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 повышения квалификации
«Специалист по OSINT»

Форма обучения: очная (с применением исключительно дистанционных образовательных технологий и электронного обучения)

Срок реализации: 34 недели

Режим занятий: от 7 до 10 академических часов в неделю

Объем программы: 262,5 академических часа

Авторы программы: Павел Банников

г. Москва, 2026 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Характеристики программы:

Дополнительная профессиональная программа повышения квалификации «Специалист по OSINT» (далее - Программа) разработана в соответствии стребованиями:

- 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**.
- Профессиональный стандарт **«Специалист по управлению рисками»** (код **08.018**) — утверждён Приказом Министерства труда и социальной защиты Российской Федерации от **18 апреля 2025 г. № 264н**, действует в период с **01.09.2025 по 01.09.2031**.
- Профессионального стандарта **«Редактор средств массовой информации»** (код **11.006**) — утверждён Приказом Министерства труда и социальной защиты Российской Федерации от **4 августа 2014 г. № 538н**;

- 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:

Основная цель вида профессиональной деятельности слушателей — выполнение прикладного анализа информации из открытых источников (OSINT) в интересах

обеспечения информационной и корпоративной безопасности, снижения рисков и поддержки управленческих решений, включая:

- выявление, сбор, верификацию и систематизацию сведений о лицах, организациях, цифровых артефактах, событиях и связях на основе общедоступных источников;
- оценку достоверности данных, выявление манипуляций, фейков и репутационных угроз, формирование доказательной базы в пределах компетенций и допустимых методов;
- выявление «красных флагов», потенциальных угроз, уязвимостей и аномалий (в том числе связанных с утечками данных, поддельными личностями/документами, мошенничеством, конфликтом интересов);
- подготовку структурированных аналитических материалов (отчётов, справок, таймлайнов, карт связей/активности) для практических сценариев (кибербезопасность и корпоративная безопасность, HR-проверки, бизнес-проверки/комплаенс, журналистские и юридические задачи);
- обеспечение правомерности, этичности и информационной безопасности процесса исследования (минимизация цифрового следа, защита данных, соблюдение ограничений по персональным данным и режимам доступа к информации).

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: уверенное пользование компьютером и браузером, базовая цифровая грамотность, готовность соблюдать правила безопасной работы с данными и этические принципы. Специальных технических знаний (программирование, администрирование) не требуется. Программа ориентирована на слушателей, достигших 18 лет, и предназначена для:

- специалистов по кибербезопасности и корпоративной безопасности;
- журналистов и исследователей;
- сотрудников органов и служб безопасности;
- HR и рекрутеров;
- частных детективов;
- адвокатов и юридических практиков;
- маркетологов и аналитиков;
- предпринимателей и бизнес-руководителей;
- инвесторов;
- государственных служащих;
- исследователей и учёных;
- иных специалистов, которым требуется проверка людей/компаний и оценка рисков по открытым данным.

1.4. Объем программы (трудоемкость): общая трудоемкость 262,5 академических часов.

1.5. Срок освоения программы - 34 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 дополнительной профессиональной программы повышения квалификации «Специалист по OSINT» является формирование и развитие у слушателей профессиональных компетенций, необходимых для выполнения полного цикла OSINT-исследования (разведки по открытым источникам) в прикладных задачах информационной и корпоративной безопасности, HR-проверок, бизнес-аналитики, журналистских и юридических расследований, с соблюдением правовых, этических и технических требований к работе с данными.

2.2. Задачи программы

Для достижения цели Программа предусматривает решение следующих задач:

1. **Сформировать методологическую основу OSINT-исследований**: понимание места OSINT среди видов разведки, логики полного цикла исследования, этапов постановки задачи, построения гипотез, сбора и проверки данных, формулирования выводов и рекомендаций.
2. **Обеспечить освоение практик операционной безопасности (OPSEC) при работе с источниками**: организация безопасной рабочей среды, минимизация цифрового следа, защита доступов, безопасное хранение и шифрование материалов исследования, создание и поддержание альтернативной цифровой личности (легенды).
3. **Сформировать правовую и этическую грамотность в работе с открытыми данными**: понимание допустимых источников и действий, ограничений при работе с персональными данными, требований к хранению и использованию материалов, принципов ответственности и профессиональной этики.
4. **Развить навыки фактологического и критического мышления**: оценка надежности источников, выявление когнитивных искажений, применение базовых подходов фактчекинга, аргументация выводов, фиксация методологии и воспроизводимость результатов.
5. **Сформировать прикладные навыки SOCMINT**: поиск и систематизация цифрового следа человека по идентификаторам (ФИО, e-mail, username, номер телефона), сопоставление профилей и связей, выявление несоответствий и репутационных рисков.
6. **Сформировать прикладные навыки IMINT/GEOINT**: верификация изображений и видео, поиск первоисточников, анализ метаданных, выявление признаков монтажа и AI-подделок, базовая геолокация и определение времени съемки.

