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Основы управления информационной безопасностью» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Безопасность корпоративных информационных систем
2. Защита и обработка конфиденциальных документов
3. Основы информационной безопасности
4. Средства и системы технического обеспечения обработки, хранения и передачи информации

Дисциплина «Основы управления информационной безопасностью» 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

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

**ОПК-5 Способен планировать проведение работ по комплексной защите информации на объекте информатизации**

ОПК-5.1. Знает принципы организации и этапы разработки комплексной системы защиты информации

ОПК-5.2. Умеет разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по комплексной системе защите информации на предприятии

ОПК-5.3. Владеет технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии

**В результате освоения дисциплины обучающийся должен**

**Знать:**

- современные подходы к управлению ИБ и направлениях их развития;
- основные стандарты, регламентирующие управление ИБ;
- принципы построения СУИБ;
- принципы разработки процессов управления ИБ;
- взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;
- подходы к интеграции СУИБ в общую систему управления предприятием;

**Уметь:**

- анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ;

- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;
- используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления ИБ;
- разрабатывать и внедрять СУИБ и оценивать ее эффективность.

**Владеть:**

- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;
- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
- методами управления информационной безопасностью автоматизированных систем;
- методами оценки информационных рисков;
- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
- навыками участия в экспертизе состояния защищенности информации на объекте защиты.

**4. Структура и содержание дисциплины**

Общая трудоёмкость дисциплины составляет 7 зачетных единиц, 252 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.	Общая модель управления (менеджмента) информационной безопасностью	7	14		18	10	10	Лабораторная работа; Реферат
2.	Планирование системы управления (менеджмента) ИБ	7	4		18	17	17	
	<b>Итого по семестру</b>	<b>7</b>	<b>18</b>		<b>36</b>	<b>27</b>	<b>27</b>	<b>Зачет</b>
1.	Реализация системы управления (менеджмента) ИБ	8	3		16	7	6	Лабораторная работа; Экзамен
2.	Проверка и совершенствование системы управления (менеджмента) ИБ	8	2		3	2	5	
3.	Обеспечение	8	13		8	9	7	

№ 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
	доверия к информационной безопасности информационных систем							
4.	Курсовая работа	8				18	18	Курсовая работа
	<b>Итого по семестру</b>	<b>8</b>	<b>18</b>		<b>27</b>	<b>36</b>	<b>36</b>	<b>Курсовая работа, Экзамен</b>

### 5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Общая модель управления (менеджмента) информационной безопасностью	5	Базовые вопросы управления	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.		2	Процессный подход	ОПК-5.1 ОПК-5.2 ОПК-5.3
3.		7	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности	ОПК-5.1 ОПК-5.2 ОПК-5.3
4.	Планирование системы управления (менеджмента) ИБ	3	Разработка системы управления информационной безопасности (СУИБ) предприятия на основе процессного подхода	ОПК-5.1 ОПК-5.2 ОПК-5.3
5.		1	Стандартизация в области управления ИБ	ОПК-5.1 ОПК-5.2 ОПК-5.3
6.	Реализация системы управления (менеджмента) ИБ	2	Ролевая структура СУИБ	ОПК-5.1 ОПК-5.2 ОПК-5.3
7.		1	Определение политики СУИБ. Правила разработки политик информационной безопасности (ИБ)	ОПК-5.1 ОПК-5.2 ОПК-5.3
8.	Проверка и совершенствование системы управления (менеджмента) ИБ	2	Внедрение мер (контрольных процедур) по обеспечению ИБ.	ОПК-5.1 ОПК-5.2 ОПК-5.3
9.	Обеспечение доверия к информационной безопасности информационных систем	6	Процесс «Обеспечение непрерывности ведения бизнеса»	ОПК-5.1 ОПК-5.2 ОПК-5.3
10.		7	Эксплуатация и независимый аудит СУИБ	ОПК-5.1 ОПК-5.2 ОПК-5.3
	<b>ВСЕГО</b>	<b>36</b>		

