

УТВЕРЖДЕНА

приказом ООО «Эдуклайн»

от «

Генеральный директор

2026 г. №

0309-17

/ Волкова А. Л. /

Разработчик программы Волков Иван Сергеевич, преподаватель.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА – ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Обеспечение защиты информации в автоматизированных системах»

Организация, осуществляющая обучение: Общество с ограниченной ответственностью «Эдуклайн»

Вид образования: дополнительное профессиональное образование

Вид программы: программа повышения квалификации

Объём: 72 академических часа

Форма обучения: заочная, исключительно с применением электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ)

Документ по итогам: удостоверение о повышении квалификации

дер. Касимово, Ленинградская область – 2026

СОДЕРЖАНИЕ

- I. Общие положения
- II. Планируемые результаты освоения программы
- III. Организационно-педагогические условия реализации программы
- IV. Учебный план и календарный учебный график
- V. Содержание программы (рабочие программы модулей)
- VI. Формы аттестации и оценочные материалы (фонд оценочных средств)
- VII. Порядок работы с обучающимися по результатам аттестации
- Приложение 1. Глоссарий основных терминов
- Приложение 2. Перечень нормативных правовых актов и методических документов
- Приложение 3. Перечень учебных изданий и информационных ресурсов
- Приложение 4. Форма протокола итоговой аттестации
- Приложение 5. Форма ведомости промежуточной аттестации

I. Общие положения

1. Настоящая дополнительная профессиональная программа – программа повышения квалификации «Обеспечение защиты информации в автоматизированных системах» (далее – программа) определяет содержание и организацию образовательной деятельности при повышении квалификации специалистов, обеспечивающих защиту информации в автоматизированных системах, в Обществе с ограниченной ответственностью «Эдуклайн» (далее – Организация).

2. Программа разработана в соответствии с требованиями: - Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (в том числе статей 2, 12, 13, 16, 17, 58, 60, 74, 76); - Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утверждённого приказом Минобрнауки России от 24.03.2025 № 266; - профессионального стандарта «Специалист по защите информации в автоматизированных системах» (код 06.033), утверждённого приказом Минтруда России от 14.09.2022 № 525н; - локальных нормативных актов Организации (о применении ЭО и ДОТ; об электронной информационно-образовательной среде; о текущем контроле и аттестации; об идентификации личности обучающихся).

Порядок применения электронного обучения и дистанционных образовательных технологий определяется локальным нормативным актом Организации на основании статьи 16 Федерального закона № 273-ФЗ.

3. Целью программы является совершенствование профессиональных компетенций обучающихся в рамках имеющейся квалификации, необходимых для обеспечения защиты информации (в том числе персональных данных) в автоматизированных системах.

4. Задачи программы: - актуализировать знания нормативно-правовой и методической базы защиты информации в автоматизированных системах; - сформировать умение выявлять и оценивать угрозы безопасности информации, разрабатывать модель угроз и модель нарушителя; - совершенствовать навыки применения организационных и технических мер и средств защиты информации; - систематизировать знания в области защиты персональных данных при их обработке в автоматизированных системах; - отработать порядок мониторинга событий и реагирования на инциденты информационной безопасности.

5. Программа построена на модульном принципе представления содержания и построения учебного плана, что позволяет обеспечить необходимую последовательность освоения материала и учёт уровня подготовки обучающихся. Программа реализуется как единый комплекс основных характеристик образования (объём, содержание, планируемые результаты) и организационно-педагогических условий, представленный в виде учебного плана, календарного учебного графика, рабочих программ модулей, оценочных и методических материалов (пункт 9 статьи 2 Федерального закона № 273-ФЗ).

6. К освоению программы допускаются лица, имеющие или получающие среднее профессиональное и (или) высшее образование (часть 3 статьи 76 Федерального закона № 273-ФЗ). Категория слушателей: работники, профессиональная деятельность которых связана с обеспечением защиты информации в автоматизированных системах. Обучающиеся, имеющие среднее профессиональное образование, совершенствуют компетенции в рамках обобщённой трудовой функции А (уровень квалификации 5) профессионального стандарта 06.033; имеющие высшее образование – в рамках обобщённой трудовой функции В (уровень квалификации 6).

