УДК 159.9

ВОЗМОЖНОСТИ ПРОФАЙЛИНГА В ЦИФРОВОМ ПРОСТРАНСТВЕ

Терновская Е. А. – *студентка факультета психологии, Томского государственного университета, г. Томск, e-mail: ternovskaakata@gmail.com*

Аннотация: *Данная статья посвящена теме киберпреступности, ее видам и способам совершения. Так же рассматривается метод профайлинга при расследовании данных преступлений. Дано определение метода и его особенности, и краткая историческая справка. Анализируются возможности применения цифрового профилирования неустановленного преступника, используя математические методы и специализированные программы. Так же представлены особенности личности киберпреступника, типология и структурные особенности.*

Ключевые слова: *киберпреступность, информационная безопасность, личность преступника, профайлинг, профилирование, цифровая криминология.*

PROFILING POSSIBILITIES IN THE DIGITAL SPACE

Ternovskaya E. A. – *student of the Faculty of Psychology, Tomsk State University, Tomsk, e-mail: ternovskaakata@gmail.com*

Abstract: *This article is devoted to the topic of cybercrime, its types and methods of commission. The method of profiling in the investigation of these crimes is also considered. The definition of the method and its features, and a brief historical background are given. The possibilities of applying digital profiling of an unidentified criminal are analyzed using mathematical methods and specialized programs. The features of the cybercriminal's personality, typology and structural features are also presented.*

Keywords: *cybercrime, information security, criminal identity, profiling, digital criminology.*

На протяжении всей истории профилирование активно использовали, и сейчас данный метод заслуженно применяется практически во всех сферах человеческой жизнедеятельности. Целью данной работы можно считать систематизацию, основанную на анализе литературы, особенностей мира киберпреступников. В рамках данной статьи будут затронуты основные моменты становления криминологического профайлинга. А также мы погрузимся в мир киберпреступлений, узнаем их классификацию и поймём, как их

раскрывают. Разберем типологию и особенности личности киберпреступника. И узнаем, какие программы специализирующиеся на цифровом профайлинга уже есть, а зачем нам нужно больше таких программ.

Начнем по порядку, понятие «profiling» происходит от английского слова «profile» («профиль») и перевести его можно как «профилирование». Профилирование человека осуществляется на основе комплексной оценки его вербального и невербального поведения, что при правильной подготовке позволяет составить подробный психологический портрет человека, полностью отражающий все важнейшие аспекты его личности [7].

В настоящий момент не существует нормативно-правовых актов, регулирующих непосредственное использование профайлинга в системе правоохранительных органов, он не является обязательной мерой при расследовании. Но есть некоторые правовые основы применения профайлинга в различных сферах. К ним можно отнести такие нормативные правовые акты, как указ Президента РФ от 15 февраля 2006 г. № 116 (в ред. от 26.12.2015) «О мерах по противодействию терроризму» или постановление Правительства РФ от 6 декабря 2012 г. № 1259 «Об утверждении Правил профессионального психологического отбора на службу в органы внутренних дел Российской Федерации» [3].

В конце 1970-х гг. была разработана программа психологического профилирования. Определение данного метода было дано Р. Ресслером: «процесс идентификации всех психологических характеристик индивидуума, составляющих общее описание личности, основанный на анализе совершенных им преступлений» [8]. В результате полученных данных эксперт может составить психологический портрет человека, который позволит классифицировать его, поможет выявить его мотивы и склонности, и прогнозировать его возможное поведение. Целью криминалистического профайлинга является определении личности по характеру и способу совершенного преступления, благодаря комплексному использованию методик психологического профилирования можно оптимизировать розыскные мероприятия.

Рассматривая тему профайлинга в историческом контексте, следует отметить, что официальное его применение началось с появлением поведенческого отдела ФБР в США (Квантико, штат Вирджиния) в 1974 году. С 1976 по 1979 год несколько агентов ФБР - наиболее известные Джон Дуглас и Роберт Ресслер - опросили 36 серийных убийц, чтобы разработать теории и категории различных типов преступников Особый интерес для них представляли серийные сексуальные преступники [10].