7. **Сформировать прикладные навыки FININT и бизнес-разведки**: сбор и анализ открытых данных о компаниях и сделках, работа с реестрами и отчетностью, анализ закупок и тендерной документации, выявление взаимосвязей, аномалий и «красных флагов».
8. **Научить оформлять результаты исследования в профессиональном формате**: подготовка структурированных аналитических отчетов и справок, формирование доказательной базы (с фиксацией источников и шагов), визуализация связей/активности (карты, графы, таймлайны) под конкретный прикладной сценарий.
9. **Сформировать навыки организации цифрового архива и управления материалами исследования**: построение системы хранения, каталогизации и поиска материалов (Obsidian/аналоги, PDF-инструменты), обеспечение сохранности, резервного копирования и контроля доступа.
10. **Освоить корректное применение ИИ-инструментов в OSINT-работе**: использование ИИ-сервисов и NotebookLM для резюмирования и первичной сортировки массивов данных, построения майндмепов/таймлайнов, при обязательном учете ограничений ИИ и последующей верификации результатов.
11. **Обеспечить формирование интегральной компетентности через итоговый проект**: выполнение комплексного OSINT-исследования на основе минимального исходного артефакта с применением методов SOCMINT, IMINT/GEOINT, FININT и фактчекинга, оценкой рисков и подготовкой итогового аналитического отчета.

3. УЧЕБНЫЙ ПЛАН

№	Название модуля / темы	Всего акад. часов	Лекции	Практика	Форма контроля
1	**Модуль 1. Введение в OSINT**	7	4	3	Тест
2	**Модуль 2. Техническая безопасность и анонимность**				
2.1	Пароли, доступы, антивирусы	7	2	5	Практическое задание
2.2	Хранение и шифрование данных	7	2	5	Практическое задание
2.3	Цифровой отпечаток и конфиденциальные браузеры	7	2	5	Практическое задание

2.4	Альтернативная цифровая личность	7	2	5	Практическое задание
2.5	Итоговое задание модуля	8	2	6	Практическое задание
3	**Модуль 3. Юридический аспект OSINT**	7	3	4	Практическое задание
4	**Модуль 4. Основы фактологического мышления**				
4.1	Гипотезы и исследовательские задачи	7	2	5	Практическое задание
4.2	Сбор и первичный анализ данных	7	2	5	Практическое задание
4.3	Ошибки восприятия и искажения	7	2	5	Практическое задание
4.4	Итоговое задание модуля	8	2	6	Практическое задание
5	**Модуль 5. SOCMINT**				
5.1	Поиск по имени и соцсетям	7,5	2	5,5	Практическое задание
5.2	Поиск по e-mail	7,5	2	5,5	Практическое задание
5.3	Username и номер телефона	7,5	2	5,5	Практическое задание
5.4	Итоговое задание модуля	9	2	7	Практическое задание
6	**Модуль 6. IMINT / GEOINT**				

6.1	Обратный поиск изображений и поиск по лицам	8	2	6	Практическое задание
6.2	Анализ метаданных фото и видео	8	2	6	Практическое задание
6.3	Проверка на монтаж и AI	8	2	6	Практическое задание
6.4	Геолокация фото и видео	8	2	6	Практическое задание
6.5	Итоговое задание модуля	10	2	8	Практическое задание
7	**Модуль 7. Финансовая и бизнес-разведка (FININT)**				
7.1	Профиль компании	9	2	7	Практическое задание
7.2	Анализ тендерной документации	9	2	7	Практическое задание
7.3	Иностранные компании и реестры	9	2	7	Практическое задание
7.4	Медиа-поиск и связи персон	9	2	7	Практическое задание
7.5	Итоговое задание модуля	10	2	8	Практическое задание
8	**Модуль 8. ИИ и цифровой архив**				
8.1	ИИ-инструменты для анализа	7	2	5	Практическое задание
8.2	Организация цифрового архива	7	2	5	Практическое задание

8.3	Итоговое задание модуля	8	2	6	Практическое задание
9	**Модуль 9. Итоговый проект курса**	42	2	40	Практическое задание
10.	**ИТОГО:**	262,5	61	201,5	

4. СОДЕРЖАНИЕ УЧЕБНОГО ПЛАНА

Модуль 1: Введение в OSINT

Модуль знакомит студентов с основами разведки на основе открытых источников, областями её применения, карьерными возможностями и структурой курса. Студенты поймут место OSINT среди других видов разведки и сформируют общее представление о навыках, которые будут развивать.

