Общество с ограниченной ответственностью

«Ти Хантер»

Утверждено

Генеральный директор

ООО «Ти Хантер»

_____ Смирнов Р.И.

Приказ № 13 от 24.05.2022 года

Дополнительная профессиональная программа повышения квалификации «Использование методов и приемов конкурентной разведки в деятельности правоохранительных органов и негосударственных структур безопасности»

срок обучения: 44 академических часа

Составители: Бедеров И.С.

Санкт-Петербург

2022

Оглавление

1. Пояснительная записка

Дополнительная профессиональная образовательная программа повышения квалификации «Использование методов и приемов конкурентной разведки в деятельности правоохранительных органов и негосударственных структур безопасности» составлена в связи с необходимостью внедрения современных методов работы с открытыми источниками информациями, а также большими данными, в целях выявления, предупреждения и расследования рисков для государства, граждан и коммерческих организаций. Программа предполагает получение новых компетенций, необходимых специалистам для профессиональной деятельности и повышение профессионального уровня в рамках имеющейся квалификации.

Программа предназначена для дополнительного профессионального образования лиц, имеющим высшее образование в соответствии с Федеральным государственным образовательным стандартом, имеющих не менее двух лет опыта практической работы в правоохранительных органах или негосударственных структурах безопасности. Программа также предназначена для дополнительного профессионального образования лиц, занятых в проведении журналистских расследований, операторов больших данных, аналитиков, специалистов по моделированию, сбору и анализу данных цифрового следа.

Сферы профессиональной деятельности специалистов:

— государственные правоохранительные органы;

— службы безопасности частных компаний;

— частные охранные и детективные организации;

— частные детективы, адвокаты, журналисты-расследователи, специалистов по моделированию, сбору и анализу данных цифрового следа;

— аналитики, операторы больших данных.

Дополнительная профессиональная образовательная программа повышения квалификации разработана в соответствии Профессиональными стандартами:

1. «Специалист по моделированию, сбору и анализу данных цифрового следа», утвержден приказом Минтруда России 09.07.2021 № 462н «Об утверждении профессионального стандарта «Специалист по моделированию, сбору и анализу данных цифрового следа».

2. «Специалист по конкурентному праву», утвержден приказом Министерства трудаи социальной защитыРоссийской Федерации от 16.09.2021 № 637н «Об утверждении профессионального стандарта "Специалист по конкурентному праву».

2. Цель реализации программы повышения квалификации

Получение современных знаний руководителями, сотрудниками и специалистами правоохранительных органов, частных служб безопасности, охранных и детективных агентств, частными детективами, адвокатами, журналистами-расследователями, аналитиками и операторами больших данных необходимых для повышения эффективности своей работы, формирование практических умений и навыков в области использования современных инструментов, методов и приемов работы.

3. Основные задачи программы повышения квалификации

Формирование у обучающихся комплексных навыков по использованию современных методов и приемов сбора, анализа, сопоставления и исследования данных в целях выявления, предупреждения и расследования правонарушений, рисков для коммерческих организаций, журналистской работы.

Описание перечня профессиональных компетенций в рамках имеющейся квалификации.

Программа направлена на освоение (совершенствование) следующих профессиональных компетенций:

- Подготовка данных цифрового следа для проведения анализа (ПК-5);

- Проектирование процесса сбора данных цифрового следа (ПК-6.1);

- Сбор и предварительный анализ данных о соответствии деятельности организации требованиям антимонопольного законодательства Российской Федерации (ПК-6.2).

В результате освоения Программы обучающийся должен знать:

— российское законодательство в области регулирования цифрового следа;

— российское законодательство в области обработки персональных данных;

— российское законодательство в области защиты интеллектуальной собственности;

— существующие в стране требования и ограничения;

— основные методы и приемы работы с данными;

— методы оценки качества данных в области информационных технологий;

— основные источники данных и программные продукты, предназначенные для работы с ними;

— международные договоры Российской Федерации, связанные с защитой конкуренции;

— экономические категории в конкурентном праве.

В результате освоения Программы обучающийся должен уметь:

— применять методы и приемы конкуретной разведки в своей профессиональной деятельности;

— использовать прикладные компьютерные программы для обработки данных;

— применять средства мониторинга для сбора и анализа цифрового следа;

— собирать идентифицирующие цифровые следы пользователей сети Интернет;

— анализировать локальные нормативные акты организации на соответствие требованиям антимонопольного законодательства Российской Федерации.

4. Категории слушателей

Категория обучающихся: Руководители, сотрудники и специалисты правоохранительных органов, частных служб безопасности, охранных и детективных агентств, частные детективы, адвокаты, журналисты-расследователи, аналитики и операторы больших данных.