Насильственных преступлений в настоящее время совершается меньше, однако число убийств на сексуальной почве по-прежнему велико. Но последнее время внимание общественности и органов правопорядка приковано к другим феноменам – терроризму и киберпреступлениям. Киберпреступность является самым быстрорастущим уголовным преступлением по сравнению с другими. Только за первые четыре месяца 2020 года обнаружено около миллиона спам-сообщений, вредоносных ПО и URL-адресов, связанных с Covid-19. Индийский криминолог, профессор Карупаннан Джайшанкар указывает, что киберпреступления больше не являются просто хакерской атакой или атакой на систему, но это атака на людей. Проблема киберпреступности определяется стремительным развитием, внедрением и использованием информационных технологий, а также использованием этих технологий в преступных целях. Она представляет собой специфический, сложный комплекс преступлений, и для ее изучения была разработана новая отрасль криминологии – киберкриминология [9].

Киберпреступность — это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных [5]. Во время взлома и кражи данных эксперты разбираются в программах и методах, с помощью которых совершено преступление; анализируют жертву, выискивают мотивы. Тщательно анализируется информация, которая была украдена.

Преступления в киберпространстве можно разделить на четыре группы. Первая группа — это преступления, направленные против конфиденциальности, такие как незаконный доступ, воздействие на компьютерные данные и т.п.

Во вторую группу входят преступления, связанные с использованием компьютерных средств, такие как подлог и мошенничество с использованием компьютерных технологий.

Третью группу составляют производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение детской порнографии, а также владении детской порнографией, находящейся в памяти ПК.

Четвертую группу составляют преступления, связанные с нарушением авторского права и смежных прав [5].

Расширение масштабов киберпреступности в России вызывает озабоченность, она приобретает все более опасные формы. Так, согласно официальным статистическим данным

МВД РФ, в 2017 г. зарегистрировано 90 587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, за 11 месяцев 2018 г. их количество составило 156 307 (прирост 89,6 %), а раскрываемость — около 25 % [6].

Поэтому вполне логично, что сейчас появляются специализированные компьютерные программы, которые помогу автоматизировать метод профайлинга. Данные программы собирают информацию в киберпространстве, обрабатывают ее и помогают в расследовании преступлений.

Зачем нужна автоматизация профайлинга, к примеру в корпоративной среде? Причин несколько. Первая — время. Профилирование сотрудников специалистом-профайлером отнимает много времени. Одна только опросная беседа в среднем длится от 40 до 60 минут. Кроме того, людям свойственно меняться, пересматривать убеждения и принципы. Поэтому для получения более точных психологических профилей оценивать сотрудников нужно постоянно, а это значит — регулярно привлекать специалистов и оплачивать их услуги или нанимать в штат.

Другая причина — расстояние. В одном офисе мы еще можем наблюдать за каждым сотрудником, чтобы видеть, как меняется человек и его поведение. В крупных компаниях, следить за каждым лично невозможно. Автоматизация дает возможность дистанционной оценки.

Еще одна причина — объективность. Работа профайлера по составлению психологического портрета не лишена субъективности. Программное же обеспечение анализирует личность по алгоритмам и не выносит «оценочных суждений». Важно, что анализ происходит без тестирования и личных бесед, а значит, ничего не отрывает сотрудников от работы, их поведение остается естественным, а атмосфера в коллективе — спокойной.

Автоматизация профайлинга базируется на том, что характер и особенности личности проявляются в речи и письме. Например, одна из таких программ - DLP-система «Контур информационной безопасности СёрчИнформ» собирает огромное количество текстов, созданных сотрудниками. Для целей профайлинга нужны не деловые, формальные тексты, а более естественные, «живые». В расчетах модуля учитываются исходящие письма, сообщения в мессенджерах и рабочих чатах. Все это каналы, по которым пользователи общаются в более расслабленном тоне, даже когда обсуждают рабочие вопросы. Для точного анализа ProfileCenter требуется минимум 30 тысяч базовых единиц текста. Чем дольше DLP-система накапливает переписку, тем более развернутые психологические портреты и верные

заключения выдает ProfileCenter [1]. Она вычисляет тип личности и структуру мышления на основании оценки текста по более чем 70 критериям. Это позволяет выявить доминирующие черты характера, базовые эмоции, сильные и слабые стороны личности. Задача модуля — указать на потенциальный риск, составить прогноз поведения человека в нормальных, критических и стрессовых обстоятельствах.

