УТВЕРЖДАЮ
Генеральный директор
_____ Лисенков Р.А.
М.П.
«_04_» _____мая_____ 2025 г.
дата утверждения

Дополнительная профессиональная программа

(программа повышения квалификации)

«Информационная безопасность»

Санкт-Петербург
2025

Оглавление

1. Пояснительная записка

1.1. Назначение программы

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность» (далее – «Программа») направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации в области информационной безопасности.

Программа обучения содержит информацию о темах обучения, практических занятиях, формах обучения, формах проведения проверки знания, а также о количестве часов, отведенных на изучение каждой темы, выполнение практических занятий и на проверку знаний. Программа регламентирует цели, планируемые результаты, содержание, условия и технологии реализации процесса обучения, оценку качества подготовки обучающихся и включает в себя в том числе: учебный план, фонд оценочных средств, формы контроля знаний и требования к его проведению, календарный учебный график и другие материалы, обеспечивающие качество подготовки обучающихся.

1.2. Нормативные документы, регламентирующие разработку программы

Программа разработана в соответствии с:

1. Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
2. Приказом Министерства науки и высшего образования Российской Федерации от 24 марта 2025 г. N 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам";
3. Приказом Министерства просвещения РФ от 27 июля 2022 г. N 629 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам";
4. Постановление Правительства РФ от 11 октября 2023 г. N 1678 "Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ";
5. Письмом Министерства образования и науки РФ от 21 апреля 2015 г. N ВК-1013/06 "О направлении методических рекомендаций по реализации дополнительных профессиональных программ"
6. Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утв. Министерством образования и науки РФ 22 января 2015 г. N ДЛ-1/05вн)
7. прочими законодательными актами, регламентирующими работу в сфере образования, а также реализацию дополнительных профессиональных программ.

2. Общая характеристика программы

2.1. Цель реализации программы

Цель: совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации.

2.2. Требования к обучающимся

К освоению Программы повышения квалификации допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

2.3. Форма и сроки обучения

Форма обучения: заочная, с применением дистанционных образовательных технологий, электронного обучения.

Трудоемкость программы: 72 академических часов.

Срок освоения программы – 9 дней.

Начало обучения – по мере набора группы.

Режим занятий: не более 8 академических часов в день.

Проверка знания проводится согласно учебному плану и календарному графику.

Форма итоговой аттестации: итоговое тестирование

3. Планируемые результаты обучения

В результате обучения слушатели должны знать:

- Основные положения и требования нормативно-правовых актов, регламентирующих их профессиональную деятельность;
- Ключевые принципы, методы и технологии, применяемые в их профессиональной сфере;
- Структуру и содержание основных отраслевых стандартов, регламентов и лучших практик, относящихся к их работе.

В результате обучения слушатели должны уметь:

- Применять полученные знания нормативно-правовой базы и профессиональных методов для решения практических задач в своей области деятельности;
- Анализировать профессиональные ситуации и документы, выявляя соответствие или несоответствие установленным требованиям и стандартам;
- Формулировать обоснованные предложения и принимать решения по совершенствованию процессов в рамках своей профессиональной компетенции.

В результате обучения слушатели должны владеть:

- Системным подходом к решению профессиональных задач и анализу рабочих ситуаций;
- Навыками работы с профессиональной информацией: поиск, анализ, интерпретация и применение нормативных документов, технической документации, отраслевых источников;
- Навыками эффективной профессиональной коммуникации для обсуждения рабочих вопросов, представления результатов анализа и аргументации своих решений.

4. Содержание программы

4.1. Учебный план

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе:			Форма аттестации/ контроля
			Лекции	Самостоя-тельная работа	Практи-ческие занятия	
1.	Основные понятия и определения в области информационной безопасности	11	11			Не предусмотрено (самоконтроль)
2.	Угрозы информационной безопасности. Каналы утечки информации	7	7			Не предусмотрено (самоконтроль)
3.	Вредоносное ПО. Компьютерные вирусы и средства защиты от них	9	9			Не предусмотрено (самоконтроль)
4.	Правовое обеспечение информационной безопасности	9	9			Не предусмотрено (самоконтроль)
5.	Стандарты информационной безопасности	7	7			Не предусмотрено (самоконтроль)
6.	Административный уровень информационной безопасности	11	11			Не предусмотрено (самоконтроль)
7.	Процедурный уровень информационной безопасности	9	9			Не предусмотрено (самоконтроль)
8.	Программно-технические методы защиты информационной безопасности	7	7			Не предусмотрено (самоконтроль)
Итоговая аттестация по Программе		2			2	Дистанционное тестирование
Всего часов по Программе		**72**	**70**	**-**	**2**	

