ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ АКАДЕМИЯ КИБЕРЁЖ

ООО "АКАДЕМИЯ КИБЕРЁЖ"

ОГРН: 1257700486702 ИНН: 7735212702 КПП: 773501001

Утверждаю
Генеральный директор

30 ноября 2025 г.

_____ **/ Денисенко Павел Андреевич**

Дополнительная профессиональная программа профессиональной переподготовки

«Специалист по информационной кибербезопасности»

Форма обучения: очная (с применением исключительно дистанционных образовательных технологий и электронного обучения)
Срок реализации: 12 месяцев, 52 недели

Режим занятий: 12 академических часов в неделю

Объем программы: 624 академических часа

Авторы программы: Василевич Иван Владиславович

г. Москва, 2026 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Характеристики программы:

Дополнительная профессиональная программа повышения квалификации «Специалист по информационной кибербезопасности» (далее - Программа) разработана в соответствии с требованиями:

- Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки Российской Федерации от 1 декабря 2016 г. N 1515 - МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИКАЗ от 1 декабря 2016 г. N 1515 ОБ УТВЕРЖДЕНИИ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (УРОВЕНЬ БАКАЛАВРИАТА);
- Профессионального стандарта **«Специалист по информационным ресурсам»** (код **06.013**) — утверждён Приказом Министерства труда и социальной защиты Российской Федерации от **19 июля 2022 г. № 420н**, действует в период с **01.03.2023 по 01.03.2029**;
- Профессионального стандарта **«Специалист по защите информации в автоматизированных системах»** (код **06.033**) — утверждён Приказом Министерства труда и социальной защиты Российской Федерации от **14 сентября 2022 г. № 525н**, действует в период с **01.03.2023 по 01.03.2029**;
- Постановления Правительства Российской Федерации от 11.10.2023 № 1678 "Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ";
- с учетом требований приказа Минобрнауки РФ от 24.03.2025 N 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

1.2. Характеристика профессиональной деятельности слушателей: Основная цель вида профессиональной деятельности слушателей:

Профессиональная деятельность слушателей, осваивающих программу, относится к сфере решения задач, связанных с обеспечением защищённости объектов информатизации в условиях существования угроз в информационной сфере.

Основная цель вида профессиональной деятельности слушателей: «Повышение защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости».

1.3. Категория слушателей: лица, имеющие среднее профессиональное и (или) высшее образование по направлению в области информационной безопасности; лица, получающие среднее профессиональное и (или) высшее образование по направлению в области

информационной безопасности. Требования к слушателям: Лица, достигшие 18 лет, уже имеющие профессиональный опыт и желающие получить новую профессию или развить полезные навыки в сфере информационной безопасности для применения в работе.

1.4. Объем программы (трудоемкость): общая трудоемкость 624 академических часов.

1.5. Срок освоения программы - 52 недели.

1.6. Форма обучения: очная (с применением исключительно электронного обучения, дистанционных образовательных технологий).

1.7. Документ, выдаваемый после завершения обучения: по окончании обучения слушателям, выдается удостоверение о повышении квалификации установленного образца. Слушателям без оконченного высшего образования и (или) среднего профессионального образования удостоверение о повышении квалификации выдаётся одновременно с получением соответствующего документа об образовании и о квалификации.

2. ЦЕЛИ И ЗАДАЧИ ПРОГРАММЫ

2.1. Цель программы

Целью реализации дополнительной профессиональной программы профессиональной переподготовки «Специалист по информационной кибербезопасности» является подготовка слушателей к выполнению профессиональной деятельности в области обеспечения защищённости автоматизированных и информационных систем от современных киберугроз, включая обнаружение и анализ инцидентов, проведение аудита (оценки) защищённости, выявление уязвимостей и разработку мер защиты, с учётом правовых и этических требований, а также требований профессиональных стандартов и нормативных правовых актов в сфере образования и информационной безопасности.