- Основные направления разведки и место OSINT среди них.
- Области применения OSINT-навыков: аналитика, кибербезопасность, бизнес, журналистика, корпоративная безопасность.
- Карьерные траектории и смежные специальности в сфере OSINT.
- Ключевые навыки, формируемые в курсе: технические, аналитические, исследовательские.
- Логика и структура курса, взаимосвязь модулей.
- Цель, формат и критерии оценки итогового проекта.
- Организационные правила курса и принципы эффективного тайм-менеджмента.

Итоговое задание: студенты выполняют подготовку к последующему обучению и самопроверку по чек-листу

Модуль 2: Техническая безопасность и анонимность

Модуль посвящён подготовке безопасной технической среды для OSINT-исследований. Студенты научатся защищать доступы, минимизировать цифровой след, безопасно хранить данные и создавать альтернативную цифровую личность.

Тема 1. Пароли, доступы и цифровая гигиена

- Основы операционной безопасности (OPSEC) для OSINT-исследователя.
- Создание и хранение надёжных паролей с использованием менеджеров.
- Важность двухфакторной аутентификации и аппаратных токенов.
- Поддержание цифровой гигиены устройства: антивирусы, обновления, проверка файлов.

Тема 2. Хранение и шифрование данных

- Принципы безопасного хранения информации и резервного копирования.
- Использование встроенных инструментов шифрования: BitLocker и FileVault.
- Работа с зашифрованными контейнерами в VeraCrypt.
- Безопасное облачное хранение и обмен файлами через Proton Drive.
- Комбинация локального и облачного шифрования для комплексной защиты.

Тема 3. Безопасное поведение при сборе данных

- Разделение личной и исследовательской активности. Концепция безопасной рабочей среды.
- Анализ и минимизация цифрового отпечатка браузера.
- Настройка конфиденциальных браузеров (Brave, DuckDuckGo) для OSINT-работы.
- Создание убедительной альтернативной личности (легенды) и принципы легендирования.
- Использование AI-инструментов для генерации деталей легенды.
- Создание и настройка анонимных аккаунтов в соответствии с легендой.
- Базовые методы сокрытия цифрового отпечатка: VPN, расширения для приватности.

Итоговое задание модуля: Подготовка безопасной рабочей среды. Студент предоставляет отчёт по чек-листу (настройки, инструменты, скриншоты), подтверждающий готовность к OSINT-работе.

Модуль 3: Юридический аспект при сборе данных

Модуль даёт понимание правовых рамок OSINT-деятельности. Студенты изучат общие принципы, особенности регулирования в РФ и других странах, а также этические дилеммы, возникающие при работе с открытыми данными.

- Различие между «открытым источником» и «законным использованием данных».
- Категории источников: открытые, условно открытые и недопустимые.
- Особенности работы с персональными данными в РФ.
- Юридические ограничения на использование технических средств (прокси, анонимизация).
- Ключевые различия в регулировании OSINT в США и странах ЕС.
- Принципы трансграничной передачи и хранение данных.
- Этические основы ответственного OSINT-исследования.
- Работа с чувствительной информацией и принятие решений в «серых зонах».

Итоговое задание модуля: Студенты решают задачи, представленные в форме кейс-тестов на оценку допустимости действий в разных юрисдикциях и с точки зрения этики.

Модуль 4: Основы фактологического мышления

Модуль формирует критическое мышление, необходимое для работы с информацией. Студенты научатся ставить исследовательские задачи, оценивать источники, выявлять когнитивные искажения и выполнять базовый фактчекинг.

Тема 1. Гипотезы и исследовательские задачи

- Принципы критического фактологического мышления.
- Основы научного метода: факт, гипотеза, нулевая гипотеза, доказательство.
- Формулирование и уточнение исследовательской задачи в рамках цикла OSINT.
- Основы статистической грамотности для оценки достоверности данных.

