Соціально-правові студії. 2020. Випуск 4 (10). С. 94-100
Social & Legal Studios. 2020. Issue 4 (10). P. 94-100

UDC (УДК) 343.95

Зачек Олег Ігорович,
кандидат технічних наук, доцент,
доцент кафедри інформаційного та аналітичного забезпечення
діяльності правоохоронних органів
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: zachekoi@gmail.com
ORCID ID: 0000-0002-4846-5718

Дмитрик Юрій Іванович,
кандидат юридичних наук,
доцент,
доцент кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: tibet@ukr.net
ORCID ID: 0000-0003-3929-3544

ЗАСТОСУВАННЯ ПРОФАЙЛІНГУ ДЛЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. Досліджено актуальні проблеми застосування передових методик профайлінгу в процесі протидії кіберзлочинності підрозділами Національної поліції. Зауважено, що профайлінг є важливим інструментом розслідування кіберзлочинів і дає змогу підвищити ефективність професійної діяльності кіберполіції. В розвинутих країнах використання профайлінгу під час розслідування кіберзлочинів є доволі поширеним. Тому в статті розглянуто досвід зарубіжних країн щодо застосування профайлінгу для боротьби з кіберзлочинністю. Запропоновано зміни до чинного законодавства.

Ключові поняття: профайлінг, профайлер, кіберзлочини, кіберполіція, інформаційна безпека.

Zachek Oleh,
PhD (Technical),
Associate Professor,
Associate Professor of the Department of Information
and Analytical Support of Law Enforcement,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: zachekoi@gmail.com
ORCID ID: 0000-0002-4846-5718

Dmytryk Yurii,
PhD (Law),
Associate Professor,
Associate Professor of the Department of Operative-Search Activity,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: tibet@ukr.net
ORCID ID: 0000-0003-3929-3544

APPLICATION OF PROFILING TO COMBAT CYBER CRIME

Abstract. The article is devoted to the study of current problems of application of advanced methods of profiling in the process of combating cybercrime by units of the National Police. The fight against cybercrime has recently become increasingly important, as there has been a significant increase in the number of cybercrimes.

Ukrainian cyber police units must use the most modern methods to combat such crimes. One such method is profiling, which is an important tool for investigating crimes, including information crimes. It allows us to classify cybercriminals, understand their habits and technologies and aims to identify the perpetrator. Due attention is not paid to psychological aspects quite often in operational and investigative activities, resulting in the problem of diagnosis and assessment of the offender. Profiling allows to solve this problem and to increase efficiency of professional activity of divisions of cyber police of National police of Ukraine. But profiling is not used practically in the activities of these units in this time, although the use of profiling in the investigation of cybercrime is quite common in the world's leading countries. Therefore, we aimed to consider the problems of application of advanced profiling techniques in the process of combating cybercrime in the activities of cyber police units, as well as to provide suggestions for improving the current legislation. None of the existing legal documents of our state provides for the use of profiling in the activities of cyber police. Underestimation of capabilities of profiling in cyber police units of the National Police of Ukraine requires rethinking currently. Profiling technologies can be successfully implemented in the activities of operational units of the National Police, including cyber police units, due to it combat crime will be more effectively. It is advisable to add to the existing search measures at the legislative level such a measure as "operational profiling" to this end, that will allow to widely use its capabilities.

Key concepts: profiling, profiler, cybercrime, cyber police, information security.

DOI 10.32518/2617-4162-2020-4-94-100

Вступ

Боротьба з кіберзлочинністю недавнім часом набуває дедалі більшої актуальності, оскільки спостерігається значне зростання кількості кіберзлочинів. Згідно з повідомленням пресслужби платформи відкритих даних Opendatabot, за останні п'ять років в Україні кількість інформаційних злочинів зросла щонайменше у 2,5 рази [1]. І для протидії таким злочинам підрозділи кіберполіції України мусять застосовувати найсучасніші методи.

Одним із таких методів є профайлінг, який є важливим інструментом розслідування злочинів, зокрема й інформаційних. Він дає змогу класифікувати кіберзлочинців, зрозуміти їхні звички і технічні навики, та має на меті виявлення злочинця.

