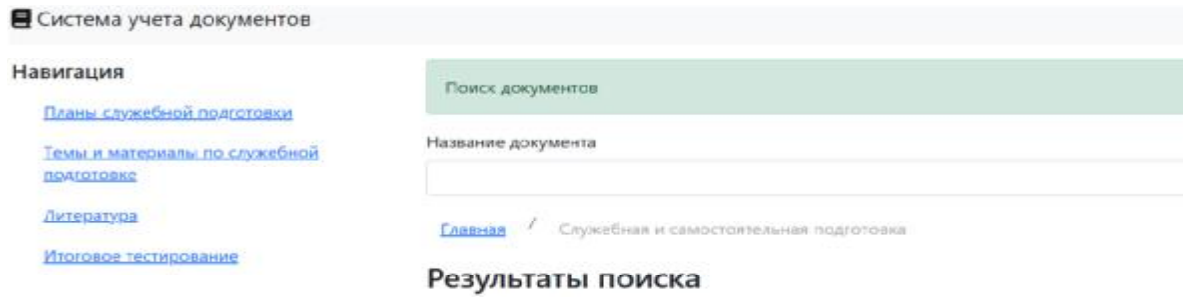


*Рис. 7*. Раздел «Служебная подготовка»

Отдельно необходимо обратить внимание и на то, что указанный электронный криминалистический ресурс с учетом соблюдения принципа безопасности распространения справочной информации криминалистического характера может быть представлен в виде мобильного приложения для сотрудников ОВД.

Подводя итог, подчеркнем, что от ученых-криминалистов в современных условиях борьбы с преступностью требуется не только исследование различных проблем раскрытия и расследования преступлений, но и изучение эффективности обеспечения внедрения в практическую деятельность разрабатываемой криминалистической продукции. Разработка и внедрение электронного криминалистического ресурса позволит повысить уровень криминалистического образования в рамках служебной подготовки и самообразования у сотрудников ОВД и эффективность практической деятельности, связанной с проведением проверок по заявлениям или сообщениям о преступлениях, дознания по уголовным делам, а также исполнения поручений следователей.

**Список использованных источников**

1. Волынский, А. Ф. Некоторые проблемы реализации социальных функций криминалистики / А. Ф. Волынский, И. В. Тишутина // Вестн. Владим. юрид. ин-та. – Владимир : ВЮИ ФСИН России. – 2009. – № 3. – С. 46–50.

2. Криминалистика социалистических стран / В. Я. Колдин [и др.]. – М. : Юрид. лит., 1986. – 517 с.

3. Логвин, В. М. О необходимости совершенствования криминалистического обеспечения деятельности органов внутренних дел / В. М. Логвин // I Минские криминал. чтения : материалы Междунар. науч.-практ. конф. : в 2 ч., Минск, 20 дек. 2018 г. – Минск, 2018. – Ч. 1. – С. 227–232.

4. Сокол, В. Ю. Тактико-криминалистическое обеспечение раскрытия и расследования преступлений (Методологические и организационные аспекты) : дис. ... канд. юрид. наук : 12.00.09 / В. Ю. Сокол ; Акад. федер. службы безопасности Рос. Федерации. – М., 1998. – 188 л.

5. Субботина, М. В. Криминалистические проблемы расследования хищений чужого имущества : дис. ... д-ра юрид. наук : 12.00.09 / М. В. Субботина ; Волгогр. акад. МВД России. – Волгоград, 2004. – 421 л.

6. Цховребова, И. А. Криминалистическое обеспечение расследования преступлений : сущность и содержание / И. А. Цховребова, В. В. Цховребов // Публич. и част. право. – 2018. – № 3. – С. 184–199.

Дата поступления в редакцию: 20.03.2024

УДК 343.985

***А. А. Чехович**, адъюнкт научно-педагогического факультета*
*Академии Министерства внутренних дел Республики Беларусь*
*e-mail: sanjess-hmr@mail.ru*

## ОПЕРАТИВНО-РОЗЫСКНАЯ ХАРАКТЕРИСТИКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

*Рассматриваются структура и содержание оперативно-розыскной характеристики несанкционированного доступа к компьютерной информации. Акцентируется внимание на особенностях ее элементов, перечень которых обосновывается как наиболее актуальный, включающий в себя описание специфики пред-*

*мета преступного посягательства, обстановки и места совершения, следы преступления и их локализацию, способ совершения, орудия совершения несанкционированного доступа к компьютерной информации, особенности личности преступника и личности потерпевшего. Анализируется содержание этих элементов для эффективного противодействия рассматриваемому виду преступления.*