В России раскрытием и расследованием киберпреступлений занимаются Управление «К» МВД России и отделы «К» региональных управлений внутренних дел, входящие в состав Бюро специальных технических мероприятий МВД России.

Как вообще происходит расследование киберпреступлений, рассказал бывший сотрудник управления «К» МВД России, для сетевого новостного портала МОСКВА24. Как и в любом расследовании здесь существует несколько стадий. Первая из них это обнаружение угрозы, любое расследование начинается с сообщения о преступлении – краже денег со счета, обнаружения шпионской программы или вируса. Заявление от пострадавшего поступает в местное отделение полиции, после чего преступление квалифицируется и проводится первичная проверка – до возбуждения дела необходимо отработать материал, найти признаки состава правонарушения и собрать доказательства. Дальше следователь возбуждает дело. Если это компьютерное преступление, то оно попадает в управление "К".

Следующим этапом становится реконструкция преступления. В случае хищения денег с использованием мобильного банкинга прежде всего необходимо установить, какая программа использовалась для неправомерного доступа и куда были переведены средства, необходимо восстановить хронологию. Этим занимаются в лаборатории или частные фирмы.

Затем идет исследование вируса. Вредоносные программы подробно исследуют, изучают какие возможности он предоставляет злоумышленнику и как им управлять. Проверкой вирусов могут также заниматься и в самом "К" или в экспертно-криминалистическом центре.

Четверным этапом считается поиск исполнителей. Обычно ходе расследования важно восстановить историю развития преступника и вернуться к моменту, когда он только набирался опыта. Часто в самом начале люди допускают гораздо больше ошибок, которые и позволяют их идентифицировать в сети. МВД вправе запрашивать самую разную информацию у интернет-провайдеров, операторов сотовой связи, владельцев интернет-ресурсов. Физический поиск и задержание хакера могут осуществить только полицейские или ФСБ.

Одним из самых важных этапов можно назвать совместное расследование с правоохранителями. Устанавливают заказчиков преступления, отслеживают денежные потоки, опечатывают компьютеры, выполняют следственно-процессуальные действия – обвинение, арест и прочее. Стоит сказать, что непосредственным расследованием дел в управлении "К" не занимаются - там только обеспечивают техническое сопровождение. Само дело могут направить и в управление по борьбе с экономическими преступлениями, и в ФСБ. Когда круг подозреваемых сужается, проводятся оперативные мероприятия по отношению к подозреваемым: прослушка телефонов, просмотр электронной переписки и прочее. При этом технику изымают только тогда, когда на это есть серьезные основания. Сами компьютеры передают на исследование экспертам - как негосударственным фирмам, так и МВД.

И последним этапом считается судебный процесс. Когда все тонкости киберпреступления установлены, а хакер пойман, начинается суд, в ходе которого опрашивают экспертов и разъясняют суду технические детали проведенной работы. Для установления вины необходимо собрать полный комплекс доказательств. Сбор доказательственной базы – самый сложный этап работы. И они обязательно должны быть получены в установленном законом порядке [2].

В целом, можно сказать, что сейчас устройства представляют собой что-то вроде «цифровых дневников» носителей информации, в которых невозможно не оставлять цифровых следов, образцов, отражающих индивидуальные особенности поведенческих признаков индивида, независимо от воли субъекта.

На сегодняшний день цифровое профилирование, являясь производным от традиционного профилирования в общепринятом понимании, успешно используется в ряде европейских стран. Применение методов цифрового профилирования в киберпространстве, наиболее сложный вид интеллектуальной деятельности в системе криминологических исследований. Немецкие криминологи, пожалуй, одними из первых стали применять в практике розыска цифровые методы профилирования. Сущность такого метода заключается в автоматизированном поиске неизвестного преступника посредством электронной обработки информации и анализе криминологической информации, в основе которого лежит совокупность логико-математических методов. Благодаря таким методам становится возможным структурирование и моделирование цифрового профиля. Уникальность его заключается в изучении и анализе с использованием ЭВМ больших объемов информации [6].