2.2. Задачи программы

Для достижения цели Программа предусматривает решение следующих задач:

Формирование базовых профессиональных представлений в области информационной безопасности:

- освоение ключевых понятий, моделей угроз и принципов обеспечения конфиденциальности, целостности и доступности информации;
- понимание роли организационных и технических мер защиты в системе обеспечения информационной безопасности.

Освоение компетенций системного и сетевого администрирования как основы обеспечения безопасности инфраструктуры:

- формирование практических навыков администрирования Linux-систем;
- изучение принципов построения и защиты серверной и сетевой инфраструктуры, включая сегментацию и управление доступом.

Развитие навыков автоматизации задач информационной безопасности:

освоение основ программирования на Python применительно к задачам ИБ;

формирование умений разрабатывать скрипты для мониторинга, анализа, обработки данных и автоматизации типовых операций безопасности.

Формирование правовой грамотности и понимания регуляторных требований в сфере защиты информации:

- изучение правовых основ защиты информации, ответственности и требований к соблюдению законодательства;
- освоение принципов корректной работы с данными и соблюдения профессиональной этики в кибербезопасности.

Освоение методов защиты IT-инфраструктуры и практик мониторинга безопасности:

- формирование навыков настройки средств защиты (в том числе межсетевых экранов и базовых средств предотвращения вторжений);
- развитие компетенций по анализу событий безопасности, логов и работе с системами мониторинга и корреляции событий (SIEM/ELK и аналоги).

Формирование прикладных навыков разведки по открытым источникам (OSINT) для корпоративной безопасности:

- освоение методов выявления цифровых следов и рисков утечек;
- развитие навыков анализа открытой информации для целей профилактики инцидентов и оценки рисков.

Формирование начальных компетенций тестирования на проникновение и оценки уязвимостей:

- освоение базовой методологии пентеста и подходов к выявлению уязвимостей;
- формирование навыков практического тестирования в изолированной среде и подготовки отчётности по результатам работ.

Формирование компетенций в области SOC-аналитики и реагирования на инциденты:

- освоение подходов к обнаружению атак и расследованию инцидентов на основе анализа логов и сетевого трафика;
- развитие навыков первичного реагирования, классификации инцидентов и подготовки отчётов для руководства и технических подразделений.

Итоговая интеграция компетенций в рамках дипломного проекта:

- выполнение практико-ориентированного проекта, включающего анализ защищённости, выявление рисков/уязвимостей и подготовку обоснованных рекомендаций по повышению уровня безопасности;
- формирование навыков структурированного представления результатов и профессионального оформления отчётных материалов.

3. УЧЕБНЫЙ ПЛАН

№	Наименование разделов и дисциплин	Всего ак. часов	В том числе:	Формы контроля
			Лекции	Практика
1	**Введение в информационную безопастность**	40	17	23
2	**Системный администратор Linux**	86	26	60
3	**Python для специалиста ИБ**	57	17	40
4	**Правовые аспекты информационной безопасности**	33	15	18
5	**Основы защиты ИТ инфраструктуры**	87	26	61
6	**Введение в OSINT: корпоративная безопасность и защита от утечек**	80	33	47
7	**Введение в пентест**	87	27	60
8	**Введение в SOC-аналитику**	87	33	54
9	**Карьера и трудоустройство**	20	14	6
	Дипломный проект	47		47
ИТОГО		624	208	416

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Общая характеристика планируемых результатов

Реализация программы профессиональной переподготовки направлена на получение слушателями **новой квалификации** и формирование компетенций, необходимых для выполнения нового вида профессиональной деятельности в области обеспечения безопасности информации в автоматизированных системах, включая задачи эксплуатации, мониторинга защищённости, аудита, анализа уязвимостей, внедрения технических и организационных мер защиты, а также документирования работ.

Планируемые результаты сформированы с учётом обобщённых трудовых функций и трудовых функций профессионального стандарта **«Специалист по защите информации в автоматизированных системах» (06.033)**.