Доволі часто в оперативно-розшуковій діяльності не приділяється належна увага психологічним аспектам діагностики й оцінювання особи злочинця, внаслідок чого виникає проблема. І, власне, профайлінг дозволяє вирішити цю проблему та підвищити ефективність професійної діяльності підрозділів кіберполіції Національної поліції України. Але наразі профайлінг у діяльності цих підрозділів майже не використовується, хоча у провідних країнах світу застосування профайлінгу під час розслідування кіберзлочинів є доволі поширеним.

Проблеми використання профайлінгу правоохоронними органами неодноразово порушувались у вітчизняній науці. Неабияка актуальність питання, що розглядається, зумовила те, що воно ставало предметом дослідження таких науковців, як В. Д. Берназ, О. М. Бандурка, В. О. Бакальчук, Ю. Л. Бєлоусов, Ф. В. Глазирін, М. І. Єнікеєв, О. В. Катуніна, В. О. Коновалова, В. О. Образцов, Б. Я. Петелін, О. М. Подільчак, О. Р. Ратінов, В. Ю. Шепітько та ін. Також це питання вивчали зарубіжні дослідники R. Yepes, D. Shinder, N. Garcia, М. Кобишева, А. Крутілін, І. Біруля, А. Філатов, Е. Черкасова. Однак праці зазначених дослідників не містять комплексного дослідження актуальних проблем та особливостей застосування передових методик профайлінгу в процесі протидії кіберзлочинності підрозділами Національної поліції.

Метою статті є розгляд проблем застосування передових методик профайлінгу в процесі протидії кіберзлочинності у діяльності підрозділів кіберполіції, а також надання пропозицій щодо вдосконалення чинного законодавства.

1. Засади використання профайлінгу в правоохоронній діяльності

Профайлінг – це сукупність психологічних методів і методик оцінки та прогнозування поведінки особи на основі аналізу найбільш інформативних особистісних ознак, характеристик зовнішності, вербальної та невербальної поведінки [2, с. 132]. Слово «profiling» утворене від англійського «profile» («профіль») та означає «профілювання».

На початковому етапі профайлінг застосовувався лише спецслужбами деяких країн, але сьогодні він застосовується набагато ширше, зокрема у кадровій роботі, в межах судочинства, у сфері безпеки, в банківській діяльності тощо.

Є такі види профайлінгу [3]:

1. Криміналістичний, коли здійснюється підготовка психологічного портрета особи, яка підозрюється у скоєнні серії злочинів.

2. Профайлінг у сфері інформаційної безпеки, коли аналізуються загрози інформаційній безпеці внаслідок витоку інформації та вивчається дотримання працівниками режиму політико-інформаційної безпеки.

3. Антитерористичний, який використовується для запобігання терористичним загрозам шляхом виявлення потенційно небезпечних учасників масових заходів.

4. Авіаційний, який дає змогу виявити потенційно небезпечних пасажирів і запобігти терористичним актам.

5. Науково-дослідний профайлінг – це науковий напрям, присвячений технологіям зчитування емоцій і дистанційному виявленню неправди.

6. Типологічний, який створює практичні психотипології для швидкого виявлення типу людини, її основних особистісних якостей, і створення моделі дій цієї людини.

7. Психотехнологічний, яким користуються фахівці з нейролінгвістичного програмування.

8. Транспортний профайлінг, що використовується для забезпечення безпеки в галузі транспортного сполучення.

9. Готельний профайлінг, який вивчає особливості сприйняття готельного сервісу представниками різних народів.

10. Бізнес-профайлінг, який використовується під час бізнес-комунікацій та переговорів для виявлення правдивості намірів бізнес-партнерів.

11. Кадровий профайлінг – застосовується під час роботи з персоналом.

12. Банківський профайлінг, що використовується для оцінки банківських ризиків під час кредитування.

13. Страховий профайлінг, що дозволяє виявляти шахраїв, які хочуть отримати незаконну вигоду внаслідок страхового випадку.