7. Срок освоения программы – 72 академических часа. Обучение проводится в течение всего календарного года по мере комплектования учебных групп; конкретные сроки начала и окончания обучения устанавливаются приказом о зачислении. Для всех видов учебных занятий академический час устанавливается продолжительностью 45 минут. Продолжительность учебной недели и учебного дня определяется расписанием занятий в пределах срока освоения программы.

8. Форма обучения – заочная. Программа реализуется **исключительно с применением электронного обучения и дистанционных образовательных технологий** в электронной информационно-образовательной среде (далее – ЭИОС) Организации, независимо от места нахождения обучающегося.

9. Ограничения предмета программы. Программа носит общий организационно-технический характер, **не содержит сведений, составляющих государственную тайну, не предусматривает работу с реальными средствами криптографической защиты информации и не требует наличия лицензий ФСБ России или ФСТЭК России**. Криптографические методы рассматриваются в обзорном порядке.

II. Планируемые результаты освоения программы

10. В результате освоения программы у обучающегося **качественно изменяются (совершенствуются)** профессиональные компетенции в рамках имеющейся квалификации (в соответствии с частями 4, 9, 10 статьи 76 Федерального закона № 273-ФЗ и Порядком № 266), соотнесённые с трудовыми функциями обобщённых трудовых функций А (уровень квалификации 5) и В (уровень квалификации 6) профессионального стандарта 06.033:

Код	Совершенствуемая компетенция	Качественное изменение (что улучшается)	ОТФ 06.033
ПК-1	Применение НПА и организационно-распорядительных документов по защите информации в АС	Актуализация знаний действующих требований ФСТЭК/ФСБ России; уверенное применение	А, В
ПК-2	Выявление и оценка угроз, разработка модели угроз и нарушителя	Освоение методик БДУ ФСТЭК России; повышение точности оценки рисков	А
ПК-3	Применение организационных и технических мер и средств защиты в АС	Расширение арсенала мер; корректная настройка средств защиты	А, В
ПК-4	Обеспечение защиты персональных данных в АС	Приведение обработки ПДн в соответствие с ФЗ-152 и подзаконными актами	А, В
ПК-5	Мониторинг событий и реагирование на инциденты ИБ	Формирование навыка своевременного реагирования	В

11. Обобщённые планируемые результаты. В результате освоения программы обучающийся должен:

знать: нормативно-правовую и методическую базу защиты информации в автоматизированных системах, систему и полномочия регуляторов (ФСТЭК России, ФСБ России, Роскомнадзор); классификацию угроз безопасности информации, порядок построения модели угроз и модели нарушителя; состав организационных и технических мер защиты информации и типовые средства защиты; требования к обработке и защите персональных данных, уровни защищённости информационных систем персональных данных; порядок мониторинга событий и реагирования на инциденты информационной безопасности;

уметь: применять требования нормативных правовых актов к защите информации в автоматизированных системах; выявлять и оценивать угрозы безопасности информации, разрабатывать модель угроз для конкретной автоматизированной системы; подбирать и настраивать организационные и технические меры и средства защиты информации; разрабатывать организационно-распорядительную документацию по информационной безопасности и защите персональных данных;

владеть: навыками анализа защищённости автоматизированных систем, подготовки документов по защите информации, реагирования на инциденты информационной безопасности.

12. Планируемые результаты по модулям:

Модуль	По итогам освоения модуля обучающийся
Модуль 1	знает понятийный аппарат, виды защищаемой информации, НПА и систему регуляторов, требования приказов ФСТЭК № 17 и № 21; умеет определять состав защищаемой информации и применимые требования
Модуль 2	знает классификацию угроз и уязвимостей, порядок построения модели угроз и нарушителя, БДУ ФСТЭК; умеет разрабатывать модель угроз и определять актуальные угрозы
Модуль 3	знает состав организационных и технических мер, типовые средства защиты; умеет подбирать и настраивать меры и средства защиты

Модуль	По итогам освоения модуля обучающийся
Модуль 4	знает правовые основы обработки ПДн, уровни защищённости ИСПДн, состав мер по приказу ФСТЭК № 21; умеет определять уровень защищённости и готовить ОРД
Модуль 5	владеет навыками комплексной разработки модели угроз, подготовки ОРД и реагирования на инцидент ИБ

III. Организационно-педагогические условия реализации программы

13. Реализация программы должна обеспечить достижение обучающимися планируемых результатов освоения программы (раздел II). Обучение проводится с полным отрывом, частичным отрывом или без отрыва от работы – в асинхронном режиме в ЭИОС.