Требования к слушателям:

Для успешного освоения Программы обучающиеся должны:

— иметь уровень образования не ниже уровня, требуемого для выполнения профессиональной деятельности;

— владеть понятийным аппаратом на уровне опытного пользователя персонального компьютера;

— обладать навыками анализа больших объемов неструктурированных данных;

— иметь представление об устройстве сети Интернет;

— ориентироваться в правовой системе Российской Федерации и нормативном регулировании оперативно-розыскной деятельности, частной детективной и охранной деятельности, защиты информации и персональных данных;

— знать основы математического анализа, информационных технологий;

— знать основы делопроизводства и электронного представления доказательной базы (eDiscowery);

— уметь работать с универсальным и специальным программным обеспечением, используемое в конкурентной разведке.

5. Содержание программы

Учебный план Программы повышения квалификации

«Использование методов и приемов конкурентной разведки в деятельности правоохранительных органов и негосударственных структур безопасности»

Срок обучения – 44 академических часа.

Форма обучения – без отрыва от работы.

Занятия проводятся в группах до 16 человек.

Промежуточная аттестация в данной программе не предусмотрена, по окончании обучения проводится итоговая аттестация в форме зачета.

№	Название раздела	Всего часов	В том числе	
			Лекции	Практическое занятие
1	Правовое и техническое обеспечение конкурентной разведки	14	10	4
2	Программные решения в конкурентной разведке	14	10	4
3	Основные методы и приемы конкурентной разведки	14	8	6
Итоговая аттестация (зачет)		2		
Итого:		**44**	18	14

Календарный учебный график

Неделя	1				2				3				
Дни													
Лекции	2	2	3	3	3	2	3	2	2	2	2	2	Зачет
Практические занятия	-	2	1	1	1	2	1	1	2	2	2	-	2

Срок освоения программы составляет 44 часа из них 18 часа лекционных занятий, 14 практических, 2 часа итоговая аттестация (зачет)

Режим занятий: 4 дня в неделю не более 4 академических часов.

Академический час – 45 минут. Предусмотрены перерывы по 5 минут между часами, по 10 минут между парами.

Форма обучения: без отрыва от работы. Обучение осуществляется круглогодично по мере набора группы.

Итоговая аттестация проводится в форме зачета.

6. Рабочая программа программы повышения квалификации

Тематический план программы «Использование методов и приемов конкурентной разведки в деятельности правоохранительных органов и негосударственных структур безопасности»

№	Название темы	Всего часов	Лекционные занятия	Практические занятия
1	**Правовое и техническое обеспечение конкурентной разведки**	**14**	**10**	**4**
1.1.	История появления конкурентной разведки и ее актуальность	2	2	-
1.2.	Правовая регламентация конкурентной разведки в России и мире	2	2	-
1.3.	Обработка персональных данных в рамках конкурентной разведки	2	2	-
1.4.	Основные виды и направления конкурентной разведки	4	2	2
1.5.	Обеспечение личной безопасности при работе в киберпространстве	4	2	2
2	**Программные решения в конкурентной разведке**	**14**	**10**	**4**
2.1.	Операционные системы для конкурентной разведки	1	1	-
2.2.	Расширения интернет-браузеров для конкурентной разведки	1	1	-
2.3.	Программные комплексы для конкурентной разведки	5	1	2
2.4.	Программное обеспечение с открытым исходным кодом (Opensource)	4	2	2
2.5.	Программное обеспечения для работы с банками данных	2	2	-
2.6.	Электронное представление материалов исследований (eDiscowery)	1	1	-
2.7.	Организация источников по конкурентной разведке (база знаний)	1	2	-
3	**Основные методы и приемы конкурентной разведки**	**14**	**8**	**6**
3.1.	Идентификация пользователей в информационно-телекоммуникационных сетях	1	0,5	-
3.2.	Идентификация пользователей социальных сетей	4	0,5	-
3.3.	Идентификация пользователей мессенджеров	4	0,5	-

3.4.	Идентификация владельцев криптовалютных кошельков	4	0,5	0,5
3.5.	Идентификация владельцев телефонных номеров	4	0,5	0,5
3.6.	Идентификация владельцев адресов электронной почты	4	0,5	0,5
3.7.	Идентификация владельцев ресурсов сети Интернет	4	0,5	0,5
3.8.	Сбор и исследование геолокационной информации в конкурентной разведке	2	1	1
3.9.	Исследование визуального контента (фото, видео) в конкурентной разведке	4	0,5	0,5
3.10.	Проведение исследований в сетях ограниченного доступа (даркнет)	4	1	1
3.11.	Логирование (фингерпринтинг) пользователей в конкурентной разведке	4	1	1
3.12.	Управление поисковой выдачей и общественным мнением (информационные войны)	4	1	0,5
4	**Итоговая аттестация (зачет)**	**2**	**-**	**-**
	Итого:	44	18	14

Кадровые условия реализации программы по разделам: Специалист, имеющий образование высшее педагогическое, стаж работы в области конкурентной разведки от 1 года до 3 лет.