Спершу термін «профайлінг» почав широко використовуватись як «авіаційний профайлінг» і передбачав опитування пасажирів та спостереження за ними для виявлення потенційно небезпечних осіб. А підготовку профайлерів для запобігання терористичним актам започаткували в Ізраїлі, ще у 80-х роках XX століття. Завдяки використанню профайлінгу авіакомпанія Ель-Аль (EL-AL) отримала статус однієї з найбезпечніших у світі [2, с. 133].

В основі профайлінгу є досягнення біології, психології та психолінгвістики, він містить методи для визначення особистісних характеристик людини з метою прогнозування та оцінки її дій.

На думку Е. С. Черкасової, терміном «профайлінг» позначають два різнопланові контексти діяльності правоохоронних органів. Перший із них – створення психологічного профілю невстановленої особи, яка вчинила злочин, на основі якого ця особа підлягає встановленню і притягненню до кримінальної відповідальності за вчинене. Інший контекст – технології спостереження під час огляду, з метою виявлення потенційно небезпечних осіб. Цей напрям активно реалізується за допомогою спеціалістів-психологів зі спеціалізацією в сфері біхевіоризму (наукове вчення поведінки) [4].

Потрібно виокремити декілька основних напрямів застосування методик профайлінгу під час розкриття та розслідування злочинів [5]:

1. *Складання психолого-криміналістичного портрета злочинця.* За визначенням А. І. Анфіногенова, «психологічний портрет злочинця – це психолого-криміналістичний метод і результат пізнання кримінальної події, орієнтований на виявлення комплексу відомостей про індивідуальні ознаки і особливості особистості суб'єкта злочину, що проявилися в сукупності обставин і слідах злочинної діяльності» [6].

Психолого-криміналістичний портрет дає змогу здійснювати пошук невідомого злочинця, а тому оперативні підрозділи й органи досудового розслідування можуть використовувати його під час розкриття і розслідування неочевидних злочинів.

Психолого-криміналістичний портрет також може використовуватися під час планування та проведення окремих слідчих дій; є основою тактики проведення оперативно-розшукових заходів, перевірки слідчих і оперативних версій.

2. *Застосування методу «географічного профілювання».* Цей метод полягає в тому, щоб виявити системність у скоєнні злочинів в певних місцях, унаслідок чого можна виявити місце перебування злочинця.

3. *Використання прийомів верифікації.* На думку Н. А. Веренікіної, «верифікація є сукупністю методів, прийомів і способів оцінки достовірності (правдивості) показань на основі знань про психологію особистості, про вербальні і невербальні комунікації, оцінки індивідуальних ознак людини» [5].

Концепція профайлінгу ґрунтується на тому, що протиправна дія та її підготовка можуть бути виявлені шляхом аналізу певних фізичних, психологічних, поведінкових ознак, що становлять характеристику підозрюваних осіб, з позицій їхньої потенційної небезпеки. Існують індикатори, які є критичними для віднесення конкретної особи до групи ризику (демонстрована агресія, прихована агресія, збудженість, відчуженість). Емоційний стан людини, який оцінюється за ознаками тривоги, страху, хвилювання тощо, розглядається як додатковий чинник під час аналізу виявлених домінуючих ознак. Є ключові ознаки у невербальній і вербальній поведінці людини, які дають змогу профайлерам виявити таку особу

в людському середовищі й віднести до категорії потенційно небезпечних.

2. Перспективи використання профайлінгу для боротьби з кіберзлочинністю

Значну перспективу має застосування профайлінгу в сфері інформаційної безпеки. Людський фактор є основною причиною виникнення загроз інформаційній безпеці (74% випадків за даними Ponemon Institute) [7]. І саме усунення цих загроз є завданням служб безпеки.