Построение искомой модели осуществляется различными способами: мысленным моделированием, реконструкцией, а также логико-математическим и кибернетическим

моделированием. Исследование и анализ информации, полученной в цифровой среде, осуществляются в результате применения математического метода многомерной экстраполяции. Данный метод исходит из того, что в жизни действует принцип инерции, который заключается в том, что наблюдаемые закономерности достаточно устойчивы в течение определенного периода времени [6].

Несмотря на то, что в научной доктрине еще окончательно не определено, что именно входит в профиль преступника, зарубежными специалистами выделено три важнейших элемента: способ совершения преступления); социальные показатели индивида (эмоционально-волевые признаки или психологические особенности) и почерк преступления (уникальные комбинации поведения) [6].

Хоть преступное поведение и уникально, в нем просматриваются закономерные связи между способом, орудием совершения преступления и индивидуальными личностными социально-психологическими особенностями лица, совершившего преступление. Орудия, средства преступления, способ его совершения подбираются преступником на основе жизненного опыта, социальной роли, интеллектуальных, эмоциональных, волевых и нравственных признаков, образующих структуру его личности. Индивид в условиях криминальной ситуации действует так, как привык действовать. Личность преступника является носителем причин совершения преступления, она является основным и важнейшим звеном всего механизма преступного поведения.

В обычном понимании принято считать, что цифровые преступления совершают высококвалифицированные программисты. Однако в общем объеме всех цифровых преступлений такой вид профессионалов занимает незначительную долю. Если целью было удалить информацию или прервать работу интернет-ресурса, преступника установить не так сложно. Обычно это молодые хакеры, которые используют чужие инструменты. Они пока не умеют создавать собственные вредоносные программы, а их целью выступает лёгкая нажива.

По мотивам совершения цифрового преступления можно выделить наиболее распространенные типы личности цифрового преступника:

- корыстный тип (объединяет всех лиц, совершивших цифровые преступления по мотивам личного обогащения);
- престижный тип (лица, совершающие преступления из престижных побуждений, т. е. для того, завоевать авторитет среди окружающих, быть все время на виду и т. д.);

- насильственный тип (данный тип цифрового преступника заключаете в совершении психического насилия в отношении лиц: ревность, завесить и т. п., однако их доля невелика).
- сексуальный тип (характерен для лиц, виновных в распространении порнографии в Интернете и получении от этого удовлетворения) [4].

Существует так же небольшая классификация личностных свойств, согласно которой все основные составляющие личности можно разделить на три группы:

1. Уголовно-правовая характеристика – совокупность данных, которые свидетельствуют о начале виновным преступной карьеры или о ее продолжении.

Цифровые преступления умышленные, в большинстве спланированы. 80 % лиц совершали преступления единолично, лишь 15 % группой лиц, по предварительному сговору. Но 50 % этих преступников ранее совершали различные преступления, 10 % из которых имели рецидив преступлений, совершили преступление при условном осуждении, в течение года после освобождения из мест лишения свободы, состояли под административном надзором, а 25 % были заключены под стражу. Это указывает на заинтересованность преступного мира совершать деяния в цифровой сфере. Такая группа цифровых преступников отличается криминальной устойчивостью и профессионализмом [4].

2. Социально-демографическая характеристика – это сведения о поле, возрасте, образовательном уровне, материальных условиях, семейном положении.

Цифровые преступления совершают как мужчины (75 %), так и женщины (25 %), в основном в возрасте 30–49 лет – 45 % и 18–24 – 25 %, что позволяет сделать вывод о сформировавшемся характере личности цифрового преступника.

3. Нравственно-психологическая характеристика – выражение отношения преступника к обществу в целом, принятым в нем ценностям и нормативно-одобряемым социальным ролям.