Тема 2. Сбор и первичный анализ данных

- Критерии оценки надёжности и заинтересованности источника.
- Метод IMVAIN (ИНФОРМ) для первичной оценки источников.
- Система оценки источников ADM code, её особенности и применение.

Тема 3. Ошибки восприятия и искажения

- Природа когнитивных искажений и их влияние на анализ.
- Основные искажения, мешающие исследователю: предвзятость восприятия, ошибка выжившего, эффект Баадера-Майнхоф.
- Типичные логические ошибки и уловки в аргументации.

Тема 4. Фактчекинг и проверка данных

- Фактчекинг как профессиональный метод и его стандарты.
- Алгоритм проверки данных: от поиска утверждений до верификации.
- Базовые инструменты и методы фактчекинга без использования глубокого поиска.

Итоговое задание модуля: Мини-исследование на основе наблюдения. Студент выполняет полный цикл: от постановки задачи и гипотезы до сбора данных, фактчекинга и оформления аналитического мини-отчёта. Проверка — ручная, по серии скриншотов этапов работы.

Модуль 5: SOCMINT (Социальный OSINT)

Модуль посвящён поиску и анализу цифрового следа человека в социальных сетях и интернете. Студенты научатся находить аккаунты по имени, e-mail, username и номеру телефона, систематизировать данные и строить первичный цифровой профиль.

Тема 1. Поиск по имени

- Ручной поиск и использование доркинга для сбора базовой биографии.
- Фиксация и систематизация данных на ранних этапах с помощью OsintTracker.
- Использование кастомных поисковых движков для целенаправленного поиска в соцсетях.
- Построение карты активного цифрового следа и визуализация присутствия объекта в сети.

Тема 2. Поиск по почте

- E-mail как уникальный цифровой идентификатор.

- Проверка адреса через базы утечек (HaveIBeenPwned) и анализ слитой информации.
- Верификация e-mail и поиск связанных аккаунтов через сервисы вроде HunterIO и Epieos.
- Поиск доменов, зарегистрированных на целевой e-mail, через Whois.
- Интеграция почтовых данных в общий цифровой профиль.

Тема 3. Работа с Username

- Никнейм как повторяющийся цифровой след.
- Поиск аккаунтов по username через агрегаторы: WhatsMyName и WhoAmI.
- Анализ и сопоставление найденных профилей.

Тема 4. Проверка по номеру телефона

- Сценарии применения проверки номера в расследованиях.
- Ручной поиск следов активности номера в интернете.
- Использование специализированных сервисов: GetContact, Truecaller, White/Yellow Pages, ThisNumber.
- Фиксация и анализ полученных телефонных данных.

Итоговое задание модуля: На основе ФИО и e-mail соискателя студенты должны собрать активный цифровой след, проверить соответствие резюме, выявить потенциальные риски и сформировать цифровой профайл с выводом для HR.

Модуль 6: IMINT / GEOINT

Модуль учит анализировать визуальный контент: проверять изображения и видео на подлинность, искать первоисточники, определять место и время съёмки, а также работать со спутниковыми снимками.

Тема 1. Обратный поиск по изображению и лицам

- Обратный поиск через Google Images и Яндекс.Картинки для нахождения первоисточника.
- Поиск по лицам с использованием специализированных сервисов: PimEyes, Facepair.
- Использование AI-инструментов и кастомных GPT для расширенного поиска по изображениям.

Тема 2. Анализ метаданных

- Извлечение и анализ метаданных из файлов с помощью ОС и веб-инструментов.
- Использование сервисов Forensically, FindExif, Visual Origins Detector.
- Работа с метаданными видео через YouTube Data Viewer и MW Metadata.

Тема 3. Проверка на монтаж и AI-подделку

- Выявление признаков монтажа в фото и видео с помощью инструментов (Forensically, InVid).

- Анализ артефактов и нестыковок для обнаружения недобросовестного редактирования.
- Проверка контента на дипфейки с использованием инструментов вроде Image Whisperer и Deepfake-o-meter.

Тема 4. Геолокация фото и видео

- Методы геолокации с использованием визуальных ключей и карт (Google Maps, Яндекс.Карты).
- Работа с историческими спутниковыми снимками в Google Earth Pro и Sentinel Hub.
- Определение времени съёмки по солнцу и тени с помощью SunCalc.
- Геопоиск контента в социальных сетях через InstaHunt и Twitter.
- Применение нейросетей (Gemini, SPOT, Pickarta) для геолокации и анализа изображений.