У діяльності служб інформаційної безпеки найбільший ефект дає прогнозування ризиків, а не фіксація порушень і здійснення службових розслідувань. Із цією метою використовуються технології аналізу поведінки User and Entity Behavioral Analytics (UBA/UEBA) – це клас систем, що дозволяють будувати моделі поведінки користувачів на основі масивів даних про них та про ІТ-обладнання за допомогою алгоритмів машинного навчання та статистичного аналізу. Як джерело даних для цих систем можуть використовуватися файли журналів мережевих і серверних компонентів, журнали систем безпеки, журнали з кінцевих станцій, дані систем автентифікації та зміст поштових повідомлень, повідомлень у месенджерах та у соціальних мережах [8]. Ці системи вивчають поведінку користувачів і фіксують зміни звичної поведінки.

Але автоматизований профайлінг зосереджується не на діях, а на особистісних характеристиках користувачів, використовуючи тексти їхнього робочого листування. З цих текстів робиться вибірка фрагментів, які демонструють індивідуальні особливості мови користувачів. Враховується довжина та складність речень, використання займенників, дієслів, пунктуація, словниковий запас користувачів, слова-паразити тощо. Загалом ураховуються понад 70 критеріїв, результати оцінки яких перевіряються на відповідність 8 психотипам класичного профайлінгу. І хоча у кожній особі можуть поєднуватися явища декількох психотипів, профайлери виокремлюють пару найбільш яскравих, які доповнюють один одного. Алгоритм виокремлює таку пару і формує профіль особи з попередженням про ризики. Точність прогнозів такої системи 75–85%, але вона може збільшуватися внаслідок урахування голосу, міміки, інтонації, клавіатурного почерку [9].

Нині застосуванням профайлінгу в сфері інформаційної безпеки займається російська компанія «СёрчИнформ», яка розробила програму для автоматизації профайлінгу «КИБ СёрчИнформ ProfileCenter». Ця програма складає психологічні профілі співробітників у автоматичному режимі та попереджує ризики від впливу людського фактора [7].

Також важливу роль відіграє профайлінг під час розслідування кіберзлочинів. Профайлінг допомагає слідчому робити висновки щодо злочинця чи місця злочину. Зважаючи на значне зростання кількості кіберзлочинів, розслідування кіберзлочинів є дуже актуальним завданням. Звичайно, не всі методики класичного профайлінгу можна застосувати до кіберзлочинів, але, на думку американського слідчого та фахівця з кібербезпеки Р. Йепеса (Yepes, 2016), основна методологія «чому+як=хто» може бути використана під час профілювання кіберзлочинів [10]. Визначення причини та способу скоєння злочину сприяє викриттю особи злочинця. Слідчі й оперативні працівники можуть розробляти профілі підозрюваних на основі аналізу деталей кіберзлочинів. Для цього вони мусять бути не лише фахівцями з профайлінгу, а й фахівцями з інформаційних технологій, кібербезпеки та цифрової криміналістики. Завдання працівника кіберполіції полягають у виявленні списку підозрюваних (чи вони діяли із-зовні, чи є інсайдерами), у вивченні атаки з технологічного боку, виявленні рівня майстерності хакера, у дослідженні жертви і мети нападу. Вивчення цих питань дає змогу звузити список підозрюваних. Але без розуміння інформаційних технологій профайлер не зможе точно визначити кіберзлочинця [10].

Як вважає Д. Шіндер (Shinder, 2010), у процесі профайлінгу більшість кіберзлочинців можуть бути описані такими характеристиками:

– певний рівень технічних знань;
– нехтування законом;
– потреба у ризику;
– насолода від маніпулювання іншими;
– мотив злочину – гроші, емоції, політичні чи релігійні переконання, сексуальне задоволення та бажання розважитися [11].

На думку Н. Гарсіа (Garcia, 2018) з Utica College в Utica, New York, розуміючи профіль кіберзлочинців, слідчі можуть розвивати свої стратегії боротьби з кіберзлочинністю та зменшувати поточну статистику кіберзлочинності [12].