4.2. Компетенции, формируемые в результате освоения программы

4.2.1. Общекультурные компетенции (ОК) *(в части, релевантной программе)*

В результате освоения программы слушатель должен обладать:

- **ОК-4** — способностью использовать основы правовых знаний в профессиональной деятельности.
- **ОК-5** — пониманием социальной значимости профессии в сфере информационной безопасности и соблюдением норм профессиональной этики.
- **ОК-6** — способностью работать в коллективе и взаимодействовать с участниками процессов обеспечения ИБ.

- **ОК-7** — способностью к коммуникации в устной и письменной формах для решения профессиональных задач.
- **ОК-8** — способностью к самоорганизации и самообразованию в условиях быстро меняющихся киберугроз.

4.2.2. Общепрофессиональные компетенции (ОПК) ***(в части, релевантной программе)***

В результате освоения программы слушатель должен обладать:

- **ОПК-4** — способностью применять информационные технологии для поиска, обработки и анализа информации в профессиональной деятельности.

  Приказ Минобрнауки РФ от 01.12.…

- **ОПК-5** — способностью использовать нормативные правовые акты в профессиональной деятельности (в том числе при обеспечении безопасности информации и персональных данных).
- **ОПК-7** — способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации.

4.2.3. Профессиональные компетенции программы (ПК) ***(сформированы с учётом профстандарта 06.033)***

В результате освоения программы слушатель должен обладать следующими профессиональными компетенциями:

- **ПК-1. Администрирование защищённых систем и управление доступом.** Способность устанавливать и настраивать ОС и прикладные компоненты с учётом требований ИБ, управлять учётными записями и полномочиями, обеспечивать регистрацию и анализ событий безопасности.
- **ПК-2. Реализация процедур обеспечения безопасности при эксплуатации АС.** Способность выполнять регламентные процедуры обеспечения безопасности, поддерживать актуальность обновлений, обеспечивать выполнение правил эксплуатации с учётом требований защиты информации.
- **ПК-3. Установка и настройка средств защиты информации.** Способность выполнять установку, наладку и настройку средств защиты, определять параметры конфигурации, проводить приёмочные испытания и оформлять изменения в эксплуатационной документации.
- **ПК-4. Мониторинг защищённости и выявление новых угроз.** Способность выявлять угрозы безопасности информации, анализировать недостатки в функционировании системы защиты, принимать меры защиты при появлении новых угроз и формировать рекомендации по модернизации/повторным проверкам.
- **ПК-5. Аудит защищённости и подготовка заключений.** Способность участвовать в работах по оценке (аудиту) защищённости, формировать выводы и рекомендации по результатам проверок.
- **ПК-6. Анализ уязвимостей и подготовка предложений по усилению защиты.** Способность проводить анализ уязвимостей программных и программно-аппаратных средств, уточнять модель угроз, проводить экспертизу защищённости и обосновывать предложения по совершенствованию системы управления защитой.
- **ПК-7. Реагирование на нештатные ситуации и обеспечение устойчивости.** Способность устранять неисправности, документировать действия по

восстановлению, применять средства резервирования и восстановления, обеспечивать отказоустойчивость и непрерывность функционирования.

- **ПК-8. Разработка и внедрение организационных мер защиты.** Способность разрабатывать и актуализировать организационно-распорядительные документы, внедрять организационные меры защиты, проводить обучение персонала по правилам работы с системой защиты.
- **ПК-9. Правомерная и этичная работа с данными и информацией.** Способность применять требования законодательства и внутренних регламентов при обработке информации и персональных данных, определять угрозы безопасности персональных данных и подбирать организационно-технические меры защиты.
- **ПК-10. Подготовка технической и отчётной документации.** Способность вести техническую документацию и оформлять результаты работ по обеспечению защиты информации в установленном формате, включая отчётность по проверкам и выполненным мерам.