Итоговое задание модуля: Полный цикл IMINT-анализа предоставленного визуального материала. Студент проводит обратный поиск, проверку метаданных, геолокацию, анализ на монтаж и формирует аналитический отчёт с выводами.

Модуль 7: Финансовая и бизнес-разведка (FININT)

Модуль посвящён сбору и анализу открытых данных о компаниях. Студенты научатся строить профили компаний, анализировать тендеры, выявлять связи и аномалии, а также работать с международными реестрами.

Тема 1. Построение профиля компании

- Сбор официальных данных о публичных и непубличных компаниях РФ через агрегаторы (Checko, Руспрофайл) и реестры.
- Анализ интеллектуальной собственности: патенты, товарные знаки.
- Изучение финансовой отчётности через сервис bo.nalog.gov.ru.
- Медиапоиск и построение карты связей ключевых сотрудников и руководителей.

Тема 2. Анализ тендерной документации

- Работа с открытыми источниками данных о госзакупках.
- Выявление красных флагов и признаков недобросовестной конкуренции в тендерах.
- Анализ документации частных закупок.

Тема 3. Сбор данных об иностранных компаниях

- Особенности работы с международными реестрами и агрегаторами.
- Использование глобальных баз данных: OpenCorporates, OpenOwnership.
- Стратегии поиска в реестрах США (California Secretary of State, Nevada SilverFlume) и Великобритании (Companies House).

Тема 4. Выводы и отчетность

- Формирование структурированного аналитического отчёта по результатам финансового OSINT-исследования.
- Визуализация связей и аномалий.

Итоговое задание модуля: Студенты выполняют комплексный анализ компании-конкурента. Построение профиля компании, анализ тендерной активности, выявление связей и потенциальных рисков. Подготовка отчёта с графом связей.

Модуль 8: ИИ-инструменты и организация цифрового архива

Модуль знакомит с применением искусственного интеллекта для анализа данных и учит выстраивать структурированную систему хранения материалов исследования для эффективной работы и воспроизводимости результатов.

Тема 1. ИИ-инструменты для сбора и анализа данных

- Роль и ограничения ИИ в OSINT-исследованиях.
- Использование ИИ для резюмирования, анализа и генерации гипотез.
- Создание кастомных ИИ-машин с системными промтами (Perplexity).
- Работа с NotebookLM для анализа локальных данных, создания таймлайнов и майндмепов.

Тема 2. Организация цифрового архива

- Принципы структурированного хранения информации и важность бэкапов.
- Организация файлового архива, работа с PDF-документами.
- Использование Obsidian для ведения заметок, построения графов связей и анализа информации.

Итоговое задание модуля: Создание и демонстрация организованного рабочего пространства. Студент предоставляет доступы/скриншоты структурированного архива в Obsidian, примеры работы с ИИ-инструментами и документацию по логике организации данных.

Итоговый проект курса

Финальный проект объединяет знания и навыки, полученные во всех модулях курса. Студенты выполняют комплексное OSINT-исследование, начиная с минимальных исходных данных, и готовят развернутый аналитический отчет.

- Построение полного цифрового профиля лица на основе минимального исходного артефакта (например, фотографии).
- Применение методологий и инструментов SOCMINT, IMINT/GEOINT, FININT и фактчекинга.
- Обеспечение анонимности и безопасности на протяжении всего исследования.
- Проверка подлинности информации, выявление «красных флагов» и построение карты связей.
- Формирование структурированного аналитического отчёта с выводами и рекомендациями для практической задачи (HR, бизнес, расследование).

5. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Программа повышения квалификации направлена на совершенствование профессиональных компетенций слушателей в сфере **сбора, мониторинга, анализа и документирования информации из открытых источников (OSINT)** для решения задач информационной безопасности и управления рисками.

Преемственность с ФГОС ВО 10.03.01 «Информационная безопасность» (приказ Минобрнауки РФ от 01.12.2016 № 1515)
В рамках программы совершенствуются (под цели OSINT) следующие компетенции из ФГОС:

Общекультурные компетенции (ОК):
ОК-4 «способностью использовать основы правовых знаний в различных сферах жизнедеятельности».
ОК-5 «способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия».
ОК-6 «способностью работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия».
ОК-8 «способностью к самоорганизации и самообразованию».