Зокрема профайлінг може допомогти у прив'язці кіберзлочинів на різних об'єктах до однієї хакерської групи, оскільки злочинці під час скоєння злочину залишають кіберслід, характерний саме для них. Злочинець у своїх діях використовує певний шаблон, який відображає його особистість. Один злочинець може використовувати вірус, який розповсюджується через електронну пошту і знищує дані, а інший здійснює злам через комп'ютерну

мережу. Шляхом аналізу кіберслідів можна з'ясувати технічні навики злочинця, що допоможе визначити його Modus operandi, тобто усталений спосіб учинення злочинів. Також профайлінг дає змогу визначити мотив злочину (наприклад, гроші, емоції, сексуальні мотиви, бажання розважитися, релігія, політика).

Під час розслідування комп'ютерних злочинів здійснюється системний аналіз і мережевий аналіз. Системний аналіз – це аналіз файлової системи комп'ютера злочинця чи жертви, який дозволяє виявити змінені файли та їх вміст, а також це перевірка записів у файлах журналу. Мережевий аналіз охоплює дослідження файлів журналів, що містять вхідний і вихідний мережевий трафік. Під час тривалої мережевої атаки можна за допомогою маршрутизатора чи шлюзу здійснити реєстрацію мережевого трафіка, необхідного для аналізу. Результати аналізу можуть бути використані для створення профілю злочинця. Експерти досліджують підписи, файли журналів, інтернет-кеш, файли зображень, метадані файлів, сайти соціальних мереж, бо як і звичайні злочинці кіберзлочинці залишають сліди, які можуть бути використані для їх профілювання та викриття. Насамперед важливими є файли системних журналів, бо вони показують, що сталося та коли, і можуть бути використані як докази. Під час профілювання файли журналів допомагають зібрати інформацію для початку створення профілю. Метою профілювання є виявлення та спроба зрозуміти злочинця, який причетний до злочину [12].

Дуже важливим є правове регулювання використання профайлінгу в діяльності підрозділів кіберполіції Національної поліції України.

Діяльність Департаменту кіберполіції Національної поліції України регулюється Положенням про Департамент кіберполіції Національної поліції України, затвердженим наказом Національної поліції України від 10.11.2015 № 85 [13]. Як і будь-який інший підрозділ Національної поліції України Департамент кіберполіції Національної поліції України керується нормами Закону України «Про Національну поліцію» [14]. Також Департамент кіберполіції керується нормами Закону України «Про ратифікацію Конвенції про кіберзлочинність» [15]. Згідно з визначенням, яке дається на офіційному сайті кіберполіції України: «Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність» [16]. Тому він також керується Законом України «Про оперативно-розшукову діяльність» [17].

У жодному з цих нормативно-правових документів не передбачено використання профайлінгу в діяльності кіберполіції. Тому подальші розробки в галузі правового регулювання застосування профайлінгу підрозділами кіберполіції Національної поліції України є дуже важливими.

Висновки

Відсутність досвіду використання профайлінгу в діяльності оперативних підрозділів Національної поліції України, зокрема підрозділів кіберполіції, недооцінка його можливостей вимагає переосмислення. Технології профайлінгу можуть бути успішно впроваджені у діяльність оперативних підрозділів Національної поліції, в тому числі підрозділів кіберполіції, що дасть змогу ефективніше протидіяти злочинності. З цією метою доцільно до наявних пошукових заходів додати на законодавчому рівні такий захід, як «оперативний профайлінг», що дасть змогу широко застосовувати його можливості. Також важливо здійснювати навчання працівників кіберполіції основам профайлінгу, для чого необхідно запровадити відповідну навчальну дисципліну в освітній процес закладів вищої освіти.

Список використаних джерел

1. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років – Opendatabot. URL: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot (дата звернення: 14.09.2020).
2. Дручек О. В. Профайлінг як метод забезпечення державної безпеки і громадського порядку: проблеми застосування. *Науковий вісник публічного та приватного права.* К., 2018. С. 132–136.
3. Виды профайлинга. URL: https://searchinform.ru/kontrol-sotrudnikov/profajling/vidy-profajlinga/ (дата звернення: 14.09.2020).
4. Черкасова Е. С. Психологический портрет лица, совершившего насильственное преступление, – профайлинг, как современное направление психологической науки. URL: http://yurpsy.com/files/xrest/3/9.htm (дата звернення: 14.09.2020).