4.2. Календарный учебный график

№ п/п	Наименование дисциплин по учебному плану	Коли-чество часов	Дни								
			1	2	3	4	5	6	7	8	9
1.	Основные понятия и определения в области информационной безопасности	11	8	3							
2.	Угрозы информационной безопасности. Каналы утечки информации	7		5	2						
3.	Вредоносное ПО. Компьютерные вирусы и средства защиты от них	9			6	3					
4.	Правовое обеспечение информационной безопасности	9				5	4				
5.	Стандарты информационной безопасности	7					4	3			
6.	Административный уровень информационной безопасности	11						5	6		
7.	Процедурный уровень информационной безопасности	9							2	7	
8.	Программно-технические методы защиты информационной безопасности	7								1	6
	Итоговая аттестация по Программе	2									2
	Всего часов по Программе:	72	8	8	8	8	8	8	8	8	8

4.3. Рабочие программы учебных модулей

Тема 1. Основные понятия и определения в области информационной безопасности

- Цель и задачи информационной безопасности (ИБ). Понятие информационной безопасности как состояния защищенности. Ключевые задачи: обеспечение конфиденциальности, целостности и доступности информации.
- Базовые принципы обеспечения ИБ: законность, системность, комплексность, непрерывность, планирование, адекватность мер.
- Объекты и субъекты защиты.
- Понятие уязвимости, угрозы и риска. Разграничение терминов. Уязвимость как слабое место, угроза как источник опасности, риск как вероятность реализации угрозы через уязвимость.
- Атака на информационную систему. Определение и классификация атак (активные/пассивные, внутренние/внешние). Стадии реализации атаки (разведка, доступ, выполнение действий, сокрытие следов).

Тема 2. Угрозы информационной безопасности. Каналы утечки информации

- Классификация угроз ИБ: по природе возникновения (естественные/искусственные), по умыслу (случайные/преднамеренные), по объекту воздействия.
- Источники угроз: внутренние (сотрудники) и внешние (хакеры, конкуренты, киберпреступники).
- Понятие канала утечки информации. Физические и технические каналы утечки.

- Технические каналы утечки: побочные электромагнитные излучения (ПЭМИН), акустические каналы (подслушивание), сетевые каналы (перехват трафика).
- Несанкционированный доступ к информации: методы и средства (подбор паролей, использование уязвимостей, социальная инженерия).

Тема 3. Вредоносное ПО. Компьютерные вирусы и средства защиты от них

- Классификация вредоносного программного обеспечения (Malware): вирусы, черви, трояны, шпионское ПО, ransomware (вымогатели), руткиты.
- Принципы работы компьютерных вирусов: механизмы заражения, резидентные и нерезидентные вирусы, полиморфные и стелс-вирусы.
- Антивирусное программное обеспечение: принципы работы (сигнатурный анализ, эвристический анализ, поведенческий анализ).
- Проактивные методы защиты: песочницы (sandboxing), системы предотвращения вторжений (HIPS).
- Действия пользователя при заражении: алгоритм обнаружения и устранения последствий, использование антивирусных сканеров.

Тема 4. Правовое обеспечение информационной безопасности

- Структура законодательства РФ в области ИБ.
- Регулирование работы с персональными данными (ПДн). Понятие ПДн. Требования к операторам ПДн. Меры по защите ПДн.
- Уголовная и административная ответственность за правонарушения в сфере ИБ.
- Лицензирование и сертификация в области ИБ. Лицензии ФСТЭК и ФСБ на деятельность по технической защите конфиденциальной информации.
- Международные стандарты и нормативные акты.

Тема 5. Стандарты информационной безопасности

- Роль и место стандартов в построении СЗИ. Добровольное и обязательное применение. Национальные и международные стандарты.
- Семейство стандартов ISO 27000. ISO 27001 как основной стандарт по созданию Системы управления информационной безопасностью (СУИБ). Структура и основные требования.
- Отечественные стандарты (серии ГОСТ Р ИСО/МЭК 27000, ГОСТ Р 56939, Р 57628). Адаптация международных стандартов и национальные разработки.
- Отраслевые стандарты: PCI DSS для платежных систем, стандарты Банка России (СТО БР ИББС) для финансового сектора.
- Руководящие документы ФСТЭК России. Требования по защите информации и порядку их выполнения для госструктур и КИИ.

