Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при правительстве Российской Федерации»
(Финансовый университет)

Бузулукский филиал Финуниверситета

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

по актуальным аспектам профессиональной деятельности

«Основы информационной безопасности: правовые аспекты и стандарты»

18 часов

Автор (составитель) – преподаватель
ПЦК экономических, учетных и кредитных дисциплин
Назарова Д.А.

Бузулук 2026

Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при правительстве Российской Федерации»
(Финансовый университет)

Бузулукский филиал Финуниверситета

Обсуждено и одобрено
на совете учебного заведения
Протокол № 3
от 26.03.2026

УТВЕРЖДАЮ
Директор филиала
Н.Н.Щавелева

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы – курсов повышения квалификации
«Основы информационной безопасности: правовые аспекты и стандарты»

Цель	Формирование системных знаний и практических навыков в области обеспечения информационной безопасности (ИБ) на основе требований законодательства Российской Федерации, нормативно-методических документов и профессиональных стандартов, необходимых для защиты информации в организации.
Профессиональная компетенция	Участник научится самостоятельно применять нормы законодательства в области информационной безопасности, разрабатывать и внедрять организационно-распорядительную документацию, обеспечивать соответствие системы защиты информации требованиям регуляторов, а также использовать профессиональные стандарты для построения эффективной системы управления информационной безопасностью в организации.
Категория слушателей	Лица, получающее среднее профессиональное образование и (или) высшее образование; Лица, имеющие среднее профессиональное образование и (или) высшее образование
Срок обучения	18 часов (3 недели)
Форма обучения	Очная с применением дистанционных образовательных технологий
Режим занятий	2 часа в день

	Наименование тем	Всего часов трудоемкости	В том числе				Форма контроля
			Аудиторные занятия			Самостоятельная работа	
			Всего часов	Из них			
				Теоретич.	Практич. за-		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Правовое регулирование отношений в сфере информационной безопасности в РФ.	2	2	-	2	-	
2	Организационно-распорядительная документация по обеспечению ИБ:	2	2	-	2	-	
3	Стандартизация в области ИБ: обзор национальных и международных стандартов (ГОСТ, ISO/IEC 27000).	2	2	-	2	-	
4	Категорирование объектов критической информационной инфраструктуры (КИИ) и правовые аспекты их защиты.	2	2	-	2	-	
5	Защита персональных данных: правовые основы, обязанности оператора, ответственность.	2	2	-	2	-	
6	Лицензирование деятельности по защите государственной тайны и технической защите информации.	2	2	-	2	-	
7	Обеспечение безопасности значимых объектов критической информационной инфраструктуры.	2	2	-	2	-	
8	Организация и проведение внутреннего контроля соблюдения требований по ИБ (комплаенс).	2	2	-	2	-	
9	Ответственность за нарушения в сфере информационной безопасности: административная, гражданско-правовая, уголовная.	2	2	-	2	-	Выполнение кейса
	Всего	18	18	-	18		

Ответственный за ДПО:

_____ Е.С. Петрянкина

Пояснительная записка

1. Направленность программы:

Рабочая программа курсов повышения квалификации «Основы информационной безопасности: правовые аспекты и стандарты» предназначена для выработки целостного восприятия системы правового регулирования и стандартизации в области информационной безопасности. Программа позволит сформировать понимание того, как требования законодательства и стандартов трансформируются в конкретные организационно-распорядительные документы и технические меры защиты, обеспечивающие безопасность организации в условиях цифровой экономики и растущих киберугроз.

2. Актуальность программы.