5. Вереникина Н. А. Профайлинг, как средство раскрытия и расследования преступлений. URL: https://cyberleninka.ru/article/n/profayling-kak-sredstvo-raskrytiya-i-rassledovaniya-prestupleniy/viewer (дата звернення: 14.09.2020).
6. Анфиногенов А. И. Психологический портрет преступника, его разработка в процессе расследования преступления : автореф. дис. на соиск. уч. степени канд. психол. наук : спец. 19.00.06. М., 1997. 28 с.
7. Защита предприятия от человеческого фактора – профайлинг для информационной безопасности. *Promdevelop* от 28 апреля 2018. URL: https://promdevelop.ru/zashhita-predpriyatiya-ot-chelovecheskogo-faktora-profajling-dlya-informatsionnoj-bezopasnosti/ (дата звернення: 14.09.2020).
8. Матвеев А. Обзор рынка систем поведенческого анализа – User and Entity Behavioral Analytics (UBA/UEBA). URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba (дата звернення: 14.09.2020).
9. Профайлинг для ИБ: как программа «читает» человека (ч. 1). URL: https://www.computerra.ru/237804/profajling-dlya-ib-kak-programma-chitaet-cheloveka-ch-1/ (дата звернення: 14.09.2020).
10. Yepes R. The Art of Profiling in a Digital World. *The Police Chief 83* (February 2016). URL: https://www.policechiefmagazine.org/the-art-of-profiling-in-a-digital-world/ (дата звернення: 14.09.2020).
11. Shinder D. Profiling and categorizing cybercriminals // Tech & Work on July 19, 2010. URL: https://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/ (дата звернення: 14.09.2020).
12. Garcia N. The use of criminal profiling in cybercrime investigations. Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity. URL: https://www.researchgate.net/publication/327187114_The_use_of_criminal_profiling_in_cybercrime_investigations (дата звернення: 14.09.2020).
13. Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Національної поліції України від 10.11.2015 № 85. Єдиний загальнодержавний публічний ресурс законодавчих та нормативно-правових актів, які стосуються діяльності поліцейських. URL: http://tranzit.ltd.ua/nakaz/ (дата звернення: 21.09.2020).
14. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України.* 2015. № 40–41. Ст. 379.
15. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. *Відомості Верховної Ради України.* 2006. № 5, 5–6. С. 128. Ст. 71.
16. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 21.09.2020).
17. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України.* 1992. № 22. Ст. 303.

References

1. Kil`kist` kiberzlochy`niv v Ukrayini zrosla vdvichi za ostanni pyat` rokiv – Opendatabot [The number of cybercrimes in Ukraine has doubled in the last five years]. Retrieved from https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot [in Ukr.].
2. Druchek, O. V. (2018). Profajling yak metod zabezpechennya derzhavnoyi bezpeky` i gromads`kogo poryadku: problemy` zastosuvannya [Profiling is a method of securing state security and a public order: problems of application]. *Naukovyi visnyk publichnogo ta pry`vatnogo prava (Scientific Bulletin of Public and Private Law)*, 132–136 [in Ukr.].
3. Vidy profaylinga [Types of profiling]. Retrieved from https://searchinform.ru/kontrol-sotrudnikov/profajling/vidy-profajlinga/ [in Russ.].
4. Cherkasova, E. S. (2013). Psihologicheskiy portret litsa, sovershivshego nasilstvennoe prestuplenie, – profayling, kak sovremennoe napravlenie psihologicheskoy nauki [Psychological portrait of a person who has committed a violent crime – profiling as a modern trend in psychological science]. Retrieved from http://yurpsy.com/files/xrest/3/9.htm [in Russ.].
5. Verenikina, N. A. (2017). Profayling, kak sredstvo raskryitiya i rassledovaniya prestupleniy [Profiling as a means of detecting and investigating crimes]. Retrieved from https://cyberleninka.ru/article/n/profayling-kak-sredstvo-raskrytiya-i-rassledovaniya-prestupleniy/viewer [in Russ.].
6. Anfinogenov, A. I. (1997). Psihologicheskij portret prestupnika, ego razrabotka v processe rassledovanija prestuplenija [Psychological portrait of the criminal, his development in the process of investigating the crime]. M. [in Russ.].
7. Zaschita predpriyatiya ot chelovecheskogo faktora – profayling dlya informatsionnoy bezopasnosti [Protection of the enterprise from the human factor – profiling for information security]. Promdevelop ot 28 aprelya