Тема 6. Административный уровень информационной безопасности

- Разработка и внедрение политик информационной безопасности. Иерархия документов: политика, стандарты, руководства, процедуры.
- Организационная структура службы ИБ. Роли и обязанности.
- Управление персоналом в контексте ИБ: подбор кадров, обучение и информирование,

процедуры при увольнении.

- Реагирование на инциденты информационной безопасности: создание Computer Security Incident Response Team (CSIRT), регламент действий.
- Управление рисками ИБ: идентификация активов, оценка и анализ рисков, выбор и внедрение контрмер.

Тема 7. Процедурный уровень информационной безопасности

- Разграничение физического доступа в помещения: пропускной режим, зонирование, охрана, системы видеонаблюдения.
- Регламентация рабочих процедур: инструкции по работе с конфиденциальной информацией, правила использования интернета и электронной почты.
- Управление паролями: требования к сложности, сроку действия, правила хранения. Процедуры восстановления доступа.
- Обеспечение чистоты рабочих мест (clean desk policy): правила работы с документами, использование сейфов, уничтожение бумажных носителей.
- Процедуры резервного копирования и восстановления данных: регламент создания копий, частота, тестирование процедуры восстановления.

Тема 8. Программно-технические методы защиты информационной безопасности

- Идентификация, аутентификация и авторизация. Пароли, токены, биометрия. Принцип минимальных привилегий.
- Системы защиты от вредоносного ПО (антивирусы), межсетевые экраны (файрволы), системы обнаружения и предотвращения вторжений.
- Криптографические методы защиты: шифрование данных, электронная подпись, VPN.
- Механизмы аудита и протоколирования (журналирования). Сбор, хранение и анализ логов для выявления аномалий и расследования инцидентов.
- Резервное копирование и восстановление: технологии и методы (полное/инкрементальное/дифференциальное копирование), схемы ротации носителей.

5. Организационно-педагогические условия

Реализация Программы проходит в полном соответствии с требованиями законодательства Российской Федерации в области образования, нормативными правовыми актами, регламентирующими данные направления деятельности. При обучении могут применяться различные виды занятий - лекции, самостоятельная работа слушателей, практические занятия, сочетание различных форм занятий и т.д. Вид занятий определяется учебным планом. При этом используются технические средства, способствующие лучшему теоретическому и практическому усвоению программного материала: видеофильмы, компьютеры, мультимедийные программы. Основные методические материалы размещаются в электронной информационно-образовательной среде с использованием программного продукта - платформы дистанционного обучения.

5.1. Квалификация педагогических кадров, обеспечивающих реализацию программы

Организация, реализующая программу, укомплектована квалифицированными кадрами. Уровень квалификации работников организации, реализующей программу, соответствует квалификационным характеристикам по соответствующей должности. Обучение по программе осуществляется преподавателями с профильным высшим образованием: квалификация преподавателей соответствует требованиям квалификационных справочников по должности «преподаватель». Педагогические работники обязаны проходят в установленном законодательством Российской Федерации порядке обучение по дополнительным профессиональным программам по профилю педагогической деятельности не реже одного раза в три года.

5.2. Материально-технические условия реализации программы

Реализация программы в очно-заочном формате требует наличия учебного кабинета, оборудованного учебной мебелью, доской или флипчартом. Технические средства обучения: компьютеры с программным обеспечением, проектор.

При необходимости, для проведения теоретических лекционных занятий, может применяться система дистанционного обучения (СДО). Для организации электронного обучения обеспечивается доступ обучающихся и педагогических работников к учебно-методическому контенту, организованному в виртуальной обучающей среде.

Применение электронного обучения и дистанционных образовательных технологий подразумевает использование такого режима обучения, при котором слушатель осваивает образовательную программу полностью или частично самостоятельно (удаленно) с использованием электронной информационно-образовательной среды (системы дистанционного обучения). Все коммуникации с педагогическим работником осуществляются посредством указанной среды (системы), а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи информации и взаимодействие слушателей и педагогических работников. Электронная информационно-образовательная среда (ЭИОС) включает в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств, которые обеспечивают освоение образовательных программ в полном объеме независимо от места

нахождения слушателей.