14. Выбор методов обучения для каждой темы определяется преподавателем с учётом состава и уровня подготовленности обучающихся, сложности изучаемого материала. Применяются: изучение электронных конспектов и нормативных документов, просмотр видеолекций, выполнение практических заданий на виртуальных стендах, тестирование, консультирование (вебинары, обмен сообщениями в ЭИОС).

15. Теоретические занятия проводятся в форме самостоятельного изучения электронных учебных материалов и видеолекций. Практические занятия проводятся с целью закрепления теоретических знаний и выработки умений и навыков на виртуальных стендах ЭИОС, максимально приближённых к реальным условиям профессиональной деятельности.

16. Кадровое обеспечение. Реализацию программы обеспечивают педагогические работники, соответствующие требованиям статьи 46 Федерального закона № 273-ФЗ и квалификационным характеристикам должности «преподаватель» (Единый квалификационный справочник, утв. приказом Минздравсоцразвития России от 26.08.2010 № 761н; номенклатура должностей – постановление Правительства РФ от 21.02.2022 № 225). К преподаванию привлекаются лица, имеющие высшее образование и (или) профессиональную переподготовку в области информационной безопасности либо информационных технологий, систематически повышающие свой профессиональный уровень.

17. Материально-техническое обеспечение и ЭИОС. Программа реализуется в электронной информационно-образовательной среде Организации – образовательном приложении «Эдуклайн» (личный кабинет обучающегося). ЭИОС обеспечивает: доступ к электронным учебным материалам, видеолекциям, тренажёрам, виртуальным стендам и тестам; синхронное и асинхронное взаимодействие обучающихся и преподавателей; фиксацию и контроль в автоматическом режиме хода и результатов обучения; хранение результатов на электронных носителях. Доступ к ЭИОС предоставляется круглосуточно на весь период обучения независимо от места нахождения обучающегося. Требования к оборудованию обучающегося: персональный компьютер (ноутбук) с доступом к сети «Интернет».

18. Идентификация личности обучающегося. Идентификация обеспечивается индивидуальной учётной записью (логин/пароль либо вход через мессенджер по одноразовому коду). При прохождении итоговой аттестации личность обучающегося дополнительно подтверждается сверкой документа, удостоверяющего личность, в режиме видео-конференц-связи. Порядок идентификации установлен локальным нормативным актом Организации.

19. Учебно-методическое и информационное обеспечение. При реализации программы используются учебные, учебно-методические, справочные и иные печатные и электронные издания (Приложение 3), а также актуальные нормативные правовые акты и методические документы ФСТЭК России и ФСБ России (Приложение 2). Все материалы размещаются в ЭИОС и доступны обучающимся на весь период обучения.

20. Оценочные материалы программы – блоки контрольных (тестовых) вопросов и практических заданий по разделам (модулям), формируемые Организацией и используемые при проведении промежуточной и итоговой аттестации (раздел VI настоящей программы). Оценочные материалы размещаются и хранятся в ЭИОС.

21. Методические материалы – электронные конспекты, презентации, видеолекции, нормативные документы, методические указания по выполнению практических заданий, инструкции по работе с виртуальными стендами. Размещаются в ЭИОС и доступны обучающимся на весь период обучения. Методические рекомендации по изучению программы: обучение рекомендуется вести последовательно по модулям; к практическим занятиям приступать после освоения соответствующего теоретического материала; при затруднениях использовать консультации преподавателя в ЭИОС.

IV. Учебный план и календарный учебный график

22. Учебный план определяет перечень, последовательность, трудоёмкость разделов (модулей) программы и формы контроля.

