ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 021B3B8C0001B3D19C40DE3E56DAF1244C
Владелец: ПОДОБРЕЕВ АНТОН ЕВГЕНЬЕВИЧ
Действителен: с 19.06.2025 до 19.09.2026

УТВЕРЖДАЮ
Директор
ООО Институт «Центрика»
А.Е.Подобреев
«01» сентября 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Защита информации и персональных данных»
(72 ч.)

г. Краснодар
2025 г.

РАЗДЕЛ 1. Аннотация дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

Дополнительная профессиональная программа повышения квалификации «Защита информации и персональных данных» (далее – программа) разработана в соответствии с требованиями следующих нормативных документов:

- Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства науки и высшего образования Российской Федерации от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Приказ Минтруда России от 14.09.2022 г. № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»;
- Приказ Министерства науки и высшего образования Российской Федерации от 17.11.2020 г. № 1427 «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность».

Планируемые результаты обучения: результатами обучения по программе «Защита информации и персональных данных» является повышение уровня профессиональных компетенций за счет освоения и (или) углубления знаний и умений в области защиты информации и персональных данных.

Слушателями являются лица, имеющие или получающие среднее профессиональное и (или) высшее образование.

Содержание программы представлено аннотацией, учебным планом, календарным графиком, содержанием учебных предметов, условиями реализации программы, системой оценки результатов освоения программы, контрольно-оценочными материалами.

Форма обучения: очно-заочная с применением дистанционных образовательных технологий.

Язык обучения: русский.

Освоение программы завершается обязательной итоговой аттестацией – итоговым экзаменом в форме тестирования в дистанционном образовательном модуле ООО Институт «Центрика».

Производственное обучение и производственная практика осуществляется по месту работы слушателей.

Слушателям, успешно окончившим курс обучения, выдаются документы, действительные на всей территории Российской Федерации:

– Удостоверение о повышении квалификации (форма итогового документа определяется ООО Институт «Центрика», заверяется печатью).

РАЗДЕЛ 2. Профессиональные компетенции и трудовые функции дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

В результате обучения слушатели приобретают знания, навыки и практические умения, необходимые для качественного совершенствования профессиональных компетенций.

Программа должна устанавливать следующие общепрофессиональные компетенции:

- ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;
- ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
- ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности;
- ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;
- ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
- ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
- ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;
- ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
- ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

- 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-11. Способен проводить эксперименты по заданной методике и обработку их результатов;
- ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
- ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.

Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности):

Обобщенные трудовые функции			Трудовые функции		
код	Наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Обслуживание систем защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	5	Проведение технического обслуживания систем защиты информации автоматизированных систем	A/01.5	5
			Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	A/02.5	5
			Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем	A/03.5	5

B	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категории значимости, в процессе их эксплуатации	6	Диагностика систем защиты информации автоматизированных систем	B/01.6	6
			Администрирование систем защиты информации автоматизированных систем	B/02.6	6
			Управление защитой информации в автоматизированных системах	B/03.6	6
			Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	B/04.6	6
			Мониторинг защищенности информации в автоматизированных системах	B/05.6	6
			Аудит защищенности информации в автоматизированных системах	B/06.6	6
			Установка и настройка средств защиты информации в автоматизированных системах	B/07.6	6
			Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	B/08.6	6
			Анализ уязвимостей внедряемой системы защиты информации	B/09.6	6
			Внедрение организационных мер по защите информации в автоматизированных системах	B/10.6	6
C	Разработка систем защиты информации	7	Тестирование систем защиты информации	C/01.7	7

	автоматизированных		автоматизированных систем		
	систем, используемых в том числе на объектах критической		Разработка проектных решений по защите информации в автоматизированных системах	C/02.7	7
	информационной инфраструктуры, в отношении которых отсутствует		Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	C/03.7	7
	необходимость присвоения им категорий значимости		Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	C/04.7	7
D	Формирование требований к защите информации в	7	Обоснование необходимости защиты информации в автоматизированной системе	D/01.7	7
	автоматизированных системах, используемых в том числе на объектах		Определение угроз безопасности информации, обрабатываемой автоматизированной системой	D/02.7	7
	критической информационной инфраструктуры, в		Разработка архитектуры системы защиты информации автоматизированной системы	D/03.7	7
	отношении которых отсутствует необходимость присвоения им категорий значимости		Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации	D/04.7	7

РАЗДЕЛ 3. Учебный план дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

№ п/п	Наименование дисциплин	Всего часов	В том числе		Форма контроля
			Лекции	Практические занятия	
1	Нормативно-правовое обеспечение в области защиты информации и персональных данных	**10**	10	-	
2	Обязанности оператора персональных данных	**12**	10	2	
3	Угрозы в области информационной безопасности	**12**	10	2	
4	Система защиты персональных данных	**12**	10	2	
5	Лицензирование и сертификация	**12**	10	2	
6	Ответственность за нарушение требований законодательства в области защиты информации и персональных данных	**12**	10	2	
7	Итоговая аттестация	**2**	2	-	Экзамен
	Всего:	**72**	**62**	**10**	

