

**ГАОУ ВО «Дагестанский государственный университет  
народного хозяйства»**

*Утверждена решением  
Ученого совета ДГУНХ,  
протокол № 11  
от 06 июня 2023 г*

**Кафедра «Информационные технологии и информационная  
безопасность»**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗ-  
ОПАСНОСТЬЮ»**

**Направление подготовки**

**10.03.01 Информационная безопасность,**

**профиль «Безопасность автоматизированных систем»**

**Уровень высшего образования - бакалавриат**

**Формы обучения – очная, очно-заочная**

**Махачкала – 2023**

**УДК 681.518(075.8)**

**ББК 32.81.73**

**Составитель** – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент** – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внешний рецензент** – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

**Представитель работодателя** - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

*Рабочая программа дисциплины «Основы управления информационной безопасностью» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»*

Рабочая программа по дисциплине «Основы управления информационной безопасностью» размещена на официальном сайте [www.dgunh.ru](http://www.dgunh.ru)

Гасанова З.А. Рабочая программа по дисциплине «Основы управления информационной безопасностью» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г., 17 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

## Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине...	4
Раздел 2. Место дисциплины в структуре образовательной программы...	6
Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся и форму(ы) промежуточной аттестации.....	6
Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.....	8
Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	12
Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	14
Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных.....	14
Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	15
Раздел 9. Образовательные технологии.....	16
Лист актуализации рабочей программы дисциплины.....	17

## Раздел 1. Перечень планируемых результатов обучения по дисциплине

Целью дисциплины «Основы управления информационной безопасностью» является формирование у студентов компетенции обучающегося в области основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

Задачами дисциплины являются:

- Рассмотреть основы управления информационной безопасностью.
- Раскрыть принципы проектирования и реализации системы управления информационной безопасности (ИБ) конкретного объекта
- Показать особенности сопровождения системы управления информационной безопасностью на предприятиях различных масштабов и отраслевой принадлежности.

### 1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Основы управления информационной безопасностью» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах

### 1.2. Планируемые результаты обучения по дисциплине

<i>Код и наименование компетенции</i>	<i>Код и наименование индикатора достижения компетенции</i>	<i>Планируемые результаты обучения по дисциплине</i>
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информаци-	ИОПК-10.1. Выбирает принципы формирования политики информационной безопасности в информационных	<b>Знать:</b> 31 - принципы формирования политики информационной безопасности в информационных системах. 32 - основы организации и методологии проведения аудита ИБ; 33 - методы и инструментальные средства проведения активного аудита ИБ.

<p>онной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты</p>	<p>системах</p>	<p><b><u>Уметь:</u></b>  У1 - разрабатывать частные политики информационной безопасности информационных систем.  <b><u>Владеть:</u></b>  В1 – навыками разработки политики безопасности  В2 – методами управления информационной безопасностью  В3 - терминологией и процессным подходом;  В4 - Методами проведения аудита системы ИБ</p>
<p>ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах</p>	<p>ИОПК-4.1.1. Организует деятельность по обнаружению и реагированию на инциденты информационной безопасности</p>	<p><b><u>Знать:</u></b>  31 - основные методы управления инцидентами;  32 – нормативные основы управления инцидентами.  <b><u>Уметь:</u></b>  У1 - разрабатывать организационно-распорядительные документы системы менеджмента инцидентов информационной безопасности организации;  У2 - организовывать деятельность по обнаружению и реагированию на инциденты информационной безопасности в организациях, информационных системах;  <b><u>Владеть:</u></b>  В1 - методами организации и управления деятельностью служб защиты информации на предприятии;</p>
	<p>ИОПК-4.1.2. Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности автоматизированных систем</p>	<p><b><u>Знать:</u></b>  31 - основные стандарты управления ИБ;  32 - основные угрозы безопасности информации и модели нарушителя в информационных системах;  33 - методики анализа рисков, программные средства анализа и управления рисками.  <b><u>Уметь:</u></b>  У1 - проводить классификацию критичных информационных ресурсов;  У2 - анализировать и оценивать информационные риски;  У3 - разрабатывать модели угроз и нарушителей информационной безопасности информационных систем  У4 - разрабатывать предложения по совершенствованию системы управления информационной безопасностью.  <b><u>Владеть:</u></b></p>

		В1 - методами оценки информационных рисков.
--	--	---

### 1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Код компетенции	Этапы формирования компетенций						
	Тема 1. Принципы, подходы и виды управления. Циклическая модель PDCA	Тема 2. Стратегии построения и внедрения СУИБ в организации	Тема 3. Назначение, структура и содержание Политики ИБ. Разработка политики безопасности	Тема 4. Управление рисками	Тема 5. Методы управления рисками	Тема 6. Управление инцидентами ИБ	Тема 7. Аудит ИБ
<b>ОПК-10</b>	+	+	+				+
<b>ОПК-4.1</b>				+	+	+	

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

Дисциплина Б1.О.29 «Основы управления информационной безопасностью» относится к обязательной части Блока 1 «Дисциплины» учебного плана направления подготовки 10.03.01 Информационная безопасность, профиля «Безопасность автоматизированных систем».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Документоведение».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Комплексное обеспечение защиты информации объекта информатизации», «Основы управления информационной безопасностью в автоматизированных системах», «Мониторинг и аудит защищенности информации в автоматизированных системах».

#### Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся, на самостоятельную работу обучающихся и форму промежуточной аттестации

Объем дисциплины в зачетных единицах составляет 3 зачетные единицы.

Очная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 64 часа, в том числе:

на занятия лекционного типа – **32** ч.

на занятия семинарского типа – **32** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **44** ч.

Форма промежуточной аттестации: зачет.

#### Очно-заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 34 часа, в том числе:

на занятия лекционного типа – **17** ч.

на занятия семинарского типа – **17** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **74** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

**Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.**

**Очная форма обучения**

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Тема 1. Принципы, подходы и виды управления. Циклическая модель PDCA	12	4	-	2	-	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейса
2.	Тема 2. Стратегии построения и внедрения СУИБ в организации	14	4	-	4	-	-	-	6	Устный опрос Подготовка реферата Подготовка презентации Письменная работа
3.	Тема 3. Назначение структура и содержание Политики ИБ	14	4	-	4	-	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение проекта Решение кейса
4.	Тема 4. Управление рисками	14	4	-	4	-	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейсов



5.	Тема 5. Методы управления рисками	14	4	-	4	-	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейса Деловая игра
6.	Тема 6. Управление инцидентами ИБ	18	6	-	6	-	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейса
7.	Тема 7. Аудит ИБ	20	6	-	6	-	-	-	8	Устный опрос Тестирование Подготовка реферата Подготовка презентации
8.	Зачет	2	-	-	2	-	-	-	0	-
9.	<b>ИТОГО:</b>	<b>108</b>	<b>32</b>	<b>-</b>	<b>32</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>44</b>	

### Очно-заочная форма обучения

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1	Тема 1. Принципы, подходы и виды управления.	12	2	-	2	-	-	-	8	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейса

	Циклическая модель PDCA									
2.	Тема 2. Стратегии построения и внедрения СУИБ в организации	12	2	-	2	-	-	-	8	Устный опрос Подготовка реферата Подготовка презентации Письменная работа
3.	Тема 3. Назначение структура и содержание Политики ИБ	14	2	-	2	-	-	-	10	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение проекта Решение кейса
4.	Тема 4. Управление рисками	14	2	-	2	-	-	-	10	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейсов
5.	Тема 5. Методы управления рисками	14	2	-	2	-	-	-	10	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейса Деловая игра
6.	Тема 6. Управление инцидентами ИБ	16	3	-	3	-	-	-	10	Устный опрос Тестирование Подготовка реферата Подготовка презентации Решение кейса
7.	Тема 7. Аудит ИБ	24	4	-	2	-	-	-	18	Устный опрос Тестирование Подготовка реферата Подготовка презентации

8.	Зачет	2	-	-	2	-	-	-	0	-
9.	<b>ИТОГО:</b>	<b>108</b>	<b>17</b>	-	<b>17</b>	-	-	-	<b>74</b>	

**Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

<b>№ п/п</b>	<b>Автор</b>	<b>Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины</b>	<b>Выходные данные</b>	<b>Количество экземпляров в библиотеке ДГУНХ/адрес доступа</b>
<b>I. Основная учебная литература</b>				
1.	Аверченков, В.И.	Аудит информационной безопасности : учебное пособие для вузов	Москва : Издательство «Флинта», 2021. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6	<a href="https://biblioclub.ru/index.php?page=book_red&amp;id=93245&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=93245&amp;sr=1</a>
2.	Аверченков, В.И.	Служба защиты информации: организация и управление	Москва : Издательство «Флинта», 2021. - 186 с. ISBN 978-5-9765-1271-9	<a href="https://biblioclub.ru/index.php?page=book_red&amp;id=93356&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=93356&amp;sr=1</a>
3.	Веселов, Г.Е.	Менеджмент риска информационной безопасности	Таганрог : Издательство Южного федерального университета, 2016. - 109 с.	<a href="https://biblioclub.ru/index.php?page=book_red&amp;id=493331&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=493331&amp;sr=1</a>
4.	Пелешенко, В.С.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления	Ставрополь : СКФУ, 2017. - 86 с.	<a href="https://biblioclub.ru/index.php?page=book_red&amp;id=467139&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=467139&amp;sr=1</a>
<b>II. Дополнительная учебная литература</b>				
<b>A) Дополнительная учебная литература</b>				
1.	-	Аудит информационной безопасности органов исполнительной власти: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский.	Москва : Издательство «Флинта», 2016. - 100 с. ISBN 978-5-9765-1277-1	<a href="https://biblioclub.ru/index.php?page=book_red&amp;id=93259&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=93259&amp;sr=1</a>
2.	Ковалев Д.В.	Информационная безопасность	Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. ISBN 978-5-9275-2364-1	<a href="https://biblioclub.ru/index.php?page=book_red&amp;id=493175&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=493175&amp;sr=1</a>