№ п/п	Наименование дисциплины (модуля)	Всего часов	теоретические занятия	практические занятия	Формы контроля
1	Правовые и организационные основы защиты информации в АС	12	6	6	зачёт (тестирование)
2	Угрозы безопасности информации, модель угроз и нарушителя, оценка рисков	14	6	8	зачёт (тестирование)
3	Организационные и технические меры и средства защиты в АС; криптография (обзорно)	18	8	10	зачёт (тестирование)
4	Защита персональных данных при обработке в АС, организационно-распорядительная документация	12	5	7	зачёт (тестирование)
5	Практикум на виртуальных стендах ЭИОС	12	–	12	зачёт по практикуму
6	Итоговая аттестация – итоговое тестирование	4	–	4	итоговое тестирование
	ИТОГО	72	25	47	

23. Учебно-тематический план (детализация модулей по темам):

№	Тема	Всего	теория	практика
1.1	Понятийный аппарат защиты информации в АС	2	1	1
1.2	Виды защищаемой информации и правовые режимы	2	1	1
1.3	Нормативно-правовая база защиты информации	2	2	–
1.4	Система регуляторов и их полномочия	2	1	1
1.5	Требования ФСТЭК России; построение системы защиты	2	1	1

N	Тема	Всего	теория	практика
1.6	Практическое занятие по модулю 1	2	–	2
2.1	Угрозы и уязвимости безопасности информации	2	1	1
2.2	Модель нарушителя	2	1	1
2.3	Модель угроз; БДУ ФСТЭК России	3	1	2
2.4	Методика оценки угроз безопасности информации	3	2	1
2.5	Оценка рисков информационной безопасности	2	1	1
2.6	Практическое занятие по модулю 2	2	–	2
3.1	Организационные меры защиты информации	2	1	1
3.2	Средства защиты от несанкционированного доступа	3	1	2
3.3	Межсетевое экранирование, COB, антивирусная защита	3	2	1
3.4	Основы сетевой безопасности	3	1	2
3.5	Криптографические методы (обзорно)	3	2	1
3.6	Выбор, внедрение и эксплуатация средств защиты	2	1	1
3.7	Практическое занятие по модулю 3	2	–	2
4.1	Правовые основы обработки персональных данных	2	1	1
4.2	Обязанности оператора персональных данных	2	1	1
4.3	Обеспечение безопасности ПДн в информационных системах	3	2	1
4.4	Организационно-распорядительная документация по ПДн	3	1	2
4.5	Практическое занятие по модулю 4	2	–	2
5.1–5.4	Практикум на виртуальных стендах ЭИОС	12	–	12
6	Итоговая аттестация	4	–	4

24. Календарный учебный график. Обучение реализуется в течение всего календарного года по мере комплектования учебных групп. Распределение учебной нагрузки – равномерное, в пределах срока освоения; все виды учебной деятельности реализуются в ЭИОС; контрольные точки фиксируются в электронном журнале.

Период (неделя)	Осваиваемые разделы (модули)	Виды учебной деятельности	Контроль
1-я неделя	Модули 1–2	видеолекции, электронные материалы, практические задания, тесты	промежуточная аттестация по модулям 1, 2
2-я неделя	Модули 3–4	видеолекции, практические задания на виртуальных стендах	промежуточная аттестация по модулям 3, 4
3-я неделя	Модуль 5; итоговая аттестация	практикум, итоговое тестирование	зачёт по практикуму; итоговое тестирование

V. Содержание программы (рабочие программы модулей)

25. В настоящем разделе закрепляются рабочие программы разделов (модулей) – темы и содержательный минимум, которые обучающиеся осваивают в рамках теоретической и практической подготовки.

Модуль 1. Правовые и организационные основы защиты информации в АС (12 ч)

Тема 1.1. Понятийный аппарат защиты информации в автоматизированных системах. Понятия «информация», «информационные технологии», «информационная система», «автоматизированная система (АС)», «защита информации», «информационная безопасность», «безопасность информации». Основные свойства безопасности информации: конфиденциальность, целостность, доступность – их содержание и взаимосвязь. Объекты и субъекты защиты информации. Понятия «носитель информации», «обладатель информации», «оператор». Жизненный цикл информации в автоматизированной системе и точки её возможной компрометации.

Тема 1.2. Виды защищаемой информации и правовые режимы. Информация ограниченного доступа и общедоступная информация. Виды тайн: государственная тайна (общие сведения, границы применения программы), коммерческая тайна, служебная тайна, профессиональная тайна, персональные данные. Режим коммерческой тайны: порядок введения, перечень сведений, гриф, обязанности работников. Соотношение видов защищаемой информации и требований к их защите.

Тема 1.3. Нормативно-правовая база защиты информации. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: основные понятия, принципы правового регулирования, обязанности обладателя информации и оператора по защите информации. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: сфера действия, основные понятия. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»: виды электронной подписи, условия признания равнозначности. Подзаконные акты и методические документы в области защиты информации.