### 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.	Общая модель управления (менеджмента) информационной безопасностью	9	Построение функциональной и организационной структуры предприятия	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.		9	Построение формальных моделей процессов создания и СУИБ	ОПК-5.1 ОПК-5.2 ОПК-5.3
3.	Планирование системы управления (менеджмента) ИБ	6	Построение формальных моделей улучшения процессов СУИБ	ОПК-5.1 ОПК-5.2 ОПК-5.3
4.		6	Обзор и анализ существующих стандартов по управлению ИБ	ОПК-5.1 ОПК-5.2 ОПК-5.3
5.		6	Разработка политики и концепции информационной безопасности	ОПК-5.1 ОПК-5.2 ОПК-5.3
6.	Реализация системы управления (менеджмента) ИБ	4	Разработка политики и концепции информационной безопасности	ОПК-5.1 ОПК-5.2 ОПК-5.3
7.		4	Создание подразделения информационной безопасности.	ОПК-5.1 ОПК-5.2 ОПК-5.3
8.		4	Работа подразделения ИБ при управлении ИБ предприятия	ОПК-5.1 ОПК-5.2 ОПК-5.3
9.		4	Создание подразделения информационной безопасности.	ОПК-5.1 ОПК-5.2 ОПК-5.3
10.	Проверка и совершенствование системы управления (менеджмента) ИБ	3	Расследование инцидента в области защиты информации	ОПК-5.1 ОПК-5.2 ОПК-5.3
11.	Обеспечение доверия к информационной безопасности информационных систем	4	Обзор программных продуктов по организации и мониторингу ИБ предприятия	ОПК-5.1 ОПК-5.2 ОПК-5.3
12.		4	Работа подразделения ИБ при управлении ИБ предприятия	ОПК-5.1 ОПК-5.2 ОПК-5.3
	<b>ВСЕГО</b>	<b>63</b>		

## 8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Базовые вопросы управления	5	написание реферата, подготовка к лабораторной работе	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.	Процессный подход	5	написание реферата, подготовка к лабораторной работе	ОПК-5.1 ОПК-5.2 ОПК-5.3
3.	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности	8	написание реферата, подготовка к лабораторной работе	ОПК-5.1 ОПК-5.2 ОПК-5.3
4.	Разработка системы управления информационной безопасности (СУИБ) предприятия на основе процессного подхода	9	написание реферата, подготовка к лабораторной работе	ОПК-5.1 ОПК-5.2 ОПК-5.3
5.	Стандартизация в области управления	2	подготовка к лабораторной работе,	ОПК-5.1

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
	ИБ		подготовка к экзамену	ОПК-5.2 ОПК-5.3
6.	Определение области и границ действия СУИБ	2	подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.1 ОПК-5.2 ОПК-5.3
7.	Ролевая структура СУИБ	2	подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.1 ОПК-5.2 ОПК-5.3
8.	Определение политики СУИБ. Правила разработки политик информационной безопасности (ИБ)	5	подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.1 ОПК-5.2 ОПК-5.3
9.	Управление информационными рисками. Выбор целей и мер управления для обработки рисков ИБ	2	подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.1 ОПК-5.2 ОПК-5.3
10.	Эксплуатация и независимый аудит СУИБ	2	подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.1 ОПК-5.2 ОПК-5.3
11.	Процесс «Обеспечение непрерывности ведения бизнеса»	3	подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.1 ОПК-5.2 ОПК-5.3
12.	Курсовая работа	18	подготовка к контрольной работе	ОПК-5.1 ОПК-5.2 ОПК-5.3
	<b>ВСЕГО</b>	<b>63</b>		