Общепрофессиональные компетенции (ОПК):

ОПК-4 «способностью использовать основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией и работы с информацией в глобальных компьютерных сетях».
ОПК-5 «способностью использовать нормативные правовые акты в профессиональной деятельности».
ОПК-7 «способностью определять информационно-технологические ресурсы, подлежащие защите, угрозы безопасности информации и возможные способы реализации угроз».

Профессиональные компетенции (ПК):

ПК-8 «способностью разрабатывать техническую документацию и нормативные методические документы в области информационной безопасности».
ПК-9 «способностью изучать научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности…».
ПК-13 «способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер, направленных на обеспечение информационной безопасности…».

В результате основания программы, слушатели:

Будут знать:

(06.033) «**Основные методы и средства обеспечения информационной безопасности**».
(06.033) «**Методики определения угроз безопасности информации, обрабатываемой автоматизированной системой**».
(06.033) «**Требования нормативных правовых актов и документов по защите информации**».
(06.013) «**Методы поиска информации в сети Интернет**».
(08.018) «**Методология и принципы построения системы управления рисками несоответствия законодательству Российской Федерации и регуляторным требованиям**».

Будут уметь:

(06.013) «**Искать информацию о новых научных разработках… по различным источникам**».
(06.013) «**Осуществлять мониторинг информационной среды**».
(06.013) «**Анализировать и обобщать информацию**».
(06.033) «**Классифицировать и оценивать угрозы безопасности информации…**».
(06.033) «**Определять и выбирать методы, средства защиты информации, вырабатывать предложения по применению методов и средств защиты информации**».
(06.033) «**Оценивать информационные риски по результатам обследования автоматизированной системы**».
(08.018) «**Использовать статистические и математические методы для обработки и визуализации массивов данных**».

Будут владеть:

(06.033) «**Систематизация результатов проведенных исследований, составление аналитической записки**».
(06.033) «**Подготовка отчетных материалов по результатам обследования автоматизированной системы**».
(06.013) «**Подготовка информационно-аналитических материалов…**».
(08.018) «**Формирование стратегической интегрированной системы управления рисками…**» (в части аналитического сопровождения и отчётности по рискам).

6. 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 – 34 недели – 262,5 академ. часов. Начало обучения – по мере наборагруппы. Режим занятий – от 7 до 10 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 обучения группы	34	265,5	**от 7 до 10 академических часов в неделю** [1]

7. ФОРМЫ АТТЕСТАЦИИ. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

7.1. Общие положения

Оценка качества освоения дополнительной профессиональной программы повышения квалификации «Специалист по OSINT» осуществляется для подтверждения достижения планируемых результатов обучения и сформированности профессиональных компетенций, необходимых для выполнения полного цикла OSINT-исследования в прикладных сценариях (безопасность, журналистика, HR, бизнес-анализ, юридическая практика).

Оценка качества освоения Программы включает:

- **текущий контроль** по отдельным урокам и модулям;
- **итоговую аттестацию** в форме защиты итогового проекта.

7.2. Формы текущего контроля

Текущий контроль осуществляется в течение всего периода обучения и проводится в следующих формах, предусмотренных Программой:

- **тестирование** по итогам отдельных уроков и модулей;
- **выполнение практических заданий и лабораторных работ** по темам и модулям (в соответствии с учебно-тематическим планом);
- **проверка отчётных материалов по практическим заданиям**, включая фиксацию хода исследования, приложений и подтверждающих материалов (например, чек-листы, скриншоты этапов работы, ссылки на источники, материалы анализа);
- **оценка соблюдения требований безопасности, правовых и этических норм** при выполнении практических работ и подготовке результатов.

Особое внимание при текущем контроле уделяется практическим результатам: корректности применения инструментов и методов OSINT, обоснованности выводов,

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

качеству фиксации и документирования хода исследования, соблюдению требований безопасной работы с данными, правовых и этических ограничений.

7.3. Итоговая аттестация

Итоговая аттестация проводится в форме **защиты финального проекта** (Модуль 9), предусматривающего выполнение полного OSINT-исследования с построением цифрового профиля объекта, визуализацией связей и подготовкой аналитического отчёта.

Итоговый проект включает:

- постановку задачи и определение границ исследования;
- формирование гипотез и планирование шагов исследования;
- сбор, проверку и анализ информации из открытых источников с применением методологических подходов и инструментов SOCMINT, IMINT/GEOINT, FININT и фактчекинга;
- фиксацию методологии и источников, обеспечение воспроизводимости результатов;
- визуализацию результатов (карта связей и активности, таймлайн и иные материалы, предусмотренные логикой кейса);
- выявление рисков и «красных флагов», формирование выводов и рекомендаций;
- оформление результатов в виде структурированного аналитического отчёта, пригодного для практических задач.