Тема 1.4. Система регуляторов и их полномочия. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): полномочия по защите информации некриптографическими методами, лицензирование деятельности по технической защите конфиденциальной информации. Федеральная служба безопасности (ФСБ России): полномочия в области криптографической защиты информации, лицензирование. Роскомнадзор: контроль и надзор в сфере обработки персональных данных. Разграничение компетенции регуляторов.

Тема 1.5. Требования ФСТЭК России и организационные основы построения системы защиты информации. Требования о защите информации, установленные приказом ФСТЭК России от 11.02.2013 № 17 (для государственных информационных систем) и приказом ФСТЭК России от 18.02.2013 № 21 (для информационных систем персональных данных). Классы защищённости и уровни защищённости. Этапы создания системы защиты информации: формирование требований, разработка системы защиты, внедрение, аттестация (оценка соответствия), сопровождение. Распределение ролей и ответственности за защиту информации в организации.

Практическое занятие 1.6. Анализ применимых требований о защите информации для условной автоматизированной системы; определение состава защищаемой информации, категории (класса/уровня) системы и перечня применимых нормативных требований.

Модуль 2. Угрозы безопасности информации, модель угроз и нарушителя, оценка рисков (14 ч)

Тема 2.1. Угрозы и уязвимости безопасности информации. Понятия «угроза безопасности информации», «уязвимость», «источник угрозы», «нарушитель», «способ реализации угрозы». Классификация угроз по источнику (антропогенные, техногенные, стихийные), по способу реализации и по последствиям (нарушение конфиденциальности, целостности, доступности). Типовые уязвимости автоматизированных систем: уязвимости программного обеспечения, конфигурации, организационные уязвимости.

Тема 2.2. Модель нарушителя. Назначение модели нарушителя. Типы нарушителей: внешний и внутренний. Категории и потенциал нарушителя (базовый, базовый повышенный, высокий). Мотивация, цели и

возможности потенциальных нарушителей. Порядок определения актуальных типов нарушителей для конкретной автоматизированной системы.

Тема 2.3. Модель угроз безопасности информации. Банк данных угроз ФСТЭК России. Назначение, структура и содержание модели угроз безопасности информации. Банк данных угроз безопасности информации (БДУ) ФСТЭК России: назначение, состав, реестр угроз и уязвимостей, порядок использования при разработке модели угроз.

Тема 2.4. Методика оценки угроз безопасности информации. Методика оценки угроз безопасности информации, утверждённая ФСТЭК России (2021). Этапы оценки угроз: определение негативных последствий, определение объектов воздействия, определение источников угроз и оценка возможностей нарушителей, оценка способов реализации угроз, определение актуальных угроз. Формирование перечня актуальных угроз.

Тема 2.5. Оценка рисков информационной безопасности. Понятие риска информационной безопасности. Качественная и количественная оценка рисков. Порядок оценки и обработки рисков, выбор мер по снижению рисков.

Практическое занятие 2.6. Разработка проекта модели угроз безопасности информации для условной автоматизированной системы с использованием БДУ ФСТЭК России и Методики оценки угроз (2021): определение нарушителей, актуальных угроз и способов их реализации.

Модуль 3. Организационные и технические меры и средства защиты в АС; криптография (обзорно) (18 ч)

Тема 3.1. Организационные меры защиты информации. Состав организационных мер: разграничение и управление доступом, управление учётными записями и полномочиями, парольная политика, регламентация действий персонала, контроль и учёт носителей информации, реагирование на инциденты. Роль организационных мер в системе защиты. Организационно-распорядительная документация как инструмент реализации организационных мер.

Тема 3.2. Средства защиты информации от несанкционированного доступа. Назначение и функции средств защиты информации от несанкционированного доступа (СЗИ от НСД): идентификация и аутентификация, управление доступом, регистрация событий безопасности, контроль целостности. Порядок выбора и настройки СЗИ от НСД. Требования к сертификации средств защиты.

Тема 3.3. Средства межсетевого экранирования, обнаружения вторжений и антивирусной защиты. Межсетевые экраны: назначение, классы, правила фильтрации. Средства обнаружения (предотвращения) вторжений: принципы работы, сигнатурный и поведенческий анализ. Средства антивирусной защиты: организация антивирусной защиты, обновление баз, реагирование на срабатывания.