Доступ обучающихся к ЭИОС осуществляется средствами всемирной компьютерной сети Интернет в круглосуточном режиме без выходных дней. Авторизация слушателей с выдачей персональных логинов и паролей производится методистом.

Для обеспечения эффективного процесса обучения с применением электронного обучения слушателям необходимо следующее материально-техническое обеспечение: персональный компьютер с выходом в информационно-коммуникационную сеть «Интернет», гарнитура (наушники и микрофон) и программное обеспечение (пакет офисных приложений, веб браузер).

Для успешного освоения обучения в электронной форме от обучающихся требуется навык использования персонального компьютера на уровне пользователя - основные приемы работы с текстом, файлами и папками в приложениях Windows, работа в информационно телекоммуникационной сети «Интернет» (в том числе использование сервисов электронной почты).

Основой применения электронного обучения и дистанционных образовательных технологий является Положение об организации и использовании электронного обучения и дистанционных образовательных технологий при реализации дополнительных профессиональных программ, основных программ профессионального обучения, дополнительных общеобразовательных программ – дополнительных общеразвивающих программ детей и взрослых, согласованное педагогическим советом и утвержденное генеральным директором.

5.3. Информационное и учебно-методическое обеспечение программы

Программа обеспечена учебно-методической документацией и материалами по всем учебным разделам. Доступ слушателей к учебно-методическим материалам, учебным пособиям, презентациям, тестам для самоконтроля возможен в электронной информационно-образовательной среде в любое удобное для слушателя время в течение периода обучения.

Практические занятия направлены на развитие творческого мышления слушателей и формирование практических умений и навыков работы.

При реализации Программы предусматриваются следующие виды внеаудиторной (самостоятельной) работы слушателей:

- работа с учебно-методическими пособиями (конспектом лекций);
- работа с рекомендованной литературой, нормативно-правовыми документами, документами административной и судебной практики;
- просмотр обучающего видео / прослушивание обучающего аудио;
- выполнение тестовых заданий (текущий и промежуточный контроль);
- подготовка к итоговой аттестации.

5.4. Организационно-сопроводительное обеспечение программы

При организации и проведении учебных занятий со слушателями по Программе преподавателям необходимо:

• ознакомиться с составом учебной группы;

• излагая материал по теме, находить разумное сочетание его теоретических и практических аспектов, при этом приоритет следует отдавать практическим вопросам;

• давать слушателям по окончании учебных занятий методические рекомендации по самостоятельному изучению обсуждаемых проблем, использованию необходимой для этого литературы;

• активно использовать при подготовке и проведении групповых обсуждений знания и опыт слушателей;

• использовать инновационные технологии в обучении;

• готовить информационно-справочный и раздаточный материал по раскрываемой теме, который может быть использован слушателями в практической работе.

При организации учебных занятий по Программе работникам образовательной организации необходимо:

• при подборе преподавателей учитывать их теоретическую подготовку и наличие практических знаний в сфере преподаваемой дисциплины, чтобы в содержательной части учебной программы нашли отражение наиболее актуальные вопросы,

• выдавать слушателям расписание учебных занятий,

• помогать преподавателям и специалистам-практикам в подготовке информационно справочного и раздаточного материала по Программе.

6. Оценка качества освоения программы

6.1. Формы контроля знаний и требования к его проведению

Текущий контроль знаний обучающихся проводится на протяжении всего обучения по программе преподавателем, ведущим занятия в учебной группе. Текущий контроль знаний включает в себя наблюдение преподавателя за учебной работой обучающихся и проверку качества знаний, умений и навыков, которыми они овладели на определенном этапе обучения посредством наблюдения и в иных формах, установленных преподавателем.

Оценка качества освоения Программы слушателями предусматривает итоговую аттестацию по программе.

Итоговая аттестация (проверка знаний) - процедура, проводимая с целью установления уровня знаний обучающихся с учетом прогнозируемых результатов обучения и требований к результатам освоения образовательной программы.

Итоговая оценка качества освоения программы проводится в виде проверки знаний в форме тестирования в системе СДО.

Итоговая аттестация, завершающая освоение программы, является обязательной.

Итоговая аттестация проводится на основе принципов объективности и независимости оценки качества подготовки слушателей.

К итоговой аттестации по Программе допускается слушатель, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план.

