Евразийская адвокатура. 2022. № 1 (56). С. 82.
Eurasian advocacy. 2022;(1(56)):82.

Правосудие и правоохранительная деятельность в евразийском пространстве
Научная статья
УДК 343.9
doi 10.52068/2304-9839_2022_56_1_82

К ПРОБЛЕМЕ ПРИМЕНЕНИЯ КРИМИНАЛИСТИЧЕСКОГО ПРОФАЙЛИНГА ПРИ РАССЛЕДОВАНИИ И РАСКРЫТИИ КИБЕРПРЕСТУПЛЕНИЙ

АКИМЕНКО Марина Алексеевна[1], ОВЧАРЕНКО Игорь Алексеевич[2]
[1] Кандидат юридических наук, доцент кафедры уголовно-правовых дисциплин и судебно-экспертной деятельности юридического института Пятигорского государственного университета
357500, г. Пятигорск, ул. Октябрьская, д. 38, Российская Федерация
[2] Эксперт центра правовой помощи и независимых экспертиз «Надежда»
355037, г. Ставрополь, ул. Серова, д. 6, корп. 1, оф. 6, Российская Федерация

Аннотация: Цель работы – исследование возможности применения криминалистического профайлинга в Российской Федерации при расследовании и раскрытии киберпреступлений. В статье использовались социологический и формально-юридический методы. В статье исследуются особенности применения криминалистического профилирования при расследовании и раскрытии киберпреступлений. Авторами рассматриваются некоторые организационно-правовые механизмы использования методик нетехнического профайлинга при расследовании и раскрытии преступлений, выявлен ряд недостатков применения данного метода на практике, и предложены организационно-правовые меры, позволившие бы их минимизировать.

Статья обладает достаточной степенью научной ценности, так как является одним из первых исследований вопросов применения криминального нетехнического профайлинга при расследовании и раскрытии киберпреступлений в новых социальных условиях пандемии COVID–19.

Ключевые слова: профайлинг, криминалистика, киберпреступление, киберпреступник

Для цитирования: Акименко М.А., Овчаренко И.А. К проблеме применения криминалистического профайлинга при расследовании и раскрытии киберпреступлений // Евразийская адвокатура. 2022. № 1 (56). С. 82. https://doi.org/10.52068/2304-9839_2022_56_1_82

Justice and law-enforcement activity In the eurasian space
Original article

ON THE PROBLEM OF THE USING OF FORENSIC PROFILING IN THE INVESTIGATION AND DISCLOSURE OF CYBERCRIMES

AKIMENKO Marina Alekseevna[1], OVCHARENKO Igor Alekseyevich[2]
[1] PhD, Associate Professor of the Department of Criminal Law Disciplines and Forensic Activity of the Law Institute of Piatigorsk State University
357500, Pyatigorsk, ul. October, 38, Russian Federation
[2] Expert of a Center of legal help «Nadezhda»
355037, Stavropol', ul. Serova, 6, korp. 1, of. 6, Russian Federation

Abstract: To study the feasibility of applying a forensic profile in the Russian Federation. Sociological and formal legal methods were used. The article examines the features of the use of forensic profiling in the investigation and detection of crimes. The authors explore some organizational and legal mechanisms for using non-technical profiling techniques in the investigation and detection of cybercrimes, identify a number of shortcomings in the application of this method in practice and propose organizational andlegal measures that would allow them to be minimized. The article has sufficient scientific value, as it is one of the first studies on the use of cybercrimes criminal non-technical profiling in the new social conditions of the COVID-19 pandemic.