Тема 3.4. Основы сетевой безопасности. Модель сетевого взаимодействия, типовые сетевые угрозы (перехват, подмена, отказ в обслуживании). Сегментирование сети, демилитаризованная зона, контроль сетевого доступа, защита периметра, защищённый удалённый доступ.

Тема 3.5. Криптографические методы защиты информации (обзорно). Назначение криптографических методов защиты. Симметричное и асимметричное шифрование (обзорно). Электронная подпись, инфраструктура открытых ключей — общие сведения. Средства криптографической защиты информации (СКЗИ): назначение, требования к применению — в обзорном порядке, без работы с реальными СКЗИ и без изучения сведений ограниченного доступа.

Тема 3.6. Выбор, внедрение и эксплуатация средств защиты. Порядок выбора средств защиты в соответствии с моделью угроз и требованиями регуляторов. Внедрение и настройка средств защиты. Эксплуатация, контроль работоспособности, обновление, вывод из эксплуатации.

Практическое занятие 3.7. Настройка организационных и технических мер защиты (разграничение доступа, регистрация событий, межсетевое экранирование) на виртуальном стенде ЭИОС.

Модуль 4. Защита персональных данных при обработке в АС, организационно-распорядительная документация (12 ч)

Тема 4.1. Правовые основы обработки персональных данных. Понятия «персональные данные», «обработка», «оператор», «субъект персональных данных». Принципы и условия обработки персональных данных. Правовые основания обработки, согласие субъекта. Специальные категории и биометрические персональные данные. Права субъектов персональных данных.

Тема 4.2. Обязанности оператора персональных данных. Обязанности оператора при сборе, хранении, использовании и уничтожении персональных данных. Уведомление уполномоченного органа об обработке персональных данных. Локализация баз данных на территории Российской Федерации. Ответственность за нарушение законодательства о персональных данных.

Тема 4.3. Обеспечение безопасности персональных данных в информационных системах. Уровни защищённости персональных данных при их обработке в информационных системах (постановление Правительства РФ от 01.11.2012 № 1119): типы актуальных угроз, порядок определения уровня защищённости. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных (приказ ФСТЭК России от 18.02.2013 № 21).

Тема 4.4. Организационно-распорядительная документация по защите персональных данных. Политика в отношении обработки персональных данных. Приказы о назначении ответственных, о перечне лиц, допущенных к обработке. Инструкции, положения, перечни обрабатываемых персональных данных. Модель угроз информационной системы персональных данных. Порядок разработки, согласования и утверждения документов.

Практическое занятие 4.5. Определение уровня защищённости условной информационной системы персональных данных и подготовка комплекта организационно-распорядительной документации оператора.

Модуль 5. Практикум на виртуальных стендах ЭИОС (12 ч)

Тема 5.1. Комплексная разработка модели угроз безопасности информации для условной автоматизированной системы (определение нарушителей, актуальных угроз, способов реализации). **Тема**

5.2. Подготовка комплекта организационно-распорядительной документации по защите персональных данных (политика, приказы, инструкции, перечни). **Тема 5.3.** Отработка сценария реагирования на инцидент информационной безопасности: выявление, регистрация, локализация, устранение последствий, документирование. **Тема 5.4.** Итоговый разбор выполненных работ, самопроверка и подготовка к итоговой аттестации.

VI. Формы аттестации и оценочные материалы (фонд оценочных средств)

26. Система оценки. Освоение программы сопровождается **промежуточной аттестацией** по каждому разделу (модулю) в форме тестирования (зачёта) в ЭИОС (статья 58 Федерального закона № 273-ФЗ). Порог успешного прохождения – не менее 60 % правильных ответов; оценка – «зачтено» / «не зачтено». Промежуточная аттестация по модулю 5 проводится в форме зачёта по практикуму. Освоение программы завершается **итоговой аттестацией** в форме итогового тестирования в ЭИОС (не менее 40 вопросов). Порог – не менее 70 % правильных ответов; оценка – «зачтено» / «не зачтено». Все виды аттестации проводятся дистанционно в ЭИОС с идентификацией личности обучающегося и фиксацией результатов (электронная ведомость, протокол).