3.	Пакин А.И.	Информационная безопасность информационных систем управления предприятием	Москва : Альтаир : МГАВТ, 2009. - 41 с.	<a href="https://biblioclub.ru/index.php?page=book_red&amp;id=429778&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=429778&amp;sr=1</a>
<b>Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ</b>				
1.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).			
2.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>			
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. <a href="http://www.standartgost.ru">www.standartgost.ru</a>			
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>			
5.	ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» <a href="http://www.standartgost.ru">www.standartgost.ru</a>			
6.	ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. <a href="http://www.standartgost.ru">www.standartgost.ru</a>			
7.	ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» <a href="http://www.standartgost.ru">www.standartgost.ru</a>			
<b>В) Периодические издания</b>				
1.	Журнал для пользователей персональных компьютеров «Мир ПК»			
2.	Научный журнал «Информатика и ее применение»			
3.	Информатика и безопасность			
4.	Журнал о компьютерах и цифровой технике «Computer Bild»			
5.	Рецензируемый научный журнал «Информатика и система управления»			
6.	Рецензируемый научный журнал «Проблемы информационной безопасности»			
<b>Г) Справочно-библиографическая литература</b>				
1.	1. Краткий энциклопедический словарь по информационной безопасности <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=58393&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=58393&amp;sr=1</a>			

## **Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (<http://e-dgunh.ru>). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области менеджмента информационной безопасности, рекомендуется использовать следующие Интернет-ресурсы:

1. <http://www.fsb.ru/> – официальный сайт ФСБ
2. <http://fstec.ru/> – официальный сайт ФСТЭК
3. <http://www.consultant.ru/> – онлайн-версия информационно-правовой системы "КонсультантПлюс"
4. <http://Standartgost.ru> - Открытая база ГОСТов

## **Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных**

### **7.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства**

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip
- Справочно-правовая система «КонсультантПлюс»

### **7.2. Перечень информационных справочных систем:**

- информационно справочная система «КонсультантПлюс».

### **7.3. Перечень профессиональных баз данных:**

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (<https://fstec.ru/tehnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>).
- Реестр операторов, осуществляющих обработку персональных данных (<https://rkn.gov.ru/personal-data/register/>);
- <http://Standartgost.ru> - Открытая база ГОСТов

## **Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Для преподавания дисциплины «Основы управления информационной безопасностью» используются следующие специальные помещения и учебные аудитории:

**Учебная аудитория для проведения учебных занятий № 4.11 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)**

### ***Перечень основного оборудования:***

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, ноутбук с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» ([www.biblioclub.ru](http://www.biblioclub.ru)), ЭБС «ЭБС Юрайт» ([www.ura.it.ru](http://www.ura.it.ru)).

### ***Перечень учебно-наглядных пособий:***

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Компьютерный класс, учебная аудитория для проведения учебных занятий № 4.2 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)**

### ***Перечень***

### ***Перечень основного оборудования:***

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, акустическая система.

Персональные компьютеры с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» ([www.biblioclub.ru](http://www.biblioclub.ru)), ЭБС «ЭБС Юрайт» ([www.ura.it.ru](http://www.ura.it.ru)) – 20 ед.

### ***Перечень учебно-наглядных пособий:***

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Помещение для самостоятельной работы № 4.5 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)**

### ***Перечень основного оборудования:***

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 24 ед.

**Помещение для самостоятельной работы № 1-1 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1)**

### ***Перечень основного оборудования:***

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

## Раздел 9. Образовательные технологии

При освоении дисциплины «Основы управления информационной безопасностью» используются следующие образовательные технологии:

- деловые и ролевые игры для выработки навыков принятия решения в случае инцидентов информационной безопасности;
- разбор конкретных ситуаций как для иллюстрации той или иной ситуации, так и в целях выработки навыков применения управленческих решений;
- проектная деятельность для выработки умений анализа информационных активов предприятия и разработки документов, регламентирующих деятельность по управлению информационной безопасностью в организации.
- внеаудиторная работа в форме обязательных консультаций и индивидуальных занятий со студентами (помощь в понимании тех или иных моделей и концепций, подготовка рефератов и эссе, а также тезисов для студенческих конференций и т.д.).



**Лист актуализации рабочей программы дисциплины  
«Основы управления информационной безопасностью»**

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_