4.3. Результаты освоения программы в части дипломного проекта

По завершении программы (в рамках дипломного проекта) слушатель способен выполнить комплексную практико-ориентированную работу: провести анализ защищённости (активы, угрозы, уязвимости), предложить технические и организационные меры защиты, подготовить структурированный отчёт и пакет рекомендаций по повышению уровня кибербезопасности объекта.

5. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Обучение организуется согласно утвержденному календарному учебному графику, который формируется по мере набора учебной группы на соответствующий период обучения. Курс обучения не привязан к началу или окончанию учебного и календарного года. Прием заявок на курс происходит в течение всего календарного года. Календарный учебный график является примерным и утверждается отдельно для каждой учебной группы.

Срок освоения программы – 52 недели – 624 академ. часов. Начало обучения – по мере наборагруппы. Режим занятий – от 12 академических часов в неделю. Для всех видов занятий академический час устанавливается продолжительностью 45 минут. Форма обучения – очная (с применением исключительно дистанционных образовательных технологий и электронного обучения).

Дата начала занятий	**Дата окончания занятий**	**Кол-во учебных недель**	**Кол-во учебных часов**	**Режим занятий**
По мере набора группы	По мере завершения	52	624	**12 академических часов в неделю.**[1]

[1]Для всех видов занятий академический час устанавливается продолжительностью 45 минут.

	обучения группы			

6. ФОРМЫ АТТЕСТАЦИИ. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

6.1. Общие положения

6.1.1. Оценка качества освоения дополнительной профессиональной программы профессиональной переподготовки «Специалист по информационной кибербезопасности» включает:

- текущий контроль успеваемости;
- промежуточную аттестацию по дисциплинам (модулям) учебного плана;
- итоговую аттестацию.

6.1.2. Оценка результатов обучения проводится по совокупности доказательств (результатов выполнения контрольных и практических заданий, отчётов, тестов, кейсов, результатов работы на учебных стендах), обеспечивающих проверку достижения планируемых результатов обучения и сформированности профессиональных компетенций.

6.1.3. Оценочные материалы формируются по каждой дисциплине (модулю) и по итоговой аттестации и включают: перечень контролируемых результатов, типовые задания, критерии и шкалы оценивания, порядок проведения и требования к оформлению результатов.

6.2. Текущий контроль успеваемости

6.2.1. Текущий контроль направлен на поэтапную проверку усвоения учебного материала и формирования практических навыков в ходе освоения дисциплин (модулей).

6.2.2. Основные формы текущего контроля:

- онлайн-тестирование (по темам и разделам);
- практические работы на виртуальных стендах (Linux, Windows, Kali Linux, средства анализа трафика, средства тестирования, SIEM/ELK и аналоги);
- лабораторные работы (настройка, диагностика, сбор и анализ событий, базовые сценарии защиты и реагирования);
- кейс-задания (анализ инцидентов, классификация атак, построение рекомендаций);
- отчёты по практическим работам (в установленном формате);
- проверка исходного кода/скриптов (Python/Bash) и результатов их запуска (логи, артефакты, выгрузки).

6.2.3. Текущий контроль фиксируется в электронных ведомостях/журналах учёта и используется для допуска к промежуточной аттестации (при наличии требований дисциплины).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Литература

- Доронин А.И. "Бизнес-разведка 2.2 + OSINT". - М.: ДМК Пресс, 2023.
- Митник К., Саймон В. "Искусство обмана". - М.: Компания АйТи, 2004.
- Кузнецов Р.А. "Кибербразведка: методы и инструменты". - М.: Эксмо, 2021.
- Бирюков А.А. "Информационная безопасность: защита и нападение". - М.: ДМК Пресс, 2017.
- Федотов Н.Н. "Форензика – компьютерная криминалистика". - М.: Юридический Мир, 2007.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