В условиях стремительной цифровизации всех сфер деятельности, ужесточения требований регуляторов (ФСТЭК, ФСБ, Роскомнадзор) и роста числа инцидентов ИБ, вопросы правовой грамотности и соблюдения стандартов становятся критически важными для устойчивого развития организаций. Слушатели смогут применить полученные знания для построения эффективной системы защиты информации, прохождения проверок надзорных органов, а также для подготовки научных и проектных работ, включая выпускные квалификационные проекты. Программа формирует у специалиста компетенции, необходимые для минимизации юридических рисков и обеспечения соответствия деятельности организации актуальным требованиям

3. Отличительные особенности программы

Основная особенность программы состоит в акцентировании внимания на практических аспектах применения правовых норм и стандартов. Слушатели не только изучают теорию, но и анализируют реальные кейсы из судебной и надзорной практики, учатся разрабатывать локальные акты и оценивать риски.

- Практико-ориентированный подход: Разбор реальных инцидентов, анализ предписаний контролирующих органов, разработка проектов документов (политики ИБ, регламенты)
- Актуальная нормативная база: Изучение последних изменений в законодательстве (152-ФЗ, 187-ФЗ, приказы ФСТЭК) и актуальных версий стандартов.
- Экспертная среда: Программа может быть адаптирована для различных отраслей (финансовый сектор, государственное управление, промышленность) с учетом специфических требований.

4. Цель и задачи программы

Цель программы: Целью программы дополнительного профессионального образования «Основы информационной безопасности: правовые аспекты и стандарты» является формирование и развитие комплекса профессиональных компетенций, позволяющих эффективно применять нормативно-правовую базу и стандарты в области информационной безопасности для построения и поддержания надежной системы защиты информации в организации.

Задачи программы

- Ознакомление с системой законодательства РФ в области информационной безопасности, персональных данных и критической информационной инфраструктуры.
- Изучение национальных и международных стандартов в области ИБ и их роли в управлении рисками.
- Обучение навыкам разработки и внедрения организационно-распорядительной документации по ИБ.
- Формирование умения определять меры ответственности за нарушения в сфере ИБ и выстраивать систему комплаенс.
- Овладение навыками анализа соответствия (аудита) информационной системы требованиям регуляторов.
- Развитие способности интерпретировать правовые и нормативные требования для принятия обоснованных управленческих решений в области защиты информации.

Профессиональная компетенция: По завершении программы участники смогут демонстрировать следующие профессиональные компетенции:

- Осуществлять правовую оценку процессов обработки информации и применять нормы законодательства в практической деятельности.
- Разрабатывать и актуализировать политики, стандарты и процедуры организации в области ИБ.
- Обеспечивать соответствие системы защиты информации требованиям регуляторов (ФСТЭК, Роскомнадзор, ФСБ).
- Проводить анализ рисков и планировать мероприятия по снижению правовых и финансовых последствий нарушений.

5. Категория обучающихся Лица, получающее среднее профессиональное образование и (или) высшее образование;

Лица, имеющие среднее профессиональное образование и (или) высшее образование

6. Сроки реализации, продолжительность образовательного процесса

Программа курсов повышения квалификации рассчитана на 18 учебных часов. Реализуется по графику.

7. Формы и режим занятий

Форма организации занятий очная и (или) с применением дистанционных образовательных технологий; групповая, индивидуально-групповая. Система занятий сориентирована не столько на передачу «готовых знаний», сколько на формирование активной личности, мотивированной к самообразованию, обладающей достаточными навыками и психологическими установками к самостоятельному поиску, отбору, анализу и использованию информации. В основе практической работы лежит выполнение различных заданий, способствующих отработке умений и навыков по использованию специализированного программного обеспечения для ведения бухгалтерского учета

8. Планируемые образовательные результаты

В результате обучения по программе обучающийся должен

знать:

Законодательные акты и нормативные документы, определяющие порядок защиты информации, персональных данных и функционирования КИИ.

Ключевые национальные и международные стандарты в области ИБ (ISO/IEC 27001, ГОСТ Р серии 57580, ГОСТ Р 56545 и др.).

Принципы построения системы управления информационной безопасностью (СУИБ).

Порядок привлечения к ответственности за нарушения в сфере ИБ.