7.4. Критерии оценки качества освоения Программы

Оценка качества освоения Программы проводится по совокупности критериев, отражающих практическую применимость сформированных компетенций:

1. **Корректность постановки исследовательской задачи** и логика проведения исследования (гипотезы, границы, последовательность шагов).
2. **Полнота и релевантность собранных данных** из открытых источников, корректность их систематизации.
3. **Достоверность и проверяемость результатов** (фактчекинг, сопоставление источников, аргументация выводов).
4. **Корректность применения инструментов и методов OSINT** (SOCMINT, IMINT/GEOINT, FININT, аналитические подходы).
5. **Соблюдение требований безопасности при работе с данными** (защита материалов исследования, минимизация цифрового следа, корректная организация рабочей среды).
6. **Соблюдение правовых и этических норм** при сборе и использовании информации.
7. **Качество документирования и оформления результата** (структура отчёта, фиксация источников, воспроизводимость, визуализация, ясность выводов и рекомендаций).

7.5. Условия допуска к итоговой аттестации и выдаче удостоверения

К итоговой аттестации допускаются слушатели, которые:

- **выполнили все практические задания и лабораторные работы**, предусмотренные Программой;
- прошли **тестирование** по итогам отдельных уроков и модулей;
- представили результаты практических работ в установленном формате, с необходимыми подтверждающими материалами и фиксацией хода исследования.

Невыполнение хотя бы одного обязательного практического задания, лабораторной работы или не прохождение предусмотренного тестирования образует академическую задолженность по Программе.

Удостоверение о повышении квалификации установленного образца выдается только при одновременном выполнении условий:

- **отсутствие академической задолженности** (выполнены все практические работы и тестирования, предусмотренные Программой);
- **успешная защита итогового проекта**.

7.6. Фиксация результатов аттестации

Результаты текущего контроля и итоговой аттестации фиксируются в оценочных материалах Программы и подтверждаются материалами, предоставленными слушателем в рамках выполнения практических заданий и итогового проекта.

Особое внимание уделяется практическим результатам: корректности применения инструментов и методов OSINT, обоснованности выводов, соблюдению требований безопасности, правовых и этических норм, а также качеству фиксации и документирования хода исследования. Выполнение практических заданий предполагает получение обратной связи от преподавателя и сравнение результатов с эталонными решениями.

8. ИТОГОВЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

По завершении курса слушатели будут готовы к практической работе в качестве OSINT-аналитиков и специалистов, использующих методы разведки по открытым источникам в профессиональной деятельности (безопасность, журналистика, HR, бизнес-анализ, юридическая практика, расследования).

Слушатели будут обладать следующими компетенциями:

- пониманием полного цикла OSINT-исследования — от постановки задачи и формулирования гипотез до подготовки аналитического отчёта;
- умением безопасно организовывать рабочую среду и хранение данных при работе с открытыми источниками;

- навыками сбора и анализа цифрового следа человека (SOCMINT): имя, e-mail, username, телефоны, аккаунты, контент и связи;
- способностью проверять и анализировать визуальные материалы (IMINT/GEOINT): изображения, видео, метаданные, геолокацию и время съёмки;
- умением проводить базовый финансовый и бизнес-анализ по открытым источникам (FININT);
- навыками фактологического мышления и фактчекинга, выявления искажений и «красных флагов»;
- способностью визуализировать результаты исследования (карты связей и активности) и формулировать обоснованные выводы и рекомендации;
- опытом документирования хода исследования и представления результатов в форме аналитического отчёта для заказчика или внутреннего использования.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Литература

Основная литература и методологии:

- **NIST SP 800-53 / ISO/IEC 27001** — стандарты информационной безопасности, разделы по управлению рисками и работе с инцидентами.
- **OSINT Framework** (от Джастина Нордхайна) — структурированное руководство по источникам и инструментам OSINT.
- **Дополнительные руководства:** «Открытый источник. Методы» (Хенк ван Эсс), методические материалы по фактчекингу и верификации источников.
- **Официальная документация** к операторам поисковых систем (Google, Яндекс) — справки по расширенным операторам поиска.