2018 (Promdevelop dated 28/04/2018). Retrieved from https://promdevelop.ru/zashhita-predpriyatiya-ot-chelovecheskogo-faktora-profajling-dlya-informatsionnoj-bezopasnosti/ [in Russ.].
8. Matveev, A. (2017). Obzor rynka sistem povedencheskogo analiza – User and Entity Behavioral Analytics (UBA/UEBA) [Market overview of behavioral analysis systems – User and Entity Behavioral Analytics (UBA/UEBA)]. Retrieved from https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba [in Russ.].
9. Profayling dlya IB: kak programma «chitaet» cheloveka (ch. 1) [Profiling for information security: how the program «reads» a person (part 1)]. Retrieved from https://www.computerra.ru/237804/profajling-dlya-ib-kak-programma-chitaet-cheloveka-ch-1/ [in Russ.].
10. Yepes, R. (2016). The Art of Profiling in a Digital World. *The Police Chief 83*. Retrieved from https://www.policechiefmagazine.org/the-art-of-profiling-in-a-digital-world/
11. Shinder, D. (2010). Profiling and categorizing cybercriminals. *Tech & Work on July 19, 2010*. Retrieved from https://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/
12. Garcia, N. (2018). The use of criminal profiling in cybercrime investigations: Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity. Retrieved from https://www.researchgate.net/publication/327187114_The_use_of_criminal_profiling_in_cybercrime_investigations
13. Pro zatverdzhennya Polozhennya pro Departament kiberpoliciyi Nacionalnoyi Policiyi Ukrayiny: Nakaz Nacionalnoyi Policiyi Ukrayiny vid 10.11.2015 № 85 [On approval of the Regulations on the Cyberpolice Department of the National Police of Ukraine: Order of the National Police of Ukraine from 10/11/2015 No. 85]. Yedynyi zahalnoderzhavnyi publichnyi resurs zakonodavchykh ta normatyvno-pravovykh aktiv, yaki stosuiutsia diialnosti politseiskykh (The only national public resource of laws and regulations relating to police activities). Retrieved from http://tranzit.ltd.ua/nakaz/ [in Ukr.].
14. Pro Natsionalnu politsiiu: Zakon Ukrainy vid 02.07.2015 r. № 580-VIII [On the National Police: Law of Ukraine No. 580-VIII of July 02, 2015]. *Vidomosti Verkhovnoi Rady Ukrainy (Bulletin of the Verkhovna Rada of Ukraine)*, 40–41, Art. 379 [in Ukr.].
15. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist [Ratification of the Convention on Cybercrime: Law of Ukraine] vid 07.09.2005 № 2824-IV. *Vidomosti Verkhovnoi Rady Ukrainy (Bulletin of the Verkhovna Rada of Ukraine)*, 5. St. 71 [in Ukr.].
16. Oficijny`j sajt kiberpoliciyi Ukrayiny` [Official site of the cyberpolice of Ukraine]. Retrieved from https://cyberpolice.gov.ua/contacts/ [in Ukr.].
17. Pro operatyvno-rozshukovu diialnist: Zakon Ukrainy vid 18 liutoho 1992 roku № 2135-XII [On search operations: Law of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy (Bulletin of the Verkhovna Rada of Ukraine)*, 22. St. 303 [in Ukr.].

Стаття: надійшла до редакції 24.09.2020
прийнята до друку 12.11.2020
The article: is received 24.09.2020
is accepted 12.11.2020