*Ключевые слова: компьютерная информация, личность преступника, несанкционированный доступ к компьютерной информации, оперативно-розыскная характеристика, предмет преступного посягательства, способ совершения преступления.*

***A. A. Chekhovich**, Postgraduate Student of the Scientific and Pedagogical Faculty*
*of the Academy of the Ministry of Internal Affairs of the Republic of Belarus*
*e-mail: sanjess-hmr@mail.ru*

## DETECTIVE CHARACTERISTICS OF UNAUTHORIZED ACCESS TO COMPUTER INFORMATION

*The structure and content of the detective characteristics of unauthorized access to computer information are considered. Attention is focused on the features of its elements, the list of which is justified as the most relevant, which includes a description of the specifics of the subject of criminal encroachment, the situation and place of commission, traces of the crime and their localization, the method of commission, the instruments of unauthorized access to computer information, the personality of the criminal and the personality of the victim. The content of these elements is analyzed in order to effectively counteract the type of crime under consideration.*

*Keywords: computer information, the identity of the criminal, unauthorized access to computer information, detective characteristics, the subject of criminal encroachment, the method of committing a crime.*

На современном этапе развития мира неотъемлемой составляющей любой сферы функционирования социума являются информационные технологии, к применению которых в последнее время злоумышленники стали прибегать все чаще и активнее. Преступники, руководствуясь деструктивными мотивами, используя информационное пространство сети Интернет, совершают различные преступления, в том числе и несанкционированный доступ к компьютерной информации (НДКИ), ответственность за который предусмотрена ст. 349 Уголовного кодекса Республики Беларусь (УК).

НДКИ понимается как доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы их защиты, совершенный из корыстной заинтересованности либо повлекший за собой по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда. При этом НДКИ несет в себе не только экономическую угрозу отдельным гражданам, но и экономике страны в целом.

Согласно данным информационного центра МВД Республики Беларусь, в 2018 г. было зарегистрировано 912 таких преступлений, 2019 г. – 2 185, 2020 г. – 1 784, 2021 г. – 1 104, 2022 г. – 1 056, 2023 г. – 1 022. Указанная статистика свидетельствует о высокой доле НДКИ в структуре киберпреступности на территории республики и отсутствии тенденции к повышению уровня раскрываемости указанного вида преступления. Этот негативный фактор детерминирует угрозу национальной безопасности в информационной сфере, на что прямо указанно в п. 20 ст. 27 гл. 4, ст. 34 гл. 5 Концепции национальной безопасности Республики Беларусь. В Концепции национальной безопасности нарушение киберустойчивости национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем рассматривается как одна из основных угроз национальной безопасности Республики Беларусь в информационной сфере.

Преступление как объект познания рассматривается в науке по-разному. Именно поэтому существуют различные характеристики преступлений: уголовно-правовая, криминалистическая, криминологическая, виктимологическая, социальная, нравственно-психологическая. Для оперативно-розыскной науки учеными для описания свойств отдельных видов и форм преступлений разработана оперативно-розыскная характеристика (ОРХ) – теоретическая информационная модель преступления, которая отражает взаимосвязь ее элементов для выбора наиболее оптимального варианта использования оперативно-розыскных сил, средств и методов для наиболее качественного и быстрого раскрытия подготавливаемого или совершенного преступления.

По мнению А. М. Абрамова, ОРХ представляет собой систему свойств и информационных признаков, присущих определенному виду преступлений, знание которых способствует эффективному решению организационно-тактических задач по их предупреждению и раскрытию, а также служит теоретической и информационной основой для разработки тактических приемов с целью эффективного раскрытия конкретных преступлений [1]. Однако данное определение затрагивает только теоретическое назначение ОРХ, а ее практическое назначение определено не в полном объеме.

И. И. Басецкий, например, определяет ОРХ как совокупность гласной и негласной информации о распространенности этого вида преступлений в республике, их характере, особенностях проявления: всесторонне раскрывает содержание понятия ОРХ, трактует ее теоретическое и практическое предназначение [2].

По мнению Д. В. Гребельского, ОРХ есть совокупность информационных признаков, упорядоченных и взаимосвязанных между собой, почерпнутых из различных информационных источников (входящих прежде всего в криминалистическую, криминологическую, психологическую, социологическую, экономическую и другие характеристики преступлений) [3].

Обобщив указанные характеристики, можно