6.1. Правовое и техническое обеспечение конкурентной разведки

Тема 1.1 "История появления конкурентной разведки и ее актуальность"

Что такое конкурентная разведка? Разведывательный цикл. Зарождение конкурентной разведки в конце XIV века. Использование методов и приемов конкурентной разведки в деятельности государственных разведок. Конкурентная разведка и появление промышленного шпионажа. Конкурентная разведка в эпоху развития информационно-телекоммуникационных технологий. Организация сообществ конкурентных разведчиков в России и мире. Разработка программных продуктов для автоматизации разведывательного цикла. Цели и задачи современной конкурентной разведки.

Тема 1.2 "Правовая регламентация конкурентной разведки в России и мире"

Отличие конкурентной разведки от промышленного шпионажа, оперативно-розыскной деятельности, государственной разведки и частной детективной деятельности. Статус и правовые основы конкурентной разведки в странах Запада и на постсоветском пространстве. Особенности использования конкурентной разведки в журналистской и оперативно-розыскной деятельности.

Тема 1.3 "Обработка персональных данных в рамках конкурентной разведки"

Закон о персональных данных РФ и его отличия от GDPR. Работа с общедоступными персональными данными. Открытые и условно открытые источники информации. Использование технических данных в рамках конкурентной разведки. Пассивные и активные мероприятия в рамках конкуретной разведки. Автоматизация конкурентной разведки. Особенности оформления и использования результатов работы в рамках конкурентной разведки.

Тема 1.4 "Основные виды и направления конкурентной разведки"

Пассивная и активная конкурентная разведка. Геопространственная конкурентная разведка (GeoINT), работа с людьми в конкурентной разведке (HumINT), исследование рекламных модулей (ADINT), аналитика больших данных, маркетинг рисков и возможностей. Расследовательская конкурентная разведка в деятельности журналистов, детективов, сотрудников правоохранительных органов и служб безопасности коммерческих организаций.

Тема 1.5 "Обеспечение личной безопасности при работе в киберпространстве"

Регламентация работы конкурентного разведчика. Использование анонимных аккаунтов и виртуальных личностей (аватаров). Использованием VPN и VPS при осуществлении конкурентной разведки. Анонимные

операционные системы. Настройки безопасности социальных аккаунтов, мессенджеров и электронной почты. Специализированные программные продукты для конкурентной разведки.

6.1.1. Методические материалы к разделу «Правовое и техническое обеспечение конкурентной разведки»

Тема 1.4 "Основные виды и направления конкурентной разведки"

Практическая часть представляет собой игру:

Слушателям предлагается разделиться по командам и сыграть в ролевую игру.

Участники:

1. Сотрудники службы безопасности
2. Журналист - расследователь/ частный детектив
3. Аналитик больших данных
4. Прокурор

Ход игры: Слушатели, в рамках обозначенных правовых норм, должны обозначить как они могли бы использовать методы конкурентной разведки, в свою очередь команда «Прокурор» должна выяснить как осуществляется конкретная работа в рамках конкурентной разведки и не нарушаются ли права и свободы граждан.

Тема 1.5 "Обеспечение личной безопасности при работе в киберпространстве"

Практическая часть представляет собой решение задач, например, расписать, как при расследовании защитить ход дела и сохранить секретность. Правовые основы использования технических аккаунтов, как обеспечить анонимность своей деятельности, получение доступа.

Дополнительно, выявление нарушений при обработке сбора данных, письменная работа с комментарием как простроить сервис, чтобы не нарушать закон, дискуссии на основании ответов слушателей.

6.2. Программные решения в конкурентной разведке

Тема 2.1 "Операционные системы для конкурентной разведки"

Основные термины и определения. Анонимные операционные системы для конкурентной разведки. Особенности настройки операционных систем, обеспечивающих конфиденциальность.

Тема 2.2 "Расширения интернет-браузеров для конкурентной разведки"

Основные термины и определения. Виды браузеров. Популярные расширения для браузеров, созданных на основе Chrome, для сбора и анализа данных. Поисковые машины. Расширенные операторы поиска.