27. Критерии оценивания. «Зачтено» – обучающийся набрал не менее установленного порога и продемонстрировал знание материала. «Не зачтено» – порог не достигнут. Для практических заданий:

«зачтено» — задание выполнено в соответствии с требованиями; «не зачтено» — задание не выполнено или выполнено с существенными ошибками.

28. Банк тестовых вопросов для промежуточной аттестации (примерный).

Модуль 1: 1. Перечислите три основных свойства безопасности информации. (*конфиденциальность, целостность, доступность*) 2. Какой федеральный закон регулирует отношения в области информации и её защиты? (*№ 149-ФЗ*) 3. Какой орган осуществляет функции по технической защите конфиденциальной информации? (*ФСТЭК России*) 4. Какой орган осуществляет надзор в сфере обработки персональных данных? (*Роскомнадзор*) 5. Приказ ФСТЭК России, устанавливающий требования к защите информации в государственных информационных системах. (*№ 17*) 6. Что относится к информации ограниченного доступа? (*сведения, доступ к которым ограничен федеральными законами*)

Модуль 2: 7. Что такое угроза безопасности информации? (*потенциальная причина нежелательного события, способного нанести ущерб*) 8. Назовите типы нарушителей по расположению относительно системы. (*внешний, внутренний*) 9. Как называется информационный ресурс ФСТЭК России, содержащий сведения об угрозах и уязвимостях? (*Банк данных угроз – БДУ*) 10. Перечислите основные этапы оценки угроз по Методике ФСТЭК (2021). (*негативные последствия, объекты воздействия, источники и возможности нарушителей, способы реализации, актуальные угрозы*) 11. Что характеризует потенциал нарушителя? (*базовый, базовый повышенный, высокий*)

Модуль 3: 12. Приведите примеры организационных мер защиты информации. (*разграничение доступа, парольная политика, регламенты, учёт носителей*) 13. Каковы основные функции СЗИ от НСД? (*идентификация/аутентификация, управление доступом, регистрация событий, контроль целостности*) 14. Назначение межсетевого экрана. (*контроль и фильтрация сетевого трафика*) 15. Что такое сегментирование сети и зачем оно применяется? (*разделение сети на зоны для ограничения распространения угроз*) 16. Какие требования предъявляются к средствам защиты информации в части сертификации? (*применение сертифицированных средств в установленных случаях*)

Модуль 4: 17. Дайте определение персональных данных. (*любая информация, относящаяся к прямо или косвенно определённому физическому лицу*) 18. Сколько уровней защищённости персональных данных установлено? (*четыре*) 19. Какой нормативный акт устанавливает уровни защищённости ПДн? (*ПП РФ № 1119*) 20. Приказ ФСТЭК России, определяющий состав мер по защите ПДн. (*№ 21*) 21. Перечислите основные организационно-распорядительные документы оператора ПДн. (*политика, приказы, инструкции, перечни, модель угроз*)

29. Банк вопросов и заданий для итоговой аттестации (примерный). 1. Понятие и свойства безопасности информации; виды защищаемой информации. 2. Система регуляторов в области защиты информации и их полномочия. 3. Требования приказов ФСТЭК России № 17 и № 21: сфера применения и содержание. 4. Порядок построения модели нарушителя. 5. Порядок разработки модели угроз безопасности информации с использованием БДУ ФСТЭК России. 6. Основные этапы Методики оценки угроз безопасности информации (2021). 7. Состав организационных мер защиты информации. 8. Состав технических мер и типовые средства защиты информации. 9. Основы сетевой безопасности; сегментирование сети. 10. Криптографические методы защиты (обзорно); электронная подпись. 11. Правовые основы обработки персональных данных; обязанности оператора. 12. Уровни защищённости ИСПДн и порядок их определения. 13. Состав организационно-распорядительной документации по защите персональных данных. 14. Порядок реагирования на инцидент информационной безопасности. 15. Практическое задание: по описанию условной автоматизированной системы определить состав защищаемой информации, тип нарушителя и перечень актуальных угроз.

(Полный банк – не менее 40 вопросов – формируется и хранится в ЭИОС.)

30. Практические задания (примерные). - Задание 1. По описанию условной АС определить состав защищаемой информации и применимые нормативные требования. - Задание 2. Разработать проект модели угроз для условной АС (нарушители, актуальные угрозы, способы реализации). - Задание 3.