Лицам, успешно прошедшим итоговую аттестацию, выдается Удостоверение установленного организацией образца.

Для проверки знаний создан фонд оценочных средств, позволяющий оценить знания, умения и уровень приобретенных компетенций.

Фонд оценочных средств соответствует целям и задачам программы, учебному плану и обеспечивает оценку качества компетенций, приобретаемых обучающимся.

6.2. Критерии оценки знаний обучающихся

Слушателям предоставляются 3 пробные попытки прохождения тестирования.

В случае, если правильные ответы на все вопросы теста составляют 65% и более, то результат тестирования считается удовлетворительным для сдачи итоговой аттестации.

В случае, если правильные ответы на все вопросы теста составляют менее 65%, то результат тестирования считается неудовлетворительным для сдачи итоговой аттестации.

6.3. Оценочные материалы

Примеры заданий итогового тестирования:

1. Что составляет классическую триаду (модель) CIA информационной безопасности?
   A. Конфиденциальность, Интегрированность, Доступность
   B. Конфиденциальность, Целостность, Аутентичность
   C. Конфиденциальность, Целостность, Доступность ✅
   D. Криптография, Идентификация, Авторизация

2. Какой тип вредоносного программного обеспечения маскирует свое присутствие в системе и предоставляет злоумышленнику удаленный контроль над компьютером жертвы?
   A. Клавиатурный шпион (Keylogger)
   B. Рекламное ПО (Adware)
   C. Троянская программа (Trojan) ✅
   D. Фарминг (Pharming)

3. Какой федеральный закон Российской Федерации устанавливает основные принципы и правовые основы защиты персональных данных?
   A. № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
   B. № 152-ФЗ "О персональных данных" ✅
   C. № 187-ФЗ "О безопасности критической информационной инфраструктуры"
   D. № 161-ФЗ "О национальной платежной системе"

4: Какой международный стандарт является наиболее известным и описывает требования к системе управления информационной безопасностью (СУИБ)?

A. ISO 9001 (Системы менеджмента качества)
B. PCI DSS (стандарт для индустрии платежных карт)
C. ISO/IEC 27001 (Системы управления информационной безопасностью) ✅
D. GOST R 54593 (Безопасность в финансовом секторе)

5: Какой механизм защиты является основным для контроля и разграничения сетевого трафика между сетевыми сегментами с разным уровнем доверия?

A. Система обнаружения вторжений (IDS)
B. Межсетевой экран (Firewall) ✅
C. Антивирусное программное обеспечение
D. Система предотвращения утечек (DLP)

7. Список рекомендуемой литературы для освоения программы

1. Основная литература и нормативные правовые акты (актуальные редакции с изменениями и дополнениями):
2. С.И. Макаренко / Информационная безопасность: учебное пособие. /– Ставрополь, 2009 г. – 372 стр.
3. В.В. Беспалов / Информационные технологии / – Томск: Изд-во Томского политехнического университета, 2012. – 134 стр.
4. Ясенев В.Н. / ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2006. – 253 стр.
5. В.В. СУХОСТАТ / Основы информационной безопасности / – СПб. : Изд-во СПбГЭУ, 2019. – 103 стр.
6. Комплексное обеспечение информационной безопасности автоматизированных систем: учеб. пособие / В.А. Челухин. - Комсомольск-на-Амуре: ФГБОУ ВПО "КнАГТУ", 2014. - 207 с.

Дополнительная литература:

1. С.И. Макаренко / Информационная безопасность / – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 стр.
2. В.В. Беспалов / Информационные технологии / – Томск: Изд-во Томского политехнического университета, 2012. – 134 стр.
3. Ю. Ю. Громов / Информационные технологии / – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2015 г. – 260 стр.
4. Е.В. Вострецова / Основы информационной безопасности / — Екатеринбург : Изд-во Урал. ун-та, 2019 г. — 204 стр.
5. А.М. Кенин / Самоучитель системного администратора / Санкт-Петербург 2019 г. - 608 стр.
6. Информационное право России: Учеб. пособие для студентов, обучающихся по специальностям (направлениям) «Юриспруденция» и «Прикладная информатика в юриспруденции». – Саратов: Изд-во Сарат. ун-та, 2010. – 196 с
7. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.
8. Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации. Учебное пособие – М.: Мир науки, 2022.
9. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. — М.: Издательство «Аспект Пресс», 2019.— 784 с.