РАЗДЕЛ 4. Календарный график дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

№	**Наименование тем / модулей**	**Часов по плану**	**Учебные дни**																																							
			1	2	3	4	5	6	7	8	9																															
1	Нормативно-правовое обеспечение в области защиты информации и персональных данных	**10**	8	2																																						
2	Обязанности оператора персональных данных	**12**		6	6																																					
3	Угрозы в области информационной безопасности	**12**			2	8	2																																			
4	Система защиты персональных данных	**12**					6	6																																		
5	Лицензирование и сертификация	**12**						2	8	2																																
6	Ответственность за нарушение требований законодательства в области защиты информации и персональных данных	**12**								6	6																															
7	Итоговая аттестация	**2**									2																															
	Всего:	**72**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**																															

РАЗДЕЛ 5. Содержание дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

№ п/п	Наименование темы / модуля	Всего часов	Содержание темы / модуля
1	Нормативно-правовое обеспечение в области защиты информации и персональных данных	**10**	Нормативно-правовая основа концепции ИБ. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности.
2	Обязанности оператора персональных данных	**12**	Обязанности оператора при сборе персональных данных. Меры по обеспечению безопасности персональных данных при их обработке. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных.
3	Угрозы в области информационной безопасности	**12**	Понятие угрозы. Виды противников или «нарушителей». Окно опасности. Классификация видов угроз ИБ по различным признакам. Угрозы доступности, целостности и конфиденциальности. Характер происхождения угроз: умышленные факторы, естественные факторы. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации.
4	Система защиты персональных данных	**12**	Основные этапы обработки и защиты персональных данных. Анализ объекта информатизации. Составление модели угроз. Техническое задание на систему защиты ПДн. Стадия проектирования. Требования методических документов. Стадия ввода в действие и эксплуатации СЗПДн. Особенности защиты персональных данных при их обработке в государственных информационных системах. Контроль в области защиты персональных данных.
5	Лицензирование и сертификация	**12**	Нормы и требования российского законодательства в области лицензирования и сертификации. Порядок оформления и получения лицензий и сертификатов в области ИБ.
6	Ответственность за нарушение требований законодательства в области защиты информации и персональных данных	**12**	Ответственность за нарушения защиты персональных данных. Уголовная ответственность за разглашение персональных данных. Административная ответственность в

			сфере защиты персональных данных. Иные виды ответственности в сфере защиты персональных данных. Возмещение ущерба, причиненного незаконным использованием персональных данных. Компенсация морального вреда.
7	Итоговая аттестация	**2**	См. раздел 9

Перечень выполняемых практических работ:

№ п/п	Наименование практических работ
1	Шифр простой замены. Пример создания программного кода, зашифровывающего и расшифровывающего сообщение по алгоритму шифра простой замены
2	Создание пользовательской формы – Шифратор Цезаря
3	Системы с закрытым ключом. Шифрование методом подстановки
4	Системы с закрытым ключом. Шифр многоалфавитной замены
5	Системы с закрытым ключом. Шифрование методом перестановки
6	Создание пользовательской формы – Шифратор файлов
7	Создание пользовательской формы – Вычисление хеш-функции
8	Вычисление хеш-функции по заданному варианту
9	Создание пользовательской формы, реализующей алгоритм шифра RSA
10	Симметричные криптосистемы

Слушатели проходят производственное обучение по месту трудоустройства и выполняют практические работы в соответствии с видом профессиональной деятельности.

РАЗДЕЛ 6. Условия реализации дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

6.1. Учебно-методическое обеспечение

1. Перечень актуальных нормативных документов.
2. Лекционные материалы.
3. Практические задания.
4. Видеоматериалы.

6.2. Требования к минимальному материально-техническому обеспечению

Реализация программы требует наличия учебного кабинета, оборудованного:

- посадочными местами по количеству слушателей;
- рабочим местом преподавателя;
- компьютером с доступом в сеть «Интернет»;
- нормативными документами;
- методической литературой;
- учебно-наглядными пособиями по программе;
- комплектом инструментов и приспособлений;
- стендами.

6.3. Кадровое обеспечение

Педагогические кадры должны иметь среднее профессиональное или высшее профессиональное образование, соответствующее профилю преподаваемой дисциплины и (или) опыт практической деятельности в соответствующей сфере.

РАЗДЕЛ 7. Информационное обеспечение дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

1. Закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2. Закон от 27.07.2006 № 152-ФЗ «О персональных данных»
3. Закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»
4. Закон от 07.07.2003 № 126-ФЗ «О связи»
5. Указ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак»
6. Указ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации»
7. Указ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
8. Указ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
9. Указание от 30.08.2023 № 6515-У «Об определении угроз безопасности при обработке персональных данных»
10. Указание от 10.12.2015 № 3889-У «Об определении угроз безопасности персональных данных»
11. Приказ от 14.09.2022 № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»
12. Приказ от 29.09.2020 № 680н «Об утверждении профессионального стандарта «Системный администратор»
13. Приказ от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер»

РАЗДЕЛ 8. Критерии оценки знаний и умений дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

Программой предусмотрено тестирование в образовательном дистанционном модуле ООО Институт «Центрика» в форме итоговой аттестации после изучения всех модулей программы.

