

**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  
«ЗАЩИТА ИНФОРМАЦИИ ОТ ВНУТРЕННИХ ИТ-  
УГРОЗ»**

**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

**Составители** – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, зав.кафедрой «Информационные технологии и информационная безопасность» ДГУНХ; Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент** – Раджабов Карахан Якубович, кандидат экономических наук, доцент, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

**Внешний рецензент** – Абдуллаев Ших-Саид Омаржанович, доктор технических наук, главный научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской академии наук.

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

*Рабочая программа дисциплины «Защита информации от внутренних IT-угроз» 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 «Защита информации от внутренних IT-угроз» размещена на официальном сайте [www.dgunh.ru](http://www.dgunh.ru)

Галяев В.С., Гасанова З.А. Рабочая программа по дисциплине «Защита информации от внутренних IT-угроз» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г., 16 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 формы промежуточной аттестации	7
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	11
Раздел 6.	Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
Раздел 7.	Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных	13
Раздел 8.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	14
Раздел 9.	Образовательные технологии	15
	Лист актуализации рабочей программы дисциплины	16

## Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины – сформировать компетенции обучающегося в области методов и подходов организации защиты корпоративной информации, а также закрытых сведений от внутренних IT-угроз, с учетом действующих нормативных и методических документов.

Задачи дисциплины:

- Рассмотреть основные типы внутренних IT-угроз и связанные с ними риски.
- Раскрыть принципы проведения профилактических мероприятия по предотвращению утечек информации, а также устранению последствий в случае утечки информации.
- Показать особенности утечки информации по различным каналам, связанным с инфраструктурой организации, а также человеческим фактором.

### 1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Защита информации от внутренних IT-угроз» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
<b>ПК</b>	<b>ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ</b>
<b>ПК-1.</b>	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей
<b>ПК-2.</b>	Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации

### 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-1. Способен выполнять комплекс задач администрирования	ИПК-1.1. Администрирует подсистему защиты информации операционных систем	<b><u>Знать:</u></b> 31 - угрозы безопасности информации и модели нарушителя в операционных системах; <b><u>Уметь:</u></b>

подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей		<p>У1 - разрабатывать модели угроз и нарушителей информационной безопасности операционных систем;</p> <p><b><u>Владеть:</u></b>  В1 - навыками конфигурирования параметров системы защиты операционных систем.</p>
	ИПК-1.2. Администрирует подсистему защиты информации СУБД	<p><b><u>Знать:</u></b>  З1 - угрозы безопасности информации и модели нарушителя информационной безопасности СУБД;</p> <p><b><u>Уметь:</u></b>  У1 - разрабатывать модели угроз и нарушителей информационной безопасности СУБД;</p> <p><b><u>Владеть:</u></b>  В1 - навыками конфигурирования параметров системы защиты информации СУБД.</p>
	ИПК-1.3. Администрирует подсистему защиты информации компьютерных сетей	<p><b><u>Знать:</u></b>  З1 - угрозы безопасности информации и модели нарушителя информационной безопасности компьютерных сетей;</p> <p><b><u>Уметь:</u></b>  У1 - разрабатывать модели угроз и нарушителей информационной безопасности компьютерных сетей;</p> <p><b><u>Владеть:</u></b>  В1 - навыками конфигурирования параметров системы защиты информации компьютерных сетей.</p>
ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в	ИПК-2.2. Обеспечивает безопасность информационных технологий, применяемых в автоматизированных системах	<p><b><u>Знать:</u></b>  З1 - особенности информационных технологий, применяемых в автоматизированных системах;</p> <p><b><u>Уметь:</u></b>  У1 – анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах;</p>

них информации		<p>У2 - осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации.</p> <p><b>Владеть:</b></p> <p>В1 - навыками конфигурирования параметров системы защиты информации автоматизированных систем, с учетом применяемых информационных технологий</p>
----------------	--	---

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

Код компетенции	Этапы формирования компетенций							
	Тема 1. Общая постановка задачи защиты от внутренних ИТ-угроз	Тема 2. Оценка ресурсов компании	Тема 3. Основные направления защиты	Тема 4. Виды конфиденциальной информации и уровни защиты	Тема 5. Классификация внутренних нарушителей	Тема 6. Правовые и организационные средства защиты	Тема 7. Технические средства защиты	Тема 8. Администрирование информационных ресурсов и потоков
ПК-1				+	+		+	+
ПК-2	+	+	+			+		

## Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.5.1 «Защита информации от внутренних ИТ-угроз» относится к дисциплинам по выбору 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 «Сети и системы передачи информации», «Аппаратные средства вычислительной техники», «Информационные технологии», «Теория информации», «Основы информационной безопасности», «Методы и средства криптографической защиты информации», «Программно-аппаратные средства защиты информации», «Безопасность вычислительных сетей», «Безопасность операционных систем», «Безопасность систем баз данных», «Технология построения защищённых автоматизированных систем».

Знания, умения и навыки, полученные студентами в рамках данной дисциплины, пригодятся им при написании выпускной квалификационной работы, а также при прохождении производственной практики.

**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 4 зачетные единицы.

**Очная форма обучения**

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 75 часов, в том числе:

на занятия лекционного типа – **30** ч.

на занятия семинарского типа – **45** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **33** 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 50 часов, в том числе:

на занятия лекционного типа – **20** ч.

на занятия семинарского типа – **30** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **58** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

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.**

**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 англоязычные занятия		
1	Тема 1. Общая постановка задачи защиты от внутренних IT-угроз	9	2	-	3	-	-	-	4	Проведение опроса Тестирование
2	Тема 2. Оценка ресурсов компании	14	4	-	3	3	-	-	4	Проведение опроса Тестирование Выполнение лабораторной работы
3	Тема 3. Основные направления защиты	14	4	-	3	3	-	-	4	Проведение опроса Тестирование Выполнение лабораторной работы
4	Тема 4. Виды конфиденциальной информации и уровни защиты*	14	4*	-	3*	3*	-	-	4	Проведение опроса Тестирование Выполнение лабораторной работы
5	Тема 5. Классификация внутренних нарушителей*	14	4*	-	3*	3*	-	-	4	Проведение опроса Тестирование Выполнение лабораторной работы
6	Тема 6. Правовые и организационные средства защиты	14	4	-	3	3	-	-	4	Проведение опроса Тестирование Выполнение лабораторной работы
7	Тема 7. Технические средства защиты	14	4	-	6	-	-	-	4	Проведение опроса Тестирование

8	Тема 8. Администрирование информационных ресурсов и потоков*	15	4*	-	6*	-	-	-	5	Проведение опроса Тестирование
9	<b>ИТОГО:</b>	108	30		30	15			33	
10	<b>Экзамен</b> (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	36								
	<b>ВСЕГО:</b>	144								

### 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 анфлогичные занятия		
1	Тема 1. Общая постановка задачи защиты от внутренних IT-угроз	11	2	-	2	-	-	-	7	Проведение опроса Тестирование
2	Тема 2. Оценка ресурсов компании	13	2	-	2	2	-	-	7	Проведение опроса Тестирование Выполнение лабораторной работы
3	Тема 3. Основные направления защиты	17	4	-	4	2	-	-	7	Проведение опроса Тестирование Выполнение лабораторной работы

4	Тема 4. Виды конфиденциальной информации и уровни защиты*	13	2*	-	2*	2*	-	-	7	Проведение опроса Тестирование Выполнение лабораторной работы
5	Тема 5. Классификация внутренних нарушителей*	13	2*	-	2*	2*	-	-	7	Проведение опроса Тестирование Выполнение лабораторной работы
6	Тема 6. Правовые и организационные средства защиты	13	2	-	2	2	-	-	7	Проведение опроса Тестирование Выполнение лабораторной работы
7	Тема 7. Технические средства защиты	12	2	-	2	-	-	-	8	Проведение опроса Тестирование
8	Тема 8. Администрирование информационных ресурсов и потоков*	16	4*	-	4*	-	-	-	8	Проведение опроса Тестирование
9	<b>ИТОГО:</b>	108	20		20	10			58	
10	<b>Экзамен</b> (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)					36				Контроль
	<b>ВСЕГО:</b>					144				