Методологию анализа и интерпретации требований регуляторов для конкретной организации.

уметь:

Ориентироваться в актуальной нормативно-правовой базе и применять ее положения к практическим ситуациям.

Разрабатывать проекты локальных нормативных актов (политики, регламенты, инструкции) по ИБ.

Оценивать соответствие объектов информатизации требованиям по защите информации.

Взаимодействовать с контролирующими органами и готовить необходимую отчетность.

Реализовывать меры профилактики и предупреждения нарушений законодательства в области ИБ.

9.Формы подведения итогов реализации программы

Формой подведения итогов реализации программы является выполнение кейса (анализ конкретной ситуации) или защита разработанного проекта локального нормативного акта (например, «Политики информационной безопасности» или «Плана реагирования на инциденты»).

10. Способы определения результативности

Освоение дополнительной профессиональной программы повышения квалификации завершается итоговой аттестацией в форме выполнения кейса, в процессе которого оценивается выполнение практических заданий, где обучающиеся должны продемонстрировать свои навыки по применению нормативно-правовой базы и стандартов для решения прикладных задач в области информационной безопасности.

Критерии оценивания индивидуальных проектных заданий
5 баллов - Полное освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой; самостоятельность и правильность выполнения задания путем выбора инструментальных средств (нормативных актов, методик) для решения поставленной задачи и аргументации своей позиции; умение выполнять задания с привнесением собственного видения проблемы.
4 балла - Освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой; уровень выполнения задания отвечает всем основным критериям, но некоторые практические навыки работы с освоенным материалом сформированы недостаточно, имеются отдельные неточности или негрубые ошибки.
3 балла - Частичное освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой; сформированность не в полной мере новых компетенций и профессиональных умений для осуществления профессиональной деятельности; уровень выполнения задания отвечает большинству требований, однако некоторые практические навыки не сформированы, много неточностей, имеются негрубые ошибки.

Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Содержание программы

Тема 1. Правовое регулирование отношений в сфере информационной безопасности в РФ
Система законодательства РФ в области информации, информационных технологий и защиты информации. Конституционные гарантии. Федеральные законы: «Об информации, информационных технологиях и о защите информации» (149-ФЗ), «О персональных данных» (152-ФЗ), «О безопасности критической информационной инфраструктуры» (187-ФЗ). Иерархия нормативных правовых актов. Полномочия регуляторов (ФСТЭК, ФСБ, Роскомнадзор, Банк России).
Практическое занятие: Анализ сферы действия законов применительно к деятельности организации.

Тема 2. Организационно-распорядительная документация по обеспечению ИБ: разработка и внедрение
Состав и структура локальных актов в области ИБ. Политика информационной безопасности. Частные политики (управление доступом, безопасность персонала, физическая защита). Регламенты реагирования на инциденты. Роль приказов и распоряжений руководителя.
Практическое занятие: Разработка структуры Политики информационной безопасности для типовой организации.

Тема 3. Стандартизация в области ИБ: обзор национальных и международных стандартов

Роль стандартов в управлении ИБ. Семейство стандартов ISO/IEC 27000. Обзор ГОСТ Р ИСО/МЭК 27001 (требования к СУИБ) и ГОСТ Р ИСО/МЭК 27002 (практические правила). Отраслевые стандарты (например, ГОСТ Р 57580.1 для банковской системы, стандарты для государственных информационных систем). Практическое занятие: Оценка соответствия процессов организации требованиям ГОСТ Р ИСО/МЭК 27001.

Тема 4. Категорирование объектов критической информационной инфраструктуры (КИИ) и правовые аспекты их защиты
Понятие КИИ. Приказ ФСТЭК № 239 «Об утверждении Порядка ведения реестра значимых объектов КИИ». Критерии категорирования. Обязанности субъектов КИИ: организационные и технические меры защиты. Ответственность за нарушение требований 187-ФЗ. Практическое занятие: Решение кейса по определению категории значимости для заданного объекта КИИ.