- Анализ кейсов нарушения принципов конфиденциальности, целостности и доступности (КЦД).
- Разбор правовых инцидентов в сфере информационной безопасности и применение нормативной базы.
- Разбор кейсов кибератак с определением вида, вектора и стадии атаки.
- Анализ атак по фреймворку MITRE ATT&CK: определение техник и фаз угроз.
- Создание и проверка хэшей файлов с использованием командной строки и онлайн-инструментов.
- Верификация цифровых подписей с использованием PGP и GPG.
- Использование VeraCrypt для создания зашифрованных контейнеров и безопасного хранения данных.
- Применение онлайн-сервисов для анализа, расшифровки и генерации криптографических данных.
- Создание безопасного пользовательского профиля и цифровой гигиены в интернете.
- Анализ кейсов по внедрению организационных мер защиты и выработка предложений по улучшению.
- Оценка инцидента ИБ: выявление уязвимостей и подбор соответствующих технических и организационных мер защиты.
- Написание скрипта для проверки сложности паролей по заданным критериям.
- Создание скрипта для автоматической записи подозрительных строк из логов в отдельный файл.
- Разработка анализатора для фильтрации вредоносных URL на основе чёрных списков.
- Реализация простого TCP-сервера и клиента для демонстрации сетевого взаимодействия.
- Получение данных с публичных API (например, курса валют или IP-геолокации).
- Разработка сканера портов с указанием диапазона и логированием результатов.
- Написание скрипта для регулярной проверки системных логов на предмет изменений.
- Создание утилиты для автоматического резервного копирования заданных директорий.
- Реализация скрипта для проверки хэшей файлов через API VirusTotal.
- Разработка инструмента для анализа подозрительных URL и генерации отчётов.
- Создание Python-утилиты для анализа логов безопасности, проверки хэшей через VirusTotal API и формирования отчета в формате CSV.
- Установка и базовая настройка Linux-сервера для корпоративной инфраструктуры.
- Разработка политики информационной безопасности для интернет-магазина.

- Настройка централизованного управления пользователями и правами доступа в домене.
- Настройка и автоматизация резервного копирования данных на сервере.
- Анализ и классификация уязвимостей корпоративной ИТ-инфраструктуры с использованием CVSS.
- Настройка межсетевого экрана и системы предотвращения вторжений для веб-сервера.
- Проведение OSINT-расследования по заданной компании с анализом цифровых следов.
- Разработка фишинговой рассылки и анализ её эффективности в корпоративной среде.
- Настройка системы сбора и корреляции событий безопасности с использованием ELK Stack.
- Проведение анализа сетевого трафика и выявление аномалий с использованием Wireshark и Zeek.
- Внедрение системы управления инцидентами и реагирования с использованием SOAR-платформы.
- Проведение тестирования на проникновение в изолированной среде с использованием Kali Linux и Metasploit.
- Анализ защищённости веб-приложения с помощью Burp Suite и OWASP ZAP.
- Разработка Bash- или Python-скрипта для автоматизации задач администрирования и мониторинга.
- Проведение аудита ИБ по чек-листу ФСТЭК и составление отчёта.
- Составление и оформление профессионального резюме
- Подготовка и прохождение собеседования с использованием методики STAR.
- Разработка плана реагирования на инциденты информационной безопасности для малого бизнеса.
- Выполнение расследования инцидента информационной безопасности с анализом логов и построением отчёта.
- Создание виртуальной инфраструктуры для моделирования атак и защиты с помощью VirtualBox и Docker.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Виртуальные машины с предустановленными дистрибутивами Kali Linux и Windows для практических занятий.

Лицензионное ПО:

- Справочно-правовые системы (КонсультантПлюс, Гарант)
- Специализированные OSINT-инструменты (Shodan)
- Программы для анализа сетевого трафика (Wireshark)
- Инструменты для тестирования на проникновение (Metasploit, Burp Suite)

Серверное оборудование для развертывания учебных стендов и симуляции атак.

Специализированное ПО для SOC-аналитики (например, Splunk или ELK Stack).

Инструменты для создания и управления виртуальными лабораториями (например, VMware vSphere).