### 8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Базовые вопросы управления	5	прием лабораторной работы, проверка реферата	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.	Процессный подход	5	прием лабораторной работы, проверка реферата	ОПК-5.1 ОПК-5.2 ОПК-5.3
3.	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности	5	прием лабораторной работы, проверка реферата	ОПК-5.1 ОПК-5.2 ОПК-5.3
4.	Разработка системы управления информационной безопасности (СУИБ) предприятия на основе процессного подхода	12	прием лабораторной работы, проверка реферата	ОПК-5.1 ОПК-5.2 ОПК-5.3
5.	Определение области и границ действия СУИБ	2	прием лабораторной работы, прием экзамена	ОПК-5.1 ОПК-5.2 ОПК-5.3
6.	Ролевая структура СУИБ	2	прием лабораторной работы, прием экзамена	ОПК-5.1 ОПК-5.2 ОПК-5.3
7.	Стандартизация в области управления ИБ	3	прием лабораторной работы, прием экзамена	ОПК-5.1 ОПК-5.2 ОПК-5.3
8.	Определение политики СУИБ. Правила разработки политик информационной безопасности (ИБ)	2	прием лабораторной работы, прием экзамена	ОПК-5.1 ОПК-5.2 ОПК-5.3
9.	Управление информационными рисками. Выбор целей и мер управления для обработки рисков ИБ	3	прием лабораторной работы, прием экзамена	ОПК-5.1 ОПК-5.2 ОПК-5.3
10.	Эксплуатация и независимый аудит СУИБ	4	прием лабораторной работы, прием экзамена	ОПК-5.1 ОПК-5.2 ОПК-5.3
11.	Процесс «Обеспечение непрерывности	2	прием лабораторной работы, прием	ОПК-5.1

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
	ведения бизнеса»		экзамена	ОПК-5.2 ОПК-5.3
12.	Курсовая работа	18	проверка курсовой работы	ОПК-5.1 ОПК-5.2 ОПК-5.3
	<b>ВСЕГО</b>	<b>63</b>		

## 9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Основы управления информационной безопасностью» 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
<b>7-й семестр</b>			
Реферат	1	30	50
Лабораторная работа	7	30	50
<b>Итого</b>		<b>60</b>	<b>100</b>
<b>8-й семестр</b>			
Лабораторная работа	5	36	60
Экзамен	1	24	40
<b>Итого</b>		<b>60</b>	<b>100</b>
<b>8-й семестр</b>			
Курсовая работа	1	60	100
<b>Итого</b>		<b>60</b>	<b>100</b>

## 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 «Основы управления информационной безопасностью» 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	<a href="http://znanium.com/go.php?id=1114032">http://znanium.com/go.php?id=1114032</a> Режим доступа: по подписке КНИТУ
А. А. Бирюков, Информационная безопасность: защита и нападение	<a href="https://e.lanbook.com/book/93278">https://e.lanbook.com/book/93278</a> Режим доступа: по подписке КНИТУ

[Электронный ресурс] : Москва : ДМК Пресс, 2017	
А.П. Жук, Е.П. Жук, Защита информации [Прочее] Учебное пособие: Москва : Издательский Центр РИОР, 2021	<a href="http://znanium.com/catalog/document?id=367588">http://znanium.com/catalog/document?id=367588</a> 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	<a href="https://www.book.ru/book/934814">https://www.book.ru/book/934814</a> 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»
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»
Э. Таненбаум, Современные операционные системы [Прочее] : М. [и др.] : Питер, 2006	9 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Э. Таненбаум, Компьютерные сети [Прочее] : М. [и др.] : Питер, 2005	26 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Н. В. Тюльпинова,, Защита интеллектуальной собственности и компьютерной информации [Прочее] учебное пособие для магистров: Саратов : Вузовское образование, 2020	<a href="http://www.iprbookshop.ru/88755.html">http://www.iprbookshop.ru/88755.html</a> 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	<a href="http://www.iprbookshop.ru/97565.html">http://www.iprbookshop.ru/97565.html</a> Режим доступа: по подписке КНИТУ
В. О. Сафонов, Основы современных операционных систем [Электронный ресурс] : Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	<a href="http://www.iprbookshop.ru/62818.html">http://www.iprbookshop.ru/62818.html</a> Режим доступа: по подписке КНИТУ

### 11.3. Электронные источники информации

При изучении дисциплины «Основы управления информационной безопасностью» 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](http://www.scopus.com)

Web of Science Доступ свободный: [apps.webofknowledge.com](http://apps.webofknowledge.com)

Информационные справочные системы

Справочно-правовая система «ГАРАНТ» Доступ свободный: [www.garant.ru](http://www.garant.ru)

Справочно-правовая система «КонсультантПлюс» Доступ свободный: [www.consultant.ru](http://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 «Основы управления информационной безопасностью»:

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.

Помещения для самостоятельной работы оснащены компьютерной техникой 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 «Основы управления информационной безопасностью» составляет 27 ч.

В процессе освоения дисциплины «Основы управления информационной безопасностью» используются следующие образовательные технологии:

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