Тема 2.3 "Программные комплексы для конкурентной разведки"

Основные термины и определения. Средства автоматизации процесса конкурентной разведки. Использование программных комплексов Maltego, Palantir, i2, Виток-OSINT, Охотник. Плюсы и минусы программных комплексов.

Тема 2.4 "Программное обеспечение с открытым исходным кодом (opensource)"

Основные термины и определения. Популярные программные продукты с открытым исходным кодом, применяемые в конкурентной разведке. Запуск и использование программных продуктов с открытым исходным кодом.

Тема 2.5 "Программное обеспечения для работы с банками данных"

Основные термины и определения. Релационные и нереляционные базы данных. Источники пополнения банков данных. Парсинг. Копирование информации с веб-ресурсов при помощи штатных средств компьютера. Использование таблиц. Программные продукты для работы с банками данных. Особенности поиска информации в банках данных.

Тема 2.6 "Электронное представление материалов исследований (eDiscowery)"

Основные термины и определения. Закрепление материалов, полученных в ходе конкуретной разведки. Доказательственность. Представление доказательной базы в электронном виде. Программные продукты для eDiscowery.

Тема 2.7 "Организация источников по конкурентной разведке (база знаний)"

Основные термины и определения. Подборки полезных источников и методик для конкуретной разведки. Программные и облачные решения для создания собственных подборок источников. Создание базы знаний - методов и приемов конкуретной разведки.

6.2.1. Методические материалы к разделу «Программные решения в конкурентной разведке»

Тема 2.3 "Программные комплексы для конкурентной разведки"

Практическая часть данного раздела представлена следующим образом:

Самостоятельная работа за компьютером и знакомство с программным обеспечением, с таким программным обеспечением как: Maltego, i2, Palantir, Виток-OSINT, ПК Охотник, ряд продуктов формата E**Discovery** .

В ходе практического занятия проводится подготовка отчета(комментариев) о плюсах и минусах программных продуктов.

Итог работы: рассмотрен интерфейс, функциональные характеристики, направления в которых применяются такие комплексы, использование комплексов для формирования доказательной базы и представления в органы дознания, следствия, суд.

Тема 2.4 "Программное обеспечение с открытым исходным кодом (opensource)"

Практическая часть данного раздела представлена следующим образом: слушателям необходимо запустить программное обеспечение, изучить основные функции, обеспечить корректную работу.

Итог практического занятия: рассмотрен интерфейс, функционал, направления в которых применяются такие комплексы, использование комплексов для формирования доказательной базы и представления в органы дознания, следствия, суд.

6.3. Основные методы и приемы конкурентной разведки

Тема 3.1 "Идентификация пользователей в информационно-телекоммуникационных сетях"

ID - уникальный идентификатор пользователя. Исследование фотографии, доменных имен, никнейма и имени пользователя. Поиск иной идентифицирующей информации о пользователе в сети Интернет. Подбор контактных данных. Перспективные методы и приемы идентификации пользователей.

Тема 3.2 "Идентификация пользователей социальных сетей"

Основные термины и определения. Принципы построения социальных сетей. Основные направления и приемы сбора данных о пользователях. Активные и пассивные приемы работы. Работа с большими данными. Исследования сообществ (групп и каналов) в социальных сетях. Рекомендуемые программные продукты. Нестандартные приемы идентификации.

Тема 3.3 "Идентификация пользователей мессенджеров"

Основные термины и определения. Принципы работы мессенджеров. Основные направления и приемы сбора данных о пользователях. Активные и пассивные приемы работы. Работа с большими данными. Исследования сообществ (групп и каналов) в социальных сетях. Рекомендуемые программные продукты. Нестандартные приемы идентификации.

Тема 3.4 "Идентификация владельцев криптовалютных кошельков"

Основные термины и определения. Особенности работы блокчейна. Основные направления и приемы сбора данных о пользователях. Работа с большими данными. Математические методы анализа открытых данных.

Исследование транзакций криптовалюты. Рекомендуемые программные продукты. Нестандартные приемы идентификации.

Тема 3.5 "Идентификация владельцев телефонных номеров"

Основные термины и определения. Принципы работы телефонных сетей. Основные направления и приемы сбора данных о номере телефона. Проверка активности телефонного номера. Активные и пассивные приемы работы. Работа с большими данными. Использование телефонного номера в качестве средства авторизации в различных сервисах. Рекомендуемые программные продукты. Нестандартные приемы идентификации.

