

ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

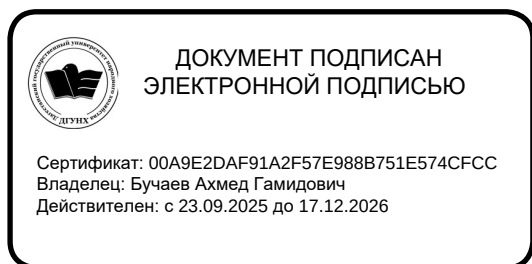
*Утверждена решением
Ученого совета ДГУНХ,
протокол № 9
от 21 марта 2026 г.*

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

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

**Направление подготовки 38.03.05 Бизнес-информатика,
профиль «Менеджмент информационных технологий и электрон-
ный бизнес»**

**Уровень высшего образования - бакалавриат
Формы обучения – очная, очно-заочная, заочная**



Махачкала – 2026

УДК 004.056.5

ББК 32.973.2

Составитель – Меджидов Заур Уруджалиевич, кандидат экономических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент - Гасанова Зарема Ахмедовна, кандидат педагогических наук, доцент, и.о. заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Меджидов Зияудин Гаджиевич, кандидат физико-математических наук, старший научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской Академии Наук

Представитель работодателя - Ботвин Тимур Анатольевич, директор по продажам в отделе продаж Яндекс Маркет для бизнеса в ООО «Технолоджикал Деливери Сервисез».

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 29 июля 2021 г., № 838, 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 «Информационная безопасность» размещена на официальном сайте www.dgunh.ru

Меджидов З.У. Рабочая программа по дисциплине «Информационная безопасность» для направления подготовки 38.03.05 Бизнес-информатика, профиль «Менеджмент информационных технологий и электронный бизнес». – Махачкала: ДГУНХ, 2026 г., 17 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 10 марта 2026 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 38.03.05 Бизнес-информатика, профиль «Менеджмент информационных технологий и электронный бизнес», д.э.н., Савзихановой С.Э.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 24 февраля 2026 г., протокол № 7.

Содержание

Раздел 1.	Перечень планируемых результатов обучения по дисциплине	4
Раздел 2.	Место дисциплины в структуре образовательной программы	5
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	7
Раздел 5.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	13
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

Цель дисциплины – сформировать компетенции обучающегося в области решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности и организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия.

Задачи изучения дисциплины

- Рассмотреть основные методики и подходы обеспечения информационной безопасности в рамках современных автоматизированных систем.
- Раскрыть принципы построения защищенных информационных систем и поддержания подсистемы защиты информации в актуальном состоянии.
- Показать особенности реализации общих методик защиты информации на различных платформах.

1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Информационной безопасности» как часть планируемых результатов освоения образовательной программы образования

код компетенции	формулировка компетенции
ПК	ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ
ПК-4	Способен разрабатывать и реализовывать проекты совершенствования ИТ-инфраструктуры предприятия для достижения стратегических целей и поддержки бизнес-процессов с учетом требований информационной безопасности

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>
ПК-4. Способен разрабатывать и реализовывать проекты совершенствования ИТ-инфраструктуры предприятия для достижения стратегических целей и поддержки бизнес-процессов с учетом требований информационной безопасности	ИПК-4.2. Управляет информационной безопасностью предприятия	<u>Знать:</u> - основные информационно-коммуникационные технологии и основные требования информационной безопасности; - виды угроз ИС и методы обеспечения информационной безопасности <u>Уметь:</u> - решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности; - выявлять угрозы информационной безопасности; <u>Владеть:</u> - культурой применения информационно-коммуникационных

		технологий с учетом основных требований информационной безопасности; - основными технологиями построения защищённых экономических информационных систем.
--	--	---

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

Код компетенции	Этапы формирования компетенций						
	Тема 1. Введение в информационную безопасность.	Тема 2. Задачи и методы информационной безопасности.	Тема 3. Угрозы информационной безопасности	Тема 4. Потенциальные противники и атаки.	Тема 5. Основные положения теории информационной безопасности информационных систем.	Тема 6. Политика безопасности информационных систем.	Тема 7. Организационно-правовые методы информационной безопасности.
ПК-4	+	+	+	+	+	+	+

Код компетенции	Этапы формирования компетенций						
	Тема 8. Основные понятия криптографии.	Тема 9. Криптографические протоколы.	Тема 10. Программно-технические методы защиты.	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	Тема 12. Стандарты обеспечения информационной безопасности.	Тема 13. Основные технологии построения защищённых экономических информационных систем.	
ПК -4	+	+	+	+	+	+	

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.09 «Информационная безопасность» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины» учебного плана направления подготовки 38.03.05 Бизнес-информатика, профиля «Менеджмент информационных технологий и электронный бизнес».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Право и антикоррупционное поведение», «Вычислительные системы, сети и телекоммуникации», «Базы данных», «Операционные системы», «Web-программирование».