Тема 5. Защита персональных данных: правовые основы, обязанности оператора, ответственность
Правовой режим обработки персональных данных. Принципы обработки. Согласие на обработку ПДн. Оценка вреда. Обязанности оператора: уведомление Роскомнадзора, принятие мер по защите ПДн. Приказы ФСТЭК и ФСБ для государственных и негосударственных информационных систем. Ответственность (административная, уголовная). Практическое занятие: Составление перечня документов оператора ПДн.

Тема 6. Лицензирование деятельности по защите государственной тайны и технической защите информации
Виды деятельности, подлежащие лицензированию в сфере ИБ. Лицензирование деятельности по технической защите информации (ТЗКИ) и по разработке средств защиты информации. Требования к соискателю лицензии. Государственная тайна: правовое регулирование, допуск, режим секретности. Практическое занятие: Анализ условий получения лицензии на ТЗКИ.

Тема 7. Обеспечение безопасности значимых объектов критической информационной инфраструктуры
Меры по обеспечению безопасности значимых объектов КИИ. Формирование и ведение реестра угроз безопасности информации. Применение сертифицированных средств защиты информации. Реагирование на компьютерные атаки. Взаимодействие с ГосСОПКА. Практическое занятие: Разработка плана мероприятий по обеспечению безопасности значимого объекта КИИ.

Тема 8. Организация и проведение внутреннего контроля соблюдения требований по ИБ (комплаенс)
Понятие комплаенс в ИБ. Организация внутреннего контроля (аудита). Проверка выполнения требований 152-ФЗ, 187-ФЗ, стандартов. Оценка эффективности принятых мер защиты. Документирование результатов контроля. Практическое занятие: Составление чек-листа для проведения внутренней проверки соблюдения требований законодательства.

Тема 9. Ответственность за нарушения в сфере информационной безопасности: административная, гражданско-правовая, уголовная
Обзор составов правонарушений в КоАП РФ (ст. 13.11, 13.12, 13.13, 19.7). Уголовная ответственность за неправомерный доступ (ст. 272 УК РФ), создание и распространение вредоносных программ (ст. 273 УК РФ). Гражданско-правовая ответственность: возмещение убытков и компенсация морального вреда. Анализ судебной практики. Практическое занятие: Разбор реальных судебных дел о нарушениях в сфере ИБ.

Список использованных источников

1. Бачило И.Л. Информационное право: учебник для вузов / И.Л. Бачило. — 6-е изд., перераб. и доп. — М. : Юрайт, 2024. — 419 с. — ISBN 978-5-534-16242-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536837

2. Полякова, Т.А. Информационная безопасность: правовые основы : учебник для СПО / Т.А. Полякова, А.А. Стрельцов. — 3-е изд., перераб. и доп. — М. : Юрайт, 2024. — 312 с. — ISBN 978-5-534-16839-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/54308

3. Кутузов, Е.В. Правовое обеспечение информационной безопасности : учебное пособие / Е.В. Кутузов. — М. : ИНФРА-М, 2023. — 218 с. — (Среднее профессиональное образование). — ISBN 978-5-16-016112-5. — Текст : электронный // Znanium [сайт]. — URL: https://znanium.com/catalog/product/1921176

4. Дорофеев, А.Ю. Стандарты информационной безопасности: ISO/IEC 27000 : учебно-практическое пособие / А.Ю. Дорофеев, И.А. Никитин. — М. : КноРус, 2023. — 284 с. — ISBN 978-5-406-11052-6. — Текст : электронный // Book.ru [сайт]. — URL: https://www.book.ru/book/943736

5. Рожнов, А.А. Организационно-правовое обеспечение информационной безопасности : учебник для СПО / А.А. Рожнов, А.В. Филиппов. — М. : Академия, 2023. — 336 с. — ISBN 978-5-4468-9542-7.