Keywords: profiling, forensics, cybercrime, cybercriminal

For citation: Akimenko M.A., Ovcharenko I.A. On the problem of the using of forensic profiling in the investigation and disclosure of cybercrimes = Eurasian advocacy. 2022;1(56): 82. (In Russ.). https://doi.org/10.52068/2304-9839_2022_56_1_82

© Акименко М.А., Овчаренко И.А., 2022

Распространяющаяся по миру коронавирусная инфекция за последние время внесла существенные коррективы во все сферы жизнедеятельности современного общества. С правовой точки зрения такие изменения можно охарактеризовать как введение специального административного режима наивысшей степени (от самоизоляции граждан до закрытия предприятий сферы услуг и введения дистанционного обучения). Причем такие ограничения вводились с использованием административного ресурса на уровне субъектов РФ, с одной стороны, показав на практике его действенность, а с другой – отразив некую «парализацию» федерального законодательства в сложившейся ситуации. Только спустя практически год коронавирусные ограничения вводятся законодателем в практико-правовое пространство (принимается соответствующая законодательная база на федеральном уровне, регулирующая и процесс дистанционного обучения, например, и правила, а также порядок удаленной работы). Причем такие нововведения географически коснулись практически всего цивилизованного сообщества. Пандемия затронула все сферы жизнедеятельности современного цивилизованного мира. Наше государство не стало исключением. Преступность как явление социальное также не могла остаться в стороне, не изменив свои основные криминологические характеристики и показатели [1].

Реалии развития современного общества, в свою очередь, требуют от правоохранителей и иных государственных органов также постоянного совершенствования механизмов противодействия и профилактики преступности.

От внедрения новых методик, направленных на собирание, исследование и анализ криминалистически значимой информации, зависит качество расследования, а соответственно, и раскрытия преступления. При этом процесс расследования любого правонарушения, и преступления прежде всего, всегда облечен в процессуальную форму.

В то же время оперативно-розыскные мероприятия зачастую осуществляются вне процессуальных процедур. Но методики выявления лица, совершившего преступления, в данном случае многоаспектны, есть и сравнительно новые, направленные на получение ориентирующей информации в отношении преступника. К таким методикам можно отнести профайлинг.

Как сравнительно новое направление исследования, направленное на установление личности преступника посредством анализа криминалистически значимой информации, методика криминалистического профайлинга в нашей стране с каждым годом используется все больше и больше.

Применение методик криминалистического профайлинга при раскрытии преступлений позволяет определить, какой тип человека способен на совершение того или иного противоправного деяния. Анализ различных доказательств по делу в ходе проведения предварительного расследования позволяет сделать определенные выводы о психологических особенностях лица, совершившего то или иное преступление. В свою очередь, знания о таких особых психологических чертах помогают либо сузить круг подозреваемых лиц, либо оптимизировать поиск преступника в случае, если органы предварительного расследования имеют дело с преступлением, совершенным в условиях неочевидности [2]. Как сравнительно новая методика криминалистический профайлинг имеет как противников, так и сторонников, поддерживающих применение метода криминального профайлинга при раскрытии и расследовании преступлений для установления личности преступника. На наш взгляд, в условиях пандемии коронавируса, охватившей большинство стран мирового сообщества и Россию в том числе, применение данного метода является достаточно эффективным, так как в сложившихся условиях диверсифицируется характер преступной деятельности, возрастают, причем достаточно быстрыми темпами, преступления с применением кибертехнологий и онлайн-пространства. Так, по данным Всемирного экономического форума, в 2018 году ущерб мировой экономике от киберпреступности составил 1,5 триллиона долларов, в 2022 году прогнозируются потери в 8 триллионов долларов, а в 2030 году они могут достигнуть 90 триллионов – эта цифра превышает объемы мирового ВВП сегодня [3].

Именно использование методик, наработанных не техническим, а психологическим профайлингом, в сложившихся условиях может стать действенным механизмом при раскрытии и расследовании киберпреступлений из-за их специфичности и в большей степени анонимности. Для решения этой задачи перспективным является изучение элементов субъективной психологической стороны криминального деяния – некоторых аспектов в поведении преступника, отражающих его личностные характеристики, объединенные в его профиль. Концептуально метод опирается на положение о том, что все криминалистические характеристики преступления являются косвенным или прямым отражением личности и поведения виновного [4].