Освоение данной дисциплины необходимо обучающемуся для успешного прохождения производственной практики и выполнения выпускной квалификационной работы.

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

Объем дисциплины в зачетных единицах составляет 4 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: экзамен, 36 ч.

Очно-заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 18 часов, в том числе:

на занятия лекционного типа – 9 ч.

на занятия семинарского типа – 9 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – 90 ч.

Форма промежуточной аттестации: экзамен, 36 ч.

Заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 14 часов, в том числе:

на занятия лекционного типа – 6 ч.

на занятия семинарского типа – 8 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – 126 ч.

Форма промежуточной аттестации: экзамен, 4ч.

Отдельные учебные занятия по дисциплине реализуются в форме практической подготовки.

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

Очное отделение

№ 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. Форма промежуточной аттестации
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
	Тема 1. Введение в информационную безопасность.	6	2	-	1	1	-	-	2	Проведение опроса Выполнение лабораторной работы
	Тема 2. Задачи и методы информационной безопасности.	6	2	-	1	1	-	-	2	Проведение опроса Выполнение лабораторной работы
	Тема 3. Угрозы информационной безопасности.*	6	2*	-	1*	1*	-	-	2	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 4. Потенциальные противники и атаки.	6	2	-	1	1	-	-	2	Проведение опроса Выполнение лабораторной работы
	Тема 5. Основные положения теории информационной безопасности информационных систем.	8	2	-	1	1	-	-	4	Проведение опроса Выполнение лабораторной работы
	Тема 6. Политика безопасности информационных систем.*	8	2*	-	1*	1*	-	-	4	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 7. Организационно-правовые методы информационной безопасности.*	12	4*	-	2*	2*	-	-	4	Проведение опроса Выполнение лабораторной работы
	Тема 8. Основные понятия криптографии.	8	2	-	1	1	-	-	4	Проведение опроса Выполнение лабора-

										торной работы
	Тема 9. Криптографические протоколы.	12	4	-	2	2	-	-	4	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 10. Программно-технические методы защиты.	12	4	-	2	2	-	-	4	Проведение опроса Выполнение лабораторной работы
	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	8	2	-	1	1	-	-	4	Проведение опроса Выполнение лабораторной работы
	Тема 12. Стандарты обеспечения информационной безопасности.*	8	2*	-	1*	1*	-	-	4	Проведение опроса Выполнение лабораторной работы
	Тема 13. Основные технологии построения защищённых экономических информационных систем.	8	2	-	1	1	-	-	4	Проведение опроса Выполнение лабораторной работы Деловая игра
	Итого	108	32	-	16	16	-	-	44	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	36								Контроль
	ВСЕГО:	144								

Очно-заочное отделение

№ 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		

	Тема 1. Введение в информационную безопасность.	8	1	-	1	0	-	-	6	Проведение опроса Выполнение лабораторной работы
	Тема 2. Задачи и методы информационной безопасности.	8	1	-	1	0	-	-	6	Проведение опроса Выполнение лабораторной работы
	Тема 3. Угрозы информационной безопасности.*	9	1*	-	1*	1*	-	-	6	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 4. Потенциальные противники и атаки.	9	1	-	1	1	-	-	6	Проведение опроса Выполнение лабораторной работы
	Тема 5. Основные положения теории информационной безопасности информационных систем.	8	1	-	1	0	-	-	6	Проведение опроса Выполнение лабораторной работы
	Тема 6. Политика безопасности информационных систем.*	7	1*	-	0	0	-	-	6	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 7. Организационно-правовые методы информационной безопасности.*	7	1*	-	0	0	-	-	6	Проведение опроса Выполнение лабораторной работы
	Тема 8. Основные понятия криптографии.	9	1	-	0	0	-	-	8	Проведение опроса Выполнение лабораторной работы
	Тема 9. Криптографические протоколы.	9	1	-	0	0	-	-	8	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 10. Программно-технические методы защиты.	9	0	-	0	1	-	-	8	Проведение опроса Выполнение лабораторной работы

	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	9	0	-	0	1	-	-	8	Проведение опроса Выполнение лабораторной работы
	Тема 12. Стандарты обеспечения информационной безопасности.	8	0	-	0	0	-	-	8	Проведение опроса Выполнение лабораторной работы
	Тема 13. Основные технологии построения защищённых экономических информационных систем.	8	0	-	0	0	-	-	8	Проведение опроса Выполнение лабораторной работы Тестирование
	Итого	108	9	-	5	4	-	-	90	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	36								Контроль
	ВСЕГО:	144								