Тема 3.6 "Идентификация владельцев адресов электронной почты"

Основные термины и определения. Принципы работы электронной почты. Основные направления и приемы сбора данных об адресе электронной почты. Служебные заголовки и трасировка. Активные и пассивные приемы работы. Работа с большими данными. Использование электронной почты в качестве средства авторизации в различных сервисах. Рекомендуемые программные продукты. Нестандартные приемы идентификации.

Тема 3.7 "Идентификация владельцев ресурсов сети Интернет"

Основные термины и определения. Принципы работы сети Интернет. Домены и хостинг. Регистрационные данные. Технологии, используемые в коде сайта. Рекламные идентификаторы. Архивные копии сайтов и их регистрационных данных. Анализ DNS. Поиск связанный сайтов. Преодоление защиты IP-адреса. Программные продукты, предназначенные для исследования ресурсов сети.

Тема 3.8 "Сбор и исследование геолокационной информации в конкурентной разведке"

Основные термины и определения. Источники геолокационной информации. Метаданные документов и геометки. Поиск геолокационной информации по контенту, содержащемуся в графическом файле. Сбор

геолокационной информации пользователей в режиме онлайн по открытым источникам. Рекомендуемые программные продукты.

Тема 3.9 "Исследование визуального контента (фото, видео) в конкурентной разведке"

Основные термины и определения. Фото и видеофорензика. Выявление признаков подделки контента. Исследование метаданных документов. Повышение качества контента. Моделирование контента. Отождествление лиц и объектов физического мира. Установления времени и места съемки. Рекомендуемые программные продукты. Нестандартные приемы исследования аудиовизуального контента.

Тема 3.10 "Проведение исследований в сетях ограниченного доступа (даркнет)"

Основные термины и определения. Виды даркнет-сетей. Виды ресурсов в даркнете. Анонимность в сетях даркнет. Поисковые машины, работающие в сетях ограниченного доступа. Методы и приемы проведения исследований в сетях даркнет. Рекомендуемые программные продукты.

Тема 3.11 "Логирование (фингерпринтинг) пользователей в конкурентной разведке"

Основные термины и определения. Принципы работы логера. Приемы маскировки логируемого контента. Логирование через электронную почту. Использование средств автоматизации логирования. Геологирование пользователей сети. Получение данных о социальных аккаунтах в рамках логирования. Исследование данных, полученных в результате логирования. Рекомендуемые программные продукты.

Тема 3.12 "Управление поисковой выдачей и общественным мнением (информационные войны)"

Актуальность информационных войн. Основные термины и определения. Принципы работы поисковых алгоритмов и поисковых машин. SEO/SERM -оптимизация контента и его продвижение. Формирование поисковой выдачи. Ботнеты. Массовое распространение контента по сети и среди пользователей социальных платформ. Мониторинг поисковой выдачи. Удаление недостоверной информации из сети. Рекомендуемые программные продукты.

6.3.1. Методические материалы к разделу «Основные методы и приемы конкурентной разведки»

Тема 3.4 "Идентификация владельцев криптовалютных кошельков"

Методические материалы к практическим занятиям по данному разделу представлены следующим образом:

ЗАДАНИЕ №1. У нас есть Биткоин-криптокошелек жертвы хакерской атаки, с которого 13.11.2020 г. были выведены активы (выбираем любой из криптокошельков ниже для варианта задания):

17jYxVgWXT8Pdf4cGGMmfzxNhFMiV1ZKdM

1NqAUpg6JMdtHph9MJEp5QUZu8snE9WVko

1FGfaB9ir8B7SiYTJzfXgowaZUfHPxj2Bj

1N9xRVSX4X6mvbqVNm62zxUXyFavBxGV2W

1zq7ro4im7KFUWnamszmb7CbBs5nZtYrE

14B3Suu4D4h4aHzxKXvRGK3JR2dUN9T818

1HccGqnCcAqpKpXiznQNo939TWFnSnoNEK

1L6VG1XbGpCFjCsdsFvsf9YBGVDhPbVCyx

15vLG7Tmn2XB9JYQfN6riYBHu2d1YCscwV

1CrkyDRSxWFgejRJbJTg1fZfdB5sMhfE47

Используя общедоступный инструментарий, установите когда, через какую площадку для обмена криптовалюты были выведены похищенные активы.

РЕШЕНИЕ ЗАДАНИЯ: похищенные активы изначально поступили на криптокошелек 1HWKvaEW31uhyHEreUHC98hqXAxxddA5CU, затем они были переведены на 1ByhxLj9x13k6mWa1VRyvyisZ1Nobkbi8J, с него - на 1N94ymqThLgaQ2EVaoJNR2JkshckqPufw8. Далее активы ушли на кошелек 15gynMvfVaamDpvJbPvSGESg9RfyJNXwS3, который по объему транзакций может иметь отношение к криптовалютной бирже, а именно "Binance".