Для проведения невербального сканирования личности киберпреступника с последующей возможностью составления обобщенного профиля следует использовать характеристики следующих качеств личности преступника: социально-демографические (пол, возраст, место проживания, наличие постоянной работы); социально-ролевые, включающие совокупность видов деятельности лица как гражданина в системе общественных отношений (уровень умственного развития, культурно-образовательный уровень, знания, навыки, умения) [5]. При этом данный вид преступлений можно отнести к преступлениям с максимальным уровнем латентности. По данным Генеральной прокуратуры РФ, расследуется и раскрывается только каждое 20-е киберпреступление, т. е. только 4,4 % от числа всех зарегистрированных в России [6]. Одной из причин такой высокой латентности данного рода преступлений, на наш взгляд, является тот факт, что в РФ компьютерные преступления вынуждены расследовать люди с юридическим образованием, тогда как во многих зарубежных странах следователями по cybercrime выступают технические эксперты с дополнительным юридическим образованием. На наш взгляд, достаточно эффективна в данном случае была бы и деятельность эксперта профайлера.

В свою очередь, проведенный анализ статистических данных по делам о киберпреступлениях позволяет по вышеуказанным критериям составить следующий обобщенный профиль киберпреступника:

1. Молодые люди (преимущественно мужского пола) от 18 до 21 года. Причем с каждым годом возрастной критерий снижается, по данным экспертов по кибербезопасности, около 10 % с хвостиком киберпреступников имеют достаточно юный возраст – 14–15 лет [7].

2. Уровень образования такого преступника достаточно высокий. Более половины киберпреступников, совершающих высокотехнологические преступления, имеют высшее образование. Косвенно об этом свидетельствует также тот факт, что в течение 2021 года специалисты по кибербезопасности отметили новый тренд – появление еще одного класса – кибернаемников. Эти лица или группировки работают исключительно по заказам, занимаются атаками на конкретные компании. В рамках своей компании они занимаются предварительной разведкой по отношению к компании, которую они собираются атаковать, создают уникальные инструменты для нападения [8]. В то же время, учитывая фактор уменьшения с каждым годом возраста киберпреступников, стоит предположить, что количество лиц, не имеющих высшего образования, в данном виде преступности также будет увеличиваться в ближайшее время.

3. Как показал анализ статистических данных по количеству приговоров суда в отношении киберпреступников, большинство из них не состоит в браке, либо брак официально не зарегистрирован, об этом косвенно может свидетельствовать и возрастной критерий киберпреступников (от 18 до 21 года). Если мы дальше будем анализировать социальные роли, то, по свидетельству экспертов, за последнее время среди киберпреступников возрастает количество трудоустроенных граждан. Вызвано это, прежде всего, появлением нового вида киберпреступников в виде кибернаемников. Киберхулиганы, как правило, трудоустроены в меньшем процентном соотношении, в том числе учитывая их значительно молодой возраст в сравнении с кибернаемниками.

В рамках данного исследования нами были обозначены лишь основные критерии обобщенного характера, определяющие профиль киберпреступника. Кроме того, анализ правоприменительной практики по данной категории дел показывает, что пострадавшие компании очень часто в частном порядке привлекают экспертов-криминалистов, чтобы провести внесудебное расследование и затем с уже собранными доказательствами и описанием идти в полицию или в суд. Отсутствие такого подготовительного этапа перед подачей заявления в полицию в большинстве случаев приводит либо к отказу в возбуждении дела, либо к превращению его в вялотекущее расследование [6]. Чтобы минимизировать сложившуюся ситуацию, на наш взгляд, необходимо разработать комплексную программу по противодействию киберпреступлениям с привлечением разного рода специалистов, прежде всего технических специалистов, специалистов-экспертов профайлеров, с дополнительным юридическим образованием, в том числе предусмотрев на базе юридических вузов получение образования по кибербезопасности. На наш взгляд, в качестве общепрофилактических мероприятий в данной области также следует повсеместно, на всех уровнях образования повышать компьютерную грамотность, отдельно предусматривая курсы, описывающие особенности работы интернет-пространства.