Официальная документация и руководства:

- **Документация по инструментам:** официальные руководства
- **Методические материалы** по анализу метаданных, геолокации и работе с открытыми реестрами.
- **Специализированные статьи и кейсы:** публикации в профильных изданиях по информационной безопасности и расследованиям — разбор применяемых методик.

Онлайн-ресурсы

Официальные ресурсы и стандарты:

- **Google Fact Check Tools / Верификатор Яндекса** — инструменты для проверки информации.
- **Have I Been Pwned** — сервис проверки данных в утечках.
- **Реестры Росстата, ФНС, ЕГРЮЛ** — официальные источники данных по юридическим лицам в РФ.
- **Сайты судов и госзакупок** (ФАС, ЕИС) — первоисточники для финансовой разведки.

- **Официальные порталы государственных услуг** — как источники открытых данных.

Обучающие платформы и виртуальные лаборатории:

- **Платформы для отработки навыков** с интерактивными заданиями по анализу данных и поиску информации.

Инструменты и репозитории:

- **GitHub-репозитории** с коллекциями OSINT-инструментов
- **Открытые базы данных:** Whois-сервисы, агрегаторы телефонов, поиск по изображениям.
- **Сервисы анализа метаданных**

Профессиональные сообщества и источники:

- **Отраслевые издания и блоги** по информационной безопасности и digital-исследованиям.
- **Специализированные форумы и сообщества** для обмена опытом в сфере работы с открытыми данными.
- **Каналы и ресурсы** с разбором легальных методик сбора и анализа информации.

10. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Практические задания и кейсы

1. **Подготовка среды и создание легенды.**
    - **Цель:** настроить безопасную среду для исследований и создать альтернативную цифровую личность.
    - **Ожидаемый результат:** рабочий профиль в OsintTracker, документированная легенда, отчёт по чек-листу безопасности.
2. **Фактчекинг публичного заявления.**
    - **Цель:** на основе утверждения публичного лица проверить его достоверность, используя научный метод и базовые инструменты.
    - **Ожидаемый результат:** мини-отчёт с пошаговым ходом проверки и обоснованным вердиктом.
3. **Построение цифрового профиля личности (SOCMINT).**
    - **Цель:** по ФИО и e-mail собрать активный цифровой след, проверить историю трудоустройства и выявить потенциальные репутационные риски.
    - **Ожидаемый результат:** цифровой профайл с картой аккаунтов, анализом связей и выводом для HR.
4. **Верификация изображения и геолокация (IMINT/GEOINT).**
    - **Цель:** проверить предоставленное фото/видео на подлинность, найти первоисточник и определить место съёмки.
    - **Ожидаемый результат:** аналитическая справка с подтверждёнными или опровергнутыми фактами, координатами и ссылками на доказательства.
5. **Анализ компании-конкурента (FININT).**

    - **Цель:** на основе открытых реестров, тендеров и медиа построить профиль компании, выявить связи и потенциальные «красные флаги».
    - **Ожидаемый результат:** отчёт с графом связей, анализом финансовых показателей и оценкой рисков.
6. **Итоговый практический проект (финальный кейс).**
    - **Цель:** выполнить полный цикл OSINT-исследования по заданному объекту (фото человека), интегрируя знания всех модулей.
    - **Ожидаемый результат:** комплексный аналитический отчёт с цифровым профилем, картой связей, фактчекингом, оценкой рисков и рекомендациями для заказчика.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Предустановленные шаблоны ОС для лабораторных работ по анонимности.

Программное обеспечение и инструменты:

- **Базовый набор:** менеджеры паролей (KeePass), браузеры для приватности, инструменты шифрования (VeraCrypt).
- **Сервисы подписки/доступа:** пробные или образовательные доступы к легальным платным сервисам.
- **Внутренний репозиторий:** сборник актуальных ссылок на бесплатные инструменты, базы данных и инструкции по их использованию.

Инфраструктура для сбора и хранения данных:

- Облачные диски с шифрованием или локальные зашифрованные хранилища для учебных материалов и отчётов.
- Система организации знаний (Obsidian, Notion) с шаблонами для структурирования исследований.

Средства коммуникации и поддержки:

- Закрытый учебный канал (чат) для обсуждения учебных вопросов и обмена опытом.
- FAQ и база знаний с типовыми решениями технических проблем, глоссарием терминов и библиотекой примеров отчётов.
- Система для проверки заданий с возможностью загрузки скриншотов и учебных отчётов.