Определить уровень защищённости условной ИСПДн и подобрать состав мер защиты по приказу ФСТЭК № 21. - Задание 4. Подготовить комплект ОРД оператора персональных данных (политика, приказ, инструкция). - Задание 5. Составить порядок реагирования на инцидент информационной безопасности.

31. Методические материалы – электронные конспекты, презентации, видеолекции, нормативные документы, методические указания по выполнению практических заданий, инструкции по работе с виртуальными стендами; размещаются в ЭИОС.

VII. Порядок работы с обучающимися по результатам аттестации

32.1. Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдаётся **удостоверение о повышении квалификации**; сведения о выданном документе вносятся в Федеральную информационную систему «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (ФИС ФРДО) в течение 30 календарных дней. **32.2.** Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительный результат, предоставляется право повторного прохождения итоговой аттестации в срок, установленный Организацией (по графику), но не более двух повторных попыток; порядок определён локальным нормативным актом Организации об аттестации. **32.3.** Лицам, освоившим часть программы и (или) отчисленным из Организации до завершения обучения, выдаётся **справка об обучении (о периоде обучения)** по образцу, установленному Организацией. **32.4.** Основания и порядок отчисления, приостановления и прекращения образовательных отношений определяются локальными нормативными актами Организации.

Приложение 1. Глоссарий основных терминов

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность информации – состояние защищённости информации, при котором обеспечены её конфиденциальность, целостность и доступность. **Доступность информации** – состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. **Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на неё. **Инцидент информационной безопасности** – событие, указывающее на нарушение или угрозу нарушения безопасности информации.

Конфиденциальность информации – обязательное для выполнения требование не допускать доступ к информации без согласия её обладателя. **Модель нарушителя** – описание типов, возможностей и мотивации потенциальных нарушителей безопасности информации. **Модель угроз безопасности информации** – систематизированное описание угроз, актуальных для конкретной информационной (автоматизированной) системы. **Несанкционированный доступ (НСД)** – доступ к информации с нарушением установленных прав и (или) правил доступа. **Оператор персональных данных** – лицо, организующее и (или) осуществляющее обработку персональных данных. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определённому физическому лицу (субъекту персональных данных). **Средство защиты информации (СЗИ)** – техническое, программное или программно-техническое средство, предназначенное для защиты информации. **Угроза безопасности информации** – совокупность условий и факторов, создающих потенциальную или реальную опасность нарушения безопасности информации. **Уязвимость** – недостаток информационной системы, использование которого нарушителем может привести к реализации угрозы. **Целостность информации** – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно уполномоченными субъектами.

Приложение 2. Перечень нормативных правовых актов и методических документов

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составов и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
8. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).
9. Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).
10. Приказ Минобрнауки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».
11. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (код 06.033), утв. приказом Минтруда России от 14.09.2022 № 525н.

Нормативные правовые акты применяются в редакции, действующей на дату реализации программы.

Приложение 3. Перечень учебных изданий и информационных ресурсов

1. Нестеров С. А. Основы информационной безопасности: учебное пособие. — СПб.: Лань.
2. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. — М.: ДМК Пресс.
3. Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие. — М.: Форум.
4. Официальный сайт ФСТЭК России (fstec.ru); Банк данных угроз безопасности информации (bdu.fstec.ru).
5. Электронные конспекты, видеолекции и методические материалы, размещённые в ЭИОС Организации.

Приложение 4. Форма протокола итоговой аттестации

ПРОТОКОЛ № _____ итоговой аттестации от « _____ » _____ 20____
г. Программа: ДПП ПК «Обеспечение защиты информации в автоматизированных системах»
(72 ч). Форма итоговой аттестации: итоговое тестирование. Состав аттестационной комиссии: председатель _____
; члены комиссии _____.

№	Ф. И. О. обучающегося	Результат (%)	Решение (зачтено / не зачтено)
1			
2			

Председатель комиссии _____ / _____ /
Члены комиссии _____ / _____ /

Приложение 5. Форма ведомости промежуточной аттестации

ВЕДОМОСТЬ промежуточной аттестации по модулю _____ от « _____ »
_____ 20 _____ г.

№	Ф. И. О. обучающегося	Форма контроля	Результат (%)	Оценка (зачтено / не зачтено)
1				
2				

Преподаватель _____ / _____ /