Список источников

1. Акименко М.А. О некоторых криминологических особенностях проявления криминальной актив-

ности транснациональной организованной преступности в период пандемии COVID–19 // Евразийская адвокатура. 2021. № 3 (52). С. 109–110.

2. Иванова Л.Ф. Проблемы и перспективы развития метода криминалистического профилирования при расследовании преступлений неочевидного характера // Вестник Южно-Уральского государственного университета. Серия: Право. 2021. Т. 21. № 1. С. 37–46.

3. В 2022 году ущерб от киберпреступности составит 8 триллионов долларов [Электронный ресурс]. URL: https://plusworld.ru/daily/cat-security-and-id/v-2022-godu-ushherb-ot-kiberprestupnosti-dostignet-8-trillionov-dollarov/.

4. Черкасова Е.С. Профайлинг как метод создания психологического портрета потенциального преступника на этапе организации предварительного расследования // Вестник НГУ. Серия: Право. 2013. Т. 9. Вып. 1. С. 72–75.

5. Криминология: учебник. 2-е изд., перераб. и доп. М.: Волтерс Клувер, 2004. С. 354.

6. Киберпреступлений становится все больше, однако их раскрываемость уменьшается // Адвокатская газета [Электронный ресурс]. URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/.

7. В Сбербанке рассчитали долю совершенных детьми киберпреступлений [Электронный ресурс]. URL: https://www.rbc.ru/society/04/07/2018/5b3ceb009a7947b19e91997e.

8. Новые тренды кибепреступности в 2022 году [Электронный ресурс]. URL: https://freedmanclub.com/novie-trendy-kiberpristupnosti-v-2022-god.

References

1. Akimenko M.A. O nekotory`x kriminologicheskix osobennostyax proyavleniya kriminal`noj aktivnosti transnacional`noj organizovannoj prestupnosti v period pandemii COVID–19 // Evrazijskaya advokatura. 2021. № 3 (52). S. 109–110.

2. Ivanova L.F. Problemy` i perspektivy` razvitiya metoda kriminalisticheskogo profilirovaniya pri rassledovanii prestuplenij neochevidnogo xaraktera // Vestnik Yuzhno-Ural`skogo gosudarstvennogo universiteta. Seriya: Pravo. 2021. T. 21. № 1. S. 37–46.

3. V 2022 godu ushherb ot kiberprestupnosti sostavit 8 trillionov dollarov [E`lektronny`j resurs]. URL: https://plusworld.ru/daily/cat-security-and-id/v-2022-godu-ushherb-ot-kiberprestupnosti-dostignet-8-trillionov-dollarov/.

4. Cherkasova E.S. Profajling kak metod sozdaniya psixologicheskogo portreta potencial`nogo prestupnika na e`tape organizacii predvaritel`nogo rassledovaniya // Vestnik NGU. Ceriya: Pravo. 2013. T. 9. Vy`p. 1. S. 72–75.

5. Kriminologiya: uchebnik. 2-e izd., pererab. i dop. M.: Volters Kluver, 2004. S. 354.

6. Kiberprestuplenij stanovitsya vse bol`she, odnako ix raskry`vaemost` umen`shaetsya // Advokatskaya gazeta [E`lektronny`j resurs]. URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/.

7. V Sberbanke rasschitali dolyu sovershenny`x det`mi kiberprestuplenij [E`lektronny`j resurs]. URL: https://www.rbc.ru/society/04/07/2018/5b3ceb009a7947b19e91997e.

8. Novy`e trendy` kibeprestupnosti v 2022 godu [E`lektronny`j resurs]. URL: https://freedmanclub.com/novie-trendy-kiberpristupnosti-v-2022-god.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

Статья поступила в редакцию 19.02.2022; одобрена после рецензирования 25.02.2022; принята к публикации 26.02.2022.

The article was submitted 19.02.2022; approved after reviewing 25.02.2022; accepted for publication 26.02.2022.

ЕВРАЗИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ПРОБЛЕМ ПРАВА

www.eurasniipp.ru info@eurasniipp.ru +7-917-40-61-340