Среди ценностных ориентаций у данной категории лиц преобладают индивидуально – и кланово-эгоистические. Нравственное и правовое сознание личности обычно деформировано или ослаблено. Корыстные мотивы порождаются гипертрофированными или извращенными потребностями, к примеру стремлением к легкой наживе. Мотивами преступных действий несовершеннолетних обычно являются исследовательский интерес, самоутверждение и жажда славы [4].

Следует отметить, что профайлинг в цифровой криминологии один из сложнейших методов расследования преступлений, и он не является обязательным методом. Но как вспомогательный метод, явно необходим. Именно профилирование лежит в основании систем классификации преступников, а они в свою очередь дают возможность понять мотивы преступника, а знание мотива существенно сужает круг подозреваемых.

Последнее время по всему миру происходит сильная цифровизация, в том числе и преступного мира. Образ преступника меняется, в киберпространство потянулись уже и общеуголовные преступники. Возможность удаленно совершить преступление, дает ощущение определенной безопасности, а возможность получить большие доходы привлекает многих. Сейчас, когда из-за пандемии COVID-19, многие аспекты жизнедеятельности человека выполняются при помощи цифровых технологий, так важно обратить внимание на киберпреступления, их раскрытие и предотвращение. Чтобы предотвратить киберпреступления, бывает мало лишь ознакомить население со способами совершения, не лишним будет и создать программы, которые помогут с профилированием населения. Например, DLP-системы, собирающие информацию о человеке в киберпространстве и способные составлять его профиль, а также определять опасность для компании. Данные системы в составе комплекса мер по раскрытию преступлений будут очень полезны, и не только при расследовании киберпреступлений.

ЛИТЕРАТУРА

1. Бируля Иван. Нетехнические методы защиты информации: профайлинг на службе ИБ [Электронный ресурс] // Anti-Malware. URL: https://www.anti-malware.ru/practice/methods/information-security-profiling (дата обращения: 20.11.2021).
2. Блохин Сергей. IT-сыщики: как расследуют киберпреступления [Электронный ресурс] // МОСКВА24 : URL: https://www.m24.ru/articles/hakery/13032015/68059?utm_source=CopyBuf (дата обращения: 23.11.2021).
3. Вахнина В. В., Мальцева Т. В., Михайлова Т. В., Ульянина О. А. Профайлинг в деятельности органов внутренних дел: учебное пособие. - Москва : Академия управления МВД России, 2019. - 98 с.
4. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология : учебное пособие. – Москва. : Академия управления МВД России, 2021. – 244 с.
5. Номоконов В. А. Киберпреступность как новая криминальная угроза [Электронный ресурс] / Криминология: вчера, сегодня, завтра. — 2012. – 11 с. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 23.11.2021).

6. Суходолов А. П., Калужина М. А., Спасенников Б. А., Колодин В. С. Цифровая криминология: метод цифрового профилирования поведения неустановленного преступника [Электронный ресурс] / Всероссийский криминологический журнал. – 2019. – 10 с. URL: https://cyberleninka.ru/article/n/tsifrovaya-kriminologiya-metod-tsifrovogo-profilirovaniya-povedeniya-neustanovlennogo-prestupnika (дата обращения: 25.11.2021).

7. Филатов Алексей. Профайлинг. Как научиться разбираться в людях и прогнозировать их поведение. - Москва : Перо, 2016. — 417 с.

8. Черкасова Е. С. Профайлинг как метод создания психологического портрета потенциального преступника на этапе организации предварительного расследования // Вестник НГУ, серия: Право, 2013, т.9, выпуск 1, С. 72-75.

9. Aldona Kipane Meaning of profiling of cybercriminals in the security context [Электронный ресурс] / Society. Health. Welfare. — Riga: Rıga Stradins University, 2019. — 15 с. URL: https://www.shs-conferences.org/articles/shsconf/pdf/2019/09/shsconf_shw2019_01009.pdf (дата обращения: 25.11.2021).

10. Introduction: the roots of modern profiling [Электронный ресурс] / - 15 с. URL: http://www.forensicresearchdigest.com/yahoo_site_admin/assets/docs/M_Hicks_and_Sales_-_1_Introduction_the_Roots_of_Modern_Profiling.18170811.pdf (дата обращения: 16.11.2021).