Критерии оценки выполнения заданий в тестовой форме:

«5» (отлично) – 91-100% правильных ответов;

«4» (хорошо) – 81-90% правильных ответов;

«3» (удовлетворительно) – 71-80% правильных ответов;

«2» (неудовлетворительно) – 70% и менее правильных ответов.

Для реализации программы учебным планом предусмотрено создание контрольно-оценочных материалов, которые включают вопросы для проведения итоговой аттестации, позволяющие оценивать уровень образовательных достижений и степень сформированности компетенций.

РАЗДЕЛ 9. Контрольно-оценочные материалы дополнительной профессиональной программы повышения квалификации «Защита информации и персональных данных»

1. Автоматизированная обработка персональных данных – это:

A. Обработка персональных данных с использованием средств автоматизации

B. Обработка персональных данных с помощью средств вычислительной техники

C. Обработка персональных данных пользователя с применением компьютера

2. Информация – это:

A. Любые данные, представленные на материальном носителе

B. Сведения, принадлежащие кому-либо и защищаемые законом

C. Сведения (сообщения, данные), независимо от формы их представления

3. Информационная система персональных данных – это:

A. Пользователь, средства автоматизации, базы данных

B. Контролируемое пространство, в котором происходит обработка персональных данных

C. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

4. Безопасность персональных данных – это:

A. Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных

B. Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность персональных данных

C. Состояние защищенности персональных данных, характеризуемое способностью технических средств обеспечить конфиденциальность персональных данных

5. Блокирование персональных данных – это:

A. Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)

B. Временное прекращение обработки персональных данных

C. Временное прекращение обработки персональных данных для уточнения персональных данных

6. Доступ к информации – это:

A. Возможность получения информации и ее использования

B. Возможность использования информации

C. Возможность доступа к информации

D. Возможность доступа к информации, но не ее использования

7. Целью Федерального закона от 27.07.2006 № 152-ФЗ является:

A. Контроль за обработкой персональных данных операторами персональных данных

B. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных

C. Соответствия законодательства РФ в сфере персональных данных Конвенции Совета Европы от 1981 года

8. Защищаемая информация – это:

A. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

B. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации

C. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов

D. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации»

9. Что понимается под понятием «Конфиденциальность персональных данных»?

A. Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных

B. Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом

C. Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных или наличия иного законного основания

10. Оператор при сборе персональных данных через свой официальный сайт обязан в соответствии с ч.2 ст.18.1 152-ФЗ на сайте опубликовать документы:

A. Политику в отношении обработки персональных данных

B. Политику в отношении обработки персональных данных + Пользовательское соглашение

C. Политику в отношении обработки персональных данных + Пользовательское соглашение + Согласие пользователя

11. Общедоступные персональные данные – это:

A. Персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта персональных данных

B. Персональные данные, доступ неограниченного круга лиц, к которым предоставлен в соответствии с федеральными законами

C. Персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности

12. Специальные категории персональных данных – это:

A. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни

B. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни

C. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни

D. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости

13. Трансграничная передача персональных данных – это:

A. Передача персональных данных на территорию иностранного государства

B. Передача персональных данных на территорию другого субъекта РФ органу власти данного субъекта, физическому лицу или юридическому лицу данного субъекта РФ

C. Передача персональных данных на территорию иностранного государства или органу власти иностранного государства

D. Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

14. Целостность информации – это:

A. Состояние информации, при котором отсутствует любое ее изменение

B. Состояние информации, при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право

C. Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

15. Что такое персональные данные?

A. Любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных)

B. Информация о частной жизни физического лица, доступ к которой он решил ограничить

C. Сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных

D. Любые сведения независимо от формы их представления

16. Оператор персональных данных - это:

A. Государственный орган, осуществляющий автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке

B. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели

обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

C. Юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке

D. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, но не определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

17. Обработка персональных данных - это:

A. Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных)

B. Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые с помощью средств вычислительной техники

C. Чтение, запись, сортировка, модификация, передача персональных данных в информационной системе

18. Распространение персональных данных - это:

A. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц

B. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

C. Передача персональных данных оператору персональных данных

19. Предоставление персональных данных - это:

A. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

B. Действия, направленные на раскрытие персональных данных по мотивированному запросу

20. Уничтожение персональных данных - это:

A. Действия, в результате которых становится невозможно определить субъекта персональных данных в информационной системе персональных данных

B. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

C. Удаление персональных данных из информационной системы персональных данных

D. Действия, направленные на уничтожение носителей персональных данных