Он также идентифицируется, как принадлежащий этой бирже рядом сервисов https://www.breadcrumbs.app/.

С кошелька 15gynMvfVaamDpvJbPvSGESg9RfyJNXwS3 активы были переведены (хэш 69c7b75757e07e9776f388fbffefb239db362d623e34894255e7a90e216887fe) на другой кошелек "Binance" 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s, который идентифицируется большинством сервисов, в т.ч. https://bitinfocharts.com/bitcoin/address/1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s или https://www.walletexplorer.com/wallet/Binance.com?from_address=1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s.

ОТВЕТ: Средства были выведены через криптовалютную биржу "Binance".

ЗАДАНИЕ №2. Вы планируете приобрести криптовалюту у физического лица. После сделки мы планируем положить криптовалюту на свой личный счет на криптобирже "Binance". Нам надо легальность происхождения активов на Биткоин-криптокошельке:

3JuLSLzwR1VuHG6LS2RN3xyA2U8KrobaeK

Используя общедоступный инструментарий, установите источники поступления криптовалюты на кошелек и легальность их происхождения.

РЕШЕНИЕ ЗАДАНИЯ: Проверка искомого адреса в онлайн-сервиса и при помощи дорков не даст результата. Проверяем транзакции, которые заводились на исследуемый криптокошелек https://www.blockchain.com/btc/address/3JuLSLzwR1VuHG6LS2RN3xyA2U8KrobaeK (или в любой другом сервисе). Входящая транзакция будет только с одного криптокошелька, имеющего адрес 1MXHVCztcy8ki5btP7eisXw9WyMnWGfrgd. Используем Google Dork [1MXHVCztcy8ki5btP7eisXw9WyMnWGfrgd -block + scam] для получения информации о криптокошельке. Находим и открываем ссылку на сообщение о мошенничестве, с указанием криптокошелька, по адресу https://www.reddit.com/r/Bitcoin/comments/c3tvau/be_aware_a_fake_peterbrandt_on_twitter_is_doing/.

ОТВЕТ: Приобретаемая криптовалюта имеет криминальное происхождение. Рекомендуется отказаться от ее приобретения.

Тема 3.5 "Идентификация владельцев телефонных номеров"

Методические материалы к данному разделу представлены следующим образом:

Задача №1: Необходимо осуществить сбор информации о факте регистрации пользователя в социальных сетях, на досках объявлений, платежных и банковских сервисах, мессенджерах и др. онлайн сервисах.

Задача №2: Необходимо получить социальной граф по телефону и (или) адресу электронной почты (возраст, поисковые интересы, регион проживания)

Тема 3.6 "Идентификация владельцев адресов электронной почты"

Методические материалы к данному разделу представлены следующим образом:

ЗАДАНИЕ №1: У Вас имеется адрес электронной почты неустановленного лица, занимающегося интернет-мошенничеством aidit45@gmail.com. Используя общедоступный инструментарий, установите адреса криптовалютных кошельков Ethereum, используемых злоумышленником, а также получите его фотографию.

РЕШЕНИЕ ЗАДАНИЯ: Для решения вам следует воспользоваться Google Dork. Пример запроса ["aidit45@gmail.com" + "eth wallet"]. Это позволит вывести все ссылки, содержащие упоминания электронного адреса совместно с кошельками Ethereum. Первая страница поисковой выдачи будет содержать ссылки на два кошелька 0x54804CBD6dB2362656F743e4C4306Dd4f98E6580 и 0x68d872FD051A8C6cB3dcb1ECd8A417e508DD3959, используемые злоумышленником. Также там будет содержаться гиперссылка не его профили в социальных сетях https://www.facebook.com/tank.dazer или https://twitter.com/tanggo1511, откуда можно получить его фотографию.

ОТВЕТ: Злоумышленник использует криптокошельки Ethereum с адресами 0x54804CBD6dB2362656F743e4C4306Dd4f98E6580 и 0x68d872FD051A8C6cB3dcb1ECd8A417e508DD3959. Ссылка на его фотографию https://scontent.xx.fbcdn.net/v/t1.6435-9/130713346_4163935426956800_2880148603427973194_n.jpg?_nc_cat=111&ccb=1-7&_nc_sid=19026a&_nc_ohc=Pzqg7n-6f-0AX8yTKNe&_nc_ht=scontent.xx&oh=00_AfBEx87J3AFErBMOZr_bOgkOIy6Xt9LJMs1rEgsCh3YNbg&oe=63AAB6A2

Тема 3.7 "Идентификация владельцев ресурсов сети Интернет"

Методические материалы к данному разделу представлены в следующем виде.