\*Реализуется в форме практической подготовки

**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.	Моргунов А.В.	Информационная безопасность : учебно-методическое пособие	Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. - 978-5-7782-3918-0	<a href="https://biblioclub.ru/index.php?page=book&amp;id=576726">https://biblioclub.ru/index.php?page=book&amp;id=576726</a>
2.	Скляр В. В.	Обеспечение безопасности АСУТП в соответствии с современными стандартами	Москва, Вологда: Инфра-Инженерия, 2018. -385 с. - 978-5-9729-0230-9	<a href="http://biblioclub.ru/index.php?page=book&amp;id=493885">http://biblioclub.ru/index.php?page=book&amp;id=493885</a>
<b>II. Дополнительная учебная литература</b>				
<b>A) Дополнительная учебная литература</b>				
1.	Загинайлов Ю.Н.	Теория информационной безопасности и методология защиты информации	Москва; Берлин: Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7	<a href="http://biblioclub.ru/index.php?page=book&amp;id=276557">http://biblioclub.ru/index.php?page=book&amp;id=276557</a>
2.	Ковалев Д.В.	Информационная безопасность	Ростов-на-Дону: Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1	<a href="http://biblioclub.ru/index.php?page=book&amp;id=493175">http://biblioclub.ru/index.php?page=book&amp;id=493175</a>
3.	Котова Л.В.	Сборник задач по дисциплине «Методы и средства защиты информации»	Москва: МПГУ, 2015. - 44 с. : ил. - Библиогр. в кн. - ISBN 978-5-4263-0221-1	<a href="http://biblioclub.ru/index.php?page=book&amp;id=469877">http://biblioclub.ru/index.php?page=book&amp;id=469877</a>
4.	Спицын В.Г.	Информационная безопасность вычислительной техники	Томск: Эль Кон-тент, 2011. - 148 с.: ил., табл.,	<a href="http://biblioclub.ru/index.php?page=book&amp;id=469877">http://biblioclub.ru/index.php?page=book&amp;id=469877</a>

			схем. - ISBN 978-5-4332-0020-3	<a href="#">age=book&amp;id=208694</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 : словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. <a href="http://biblioclub.ru/index.php?page=book&amp;id=58393">http://biblioclub.ru/index.php?page=book&amp;id=58393</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 России;
2. <http://fstec.ru/> – официальный сайт ФСТЭК России;
3. <http://www.consultant.ru/> – онлайн-версия информационно-правовой системы «КонсультантПлюс»;
4. <http://Standartgost.ru/> – открытая база ГОСТов;
5. <http://www.garant.ru/> – онлайн-версия информационно-правовой системы «Гарант».

## **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:**

1. Windows 10
2. Microsoft Office Professional
3. Adobe Acrobat Reader DC
4. VLC Media player
5. 7-zip
6. ПАК Соболь
7. МДЗ-Эшелон
8. Dallas Lock 8.0-K
9. «ФИКС»
10. «Terrier-2.0»
11. «Ревизор-1 XP»
12. «Ревизор-2 XP»
13. AstraLinux
14. DLP-система "Контур информационной безопасности Searchinform"

### **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 (<http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi>);
- Государственный реестр сертифицированных средств защиты информации (<http://clsz.fsb.ru/certification.htm>);
- Научная электронная библиотека (<https://elibrary.ru/>).

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

Для преподавания дисциплины «Защита информации от внутренних IT-угроз» используются следующие специальные помещения:

**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.urait.ru](http://www.urait.ru)).

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

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Лаборатория защищенных автоматизированных систем, учебная аудитория для проведения учебных занятий № 4.13 (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 – 20 ед.

Типовой комплект учебного оборудования «Криптографические системы».

Программно-аппаратные комплексы ViPNet

### ***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

Образовательные технологии, используемые при проведении учебных занятий по дисциплине «Защита информации от внутренних IT-угроз», обеспечивают развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств, поиска информации.

При освоении дисциплины «Организация защиты сведений, составляющих государственную тайну» используются следующие образовательные технологии:

- выполнение лабораторных работ для выработки навыков работы с правовыми и организационными документами, регламентирующими проведение мероприятий по защите конфиденциальных сведений от внутренних IT-угроз;
- проведение устных опросов в целях развития навыков поиска решений и межличностной коммуникации;
- 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  
«Защита информации от внутренних IT-угроз»**

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 \_\_\_\_\_