6. Терехов, А.М. Защита информации: правовые аспекты : учебное пособие / А.М. Терехов. — СПб. : Лань, 2023. — 208 с. — ISBN 978-5-8114-4251-3. — Текст : электронный // Лань : электронно-библиотечная система [сайт]. — URL: https://e.lanbook.com/book/254687

7. Чернов, А.А. Управление информационной безопасностью: стандарты и практики : учебник / А.А. Чернов, В.И. Ярочкин. — Москва : РИОР : ИНФРА-М, 2024. — 248 с. — ISBN 978-5-369-01982-3. — Текст : электронный // Znanium [сайт]. — URL: https://znanium.com/catalog/product/2051345

8. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ). — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

9. Трудовой кодекс Российской Федерации : Федеральный закон от 30.12.2001 №197-ФЗ (ред. от 25.02.2025). — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

10. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30.12.2001 № 195-ФЗ (ред. от 26.12.2024). — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

11. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 24.02.2025). — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

12. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024). — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

13. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 26.02.2024). — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

14. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 08.08.2024). — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

15. Об утверждении Требований к защите информации, не составляющей государственную тайну : Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 05.10.2023). — Текст : элек-

тронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

16. Об утверждении Порядка определения угроз безопасности информации : Приказ ФСТЭК России от 05.02.2021 № 29. — Текст : электронный // СПС «КонсультантПлюс». — URL: http://www.consultant.ru

17. ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования : утвержден и введен в действие Приказом Росстандарта от 30.09.2021 № 1085-ст. — Текст : электронный // Электронный фонд правовых и нормативно-технических документов. — URL: https://docs.cntd.ru

Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Бузулукский филиал Финуниверситета

АННОТАЦИЯ

дополнительной профессиональной программы – курса повышения квалификации «Основы информационной безопасности: правовые аспекты и стандарты»

Цель программы: Формирование системных знаний и практических навыков в области обеспечения информационной безопасности (ИБ) на основе требований законодательства Российской Федерации, нормативно-методических документов и профессиональных стандартов, необходимых для защиты информации в организации.

Категория слушателей: Лица, получающее среднее профессиональное образование и (или) высшее образование;

Лица, имеющие среднее профессиональное образование и (или) высшее образование

Форма обучения: Очная с применением дистанционных образовательных технологий

Профессиональная компетенция: Участник научится самостоятельно применять нормы законодательства в области информационной безопасности, разрабатывать и внедрять организационно-распорядительную документацию, обеспечивать соответствие системы защиты информации требованиям регуляторов, а также использовать профессиональные стандарты для построения эффективной системы управления информационной безопасностью в организации С целью овладения профессиональной компетенцией слушатель в ходе освоения программы должен **уметь**:

Ориентироваться в актуальной нормативно-правовой базе и применять ее положения к практическим ситуациям.

Разрабатывать проекты локальных нормативных актов (политики, регламенты, инструкции) по ИБ.

Оценивать соответствие объектов информатизации требованиям по защите информации.

Взаимодействовать с контролирующими органами и готовить необходимую отчетность.

Реализовывать меры профилактики и предупреждения нарушений законодательства в области ИБ..

знать:

Законодательные акты и нормативные документы, определяющие порядок защиты информации, персональных данных и функционирования КИИ.

Ключевые национальные и международные стандарты в области ИБ (ISO/IEC 27001, ГОСТ Р серии 57580, ГОСТ Р 56545 и др.).

Принципы построения системы управления информационной безопасностью (СУИБ).

Порядок привлечения к ответственности за нарушения в сфере ИБ.

Методологию анализа и интерпретации требований регуляторов для конкретной организации.

Формой подведения итогов реализации программы является выполнение кейса (анализ конкретной ситуации)

Выдаваемый документ: удостоверение

Директор Н.Н. Щавелева

Ответственный за ДПО Е.С. Петрянкина