Задача: найти IP-адреса, доменные имена, сайты, незаконное использование, компрометирующие данные, получить сведения о владельце интернет ресурса, архивные данные, архив сайта, утечки данных, технологии, которые использовались на сайте (чаты/банковские клиенты).

Итог работы: разбор ситуаций со слушателями, дискуссия.

Дополнительно, ниже представлено задание для самостоятельного решения на практическом занятии.

ЗАДАНИЕ №1: В ходе мониторинга сети Интернет был выявлен Telegram-канал, распространяющий призывы к распространению ложных сообщений о терроризме в Российской Федерации. В описании канала была дана ссылка на адрес Биткоин-криптокошелька, предназначенного для сбора пожертвований:

bc1quhvee5437xj9ef8r2usmnmwdz6clfzmr3sd3dp

Используя общедоступный инструментарий, установите когда и через какую площадку для обмена криптовалюты выводились активы с данного

криптокошелька. Установите с каких площадок вносились активы на данный криптокошелек.

РЕШЕНИЕ ЗАДАНИЯ: Вывод средств с криптокошелька осуществлялся по цепочке транзакций 34T1ieC9r82qTx8xCreyQo7d5ttakp2z1V - 1PueNG87RsRepg3JP7gxkfGxnbUxtW9Wyn. При этом криптокошелек 1PueNG87RsRepg3JP7gxkfGxnbUxtW9Wyn был идентифицирован https://www.breadcrumbs.app/, как принадлежащий бирже "Binance" В случае использования иного инструментария, участие "Binance" будет идентифицирована в следующих транзакциях, идущих с 1PueNG87RsRepg3JP7gxkfGxnbUxtW9Wyn на bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h https://bitinfocharts.com/bitcoin/address/bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h или 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s https://www.walletexplorer.com/wallet/Binance.com?from_address=1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s. Ввод активов осуществлялся с криптокошельков bc1qp92qtme2cngxwg8pkz2jqftqefe5nydflap786, отнесенного к бирже "BitZlato" https://www.walletexplorer.com/wallet/BitZlato.com?from_address=bc1qp92qtme2cngxwg8pkz2jqftqefe5nydflap786.

ОТВЕТ: Вывод активов осуществлялся через "Binance", а ввод - через "BitZlato"

Тема 3.8 "Сбор и исследование геолокационной информации в конкурентной разведке"

Методические материалы к данному разделу представлены следующим образом:

Слушателям необходимо разбиться по парам и на основе недавнего события(например, драка или митинг) собрать данные о пользователях, которые могли быть свидетелем, комментировать, т.к. находились рядом. Также, слушателям необходимо собрать информацию о событии и возможных свидетелей и участниках.

Тема 3.9 "Исследование визуального контента (фото, видео) в конкурентной разведке"

Методические материалы к данному разделу представлены в виде задач.

Задача №1: Необходимо установить место съемки контента и лица, находящихся на фото/видео.
Задача №2: Идентификация лица и места съемки на фото или видео.
Задача №3: Форензика и (или) выявление признаков фальсификации, идентификация уникального контента животных, растений, машин.
Итогом практического занятия является обсуждение результатов работы слушателей.

Тема 3.10 "Проведение исследований в сетях ограниченного доступа (даркнет)"

Методические материалы к данному разделу представлены в виде задач.

Задача №1: Необходимо осуществить вход и обеспечить корректную работы сети даркнет.

Задача №2: Необходимо идентифицировать владельца теневого маркета по открытым источникам.

Тема 3.11 "Логирование (фингерпринтинг) пользователей в конкурентной разведке"

Методические материалы к данному разделу представлены следующим образом:

Практическое задание:

Цель - получение данных об устройстве пользователя

Задача: используя сгенерированные анонимные аккаунты, попробовать получить информацию об устройстве и соединении партнера, логирование и цифровой след (***фингерпринтинг***).

Ход занятия – слушателям необходимо разбиться на пары и собрать данные друг о друге.

Тема 3.12 "Управление поисковой выдачей и общественным мнением (информационные войны)"

Методические материалы к данному разделу представлены следующим образом:

Практическая работа: написать контент, чтоб при поиске он находил материал через ключевые слова. План удаления.

Берем учебный контент, заведомо ложный, предложить пути удаления этой информации, удаление по праву на забвение, блокировка ресурса, удаление через поисковую машину.