Заочное отделение

№ 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		
	Тема 1. Введение в информационную безопасность.	10	1	-	1	0	-	-	8	Проведение опроса Выполнение лабораторной работы
	Тема 2. Задачи и методы информационной безопасности.	10	1	-	1	0	-	-	8	Проведение опроса Выполнение лабораторной работы
	Тема 3. Угрозы информационной	13	1*	-	1*	1*	-	-	10	Проведение опроса

	безопасности.*									Выполнение лабораторной работы Тестирование
	Тема 4. Потенциальные противники и атаки.	13	1	-	1	1	-	-	10	Проведение опроса Выполнение лабораторной работы
	Тема 5. Основные положения теории информационной безопасности информационных систем.	11	1	-	0	0	-	-	10	Проведение опроса Выполнение лабораторной работы
	Тема 6. Политика безопасности информационных систем.*	11	1*	-	0	0	-	-	10	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 7. Организационно-правовые методы информационной безопасности.	10	0	-	0	0	-	-	10	Проведение опроса Выполнение лабораторной работы
	Тема 8. Основные понятия криптографии.	10	0	-	0	0	-	-	10	Проведение опроса Выполнение лабораторной работы
	Тема 9. Криптографические протоколы.	10	0	-	0	0	-	-	10	Проведение опроса Выполнение лабораторной работы Тестирование
	Тема 10. Программно-технические методы защиты.	11	0	-	0	1	-	-	10	Проведение опроса Выполнение лабораторной работы
	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	11	0	-	0	1	-	-	10	Проведение опроса Выполнение лабораторной работы
	Тема 12. Стандарты обеспечения информационной безопасности.	10	0	-	0	0	-	-	10	Проведение опроса Выполнение лабораторной работы
	Тема 13. Основные технологии	10	0	-	0	0	-	-	10	Проведение опроса

	построения защищённых экономических информационных систем.									Выполнение лабораторной работы Тестирование
	Итого	140	6	-	4	4	-	-	126	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	4								Контроль
	ВСЕГО:	144								

*Реализуется в форме практической подготовки

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

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
I. Основная учебная литература				
1.	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие	Москва; Берлин: Директ-Медиа, 2015. - 253 с	https://biblioclub.ru/index.php?page=book_red&id=276557&sr=1
2.	Ю.Н. Загинайлов	Основы информационной безопасности : курс визуальных лекций: учебное пособие	Москва; Берлин: Директ-Медиа, 2015. - 105 с	https://biblioclub.ru/index.php?page=book_red&id=362895&sr=1
II. Дополнительная учебная литература				
А) Дополнительная учебная литература				
1.	Петренко В.И	Теоретические основы защиты информации : учебное пособие	Ставрополь: СКФУ, 2015. - 222 с.	https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1
2.	Шилов, А.К.	Управление информационной безопасностью : учебное пособие/	Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2018. – 121 с.	https://biblioclub.ru/index.php?page=book_red&id=500065&sr=1
Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ				
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. www.standartgost.ru			
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru			
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru			
5.	ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru			
6.	ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информа-			

	ционной безопасности. www.standartgost.ru
7.	ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» www.standartgost.ru
<i>В) Периодические издания</i>	
1.	Научный журнал «Информатика и ее применение»
2.	Информатика и безопасность
3.	Рецензируемый научный журнал «Информатика и система управления»
4.	Рецензируемый научный журнал «Проблемы информационной безопасности»
<i>Г) Справочно-библиографическая литература</i>	
1.	1. Краткий энциклопедический словарь по информационной безопасности https://biblioclub.ru/index.php?page=book_red&id=58393&sr=1

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

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 информационных технологий, используемых при изучении дисциплины, включая перечень лицензионного программного обеспечения, информационных справочных систем, 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
- Microsoft Visual Studio
- Справочно-правовая система «Консультант Плюс»

7.2. Перечень информационных справочных систем:

- информационно справочная система «Консультант Плюс».

7.3. Перечень профессиональных баз данных:

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (<https://fstec.ru/tekhnicheskaya-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
- Научная электронная библиотека <https://elibrary.ru/>

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

Для преподавания дисциплины «Информационная безопасность» используются следующие специальные помещения – **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, персональный компьютер (моноблок) с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.urait.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 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), ЭБС «ЭБС Юрайт» (www.urait.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 Даге-

стан, 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 «Информационная безопасность» используются следующие образовательные технологии:

1. Проблемные лекции;
2. Практические занятия в форме практикума ;
3. Использование медиаресурсов, энциклопедий, электронных библиотек и Интернет;
4. Информационный проект;
5. Проведение занятий в режиме видеоконференцсвязи;
6. Консультирование студентов с использованием электронной почты.

Лист актуализации рабочей программы дисциплины

«Информационная безопасность»

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 _____