7. Итоговая аттестация

Итоговая аттестация предусмотрела в форме зачета. Перечень заданий к зачету:

1. Сбор данных в целях идентификации пользователя социальной сети
2. Сбор данных в целях идентификации пользователя электронной почты
3. Сбор данных в целях идентификации пользователя номера телефона
4. Сбор данных в целях идентификации пользователя мессенджера
5. Сбор данных в целях идентификации администратора сообщества (чата или канала)
6. Сбор данных в целях идентификации владельца криптовалютного кошелька
7. Сбор данных в целях идентификации администратора вебсайта
8. Сбор данных в целях идентификации пользователя Даркнет
9. Сбор данных о визуальном контенте в целях идентификации их автора
10. Сбор данных об устройстве и соединении пользователя (логирование)

Способ оценки

- Зачет проводится в практической форме;
- Состоит из 3-х любых заданий;
- Оценивается полнота и точность решения заданий;
- Каждый вопрос оценивается в 5 баллов;
- Максимальная оценка: 15 баллов;
- Система оценки: зачет/не зачет;
- Для получения зачета необходимо набрать 10 баллов.

8. Материально-техническое оснащение

Учебный кабинет:

— стул 20 шт.

— стол -10 шт.

— компьютер – 20 шт.

— ЖК- телевизор - 1 шт.

— Тумба – 1 шт.

— Вешалка для одежды – 2 шт.

— Куллер – 1 шт.

— бумага, ручки, карандаши, маркеры

Учебно-методическое обеспечение:

1) Учебная программа повышения квалификации;

2) Презентационные материалы в эл. виде и на бумажном носителе.

9. Организационно –педагогические условия

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих действующим международным договорам и нормативным правовым актам. В ходе занятий преподаватель обязан увязывать новый материал с ранее изученным, дополнять основные положения примерами из практики, соблюдать логическую последовательность изложения.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы по вопросам выявления, анализа и минимизации финансовых рисков.

Соотношение теоретических и практических занятий может быть изменено преподавателем с учетом уровня усвоения обучающимися разделов образовательной программы.

Для реализации программы необходимо наличие учебных кабинетов (учебных аудиторий), оборудованных учебной мебелью, учебной доской.

10. Список литературы

1) «Специалист по моделированию, сбору и анализу данных цифрового следа», утвержден приказом Минтруда России 09.07.2021 № 462н «Об утверждении профессионального стандарта «Специалист по моделированию, сбору и анализу данных цифрового следа».

2) «Специалист по конкурентному праву», утвержден приказом Министерства трудаи социальной защитыРоссийской Федерации от 16.09.2021 № 637н «Об утверждении профессионального стандарта "Специалист по конкурентному праву».

3) He Xi, He Ketai, Lin Shenwen, Yang Jinglin. Bitcoin Address Clustering Method Based on Multiple Heuristic Conditions. https://www.researchgate.net/publication/351019556_Bitcoin_Address_Clustering_Method_Based_on_Multiple_Heuristic_Conditions. 2021 г.

4) Авдошин С.М., Лазаренко А.В. Методы деанонимизации пользователей биткоин. Труды Института системного программирования РАН. 2018 г.

5) Лучшие инструменты для блокчейн-анализа и как они работают. https://bitnovosti.com/2021/01/16/luchshie-instrumenty-dlya-blokchejn-analiza-i-kak-oni-rabotayut/. 2021 г.

6) Knowing Your Coin Privacy (Using KYCP.org). https://medium.com/samourai-wallet/knowing-your-coin-privacy-using-kycp-org-7b3b4385d8b. 2019 г.

7) Исследование веб-сайтов в рамках OSINT. https://habr.com/ru/company/tomhunter/blog/. 2022 г.

8) Paul Vines, Franziska Roesner, Tadayoshi Kohno. Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob. School of Computer Science & Engineering, University of Washington. 2017 г.

9) Igor S. Bederov. Traps used by cyber detectives… https://medium.com/@ibederov_en/traps-used-by-cyber-detectives-c778b4853f1a. 2022 г.

10) Igor S. Bederov. Check and locate phone number in OSINT. https://medium.com/@ibederov_en/check-and-locate-phone-number-in-osint-8beb8af50d5e. 2022 г.

11) Igor S. Bederov. Fingerprinting email senders… https://medium.com/@ibederov_en/fingerprinting-email-senders-84819fd4a443. 2022 г.

12) 10 лучших бесплатных OSINT-инструментов по версии компании T.Hunter. https://habr.com/ru/company/tomhunter/blog/654369/. 2022 г.

13) OSINT для сбора информации о рекламных идентификаторах на сайтах. https://habr.com/ru/company/tomhunter/blog/585566/. 2021 г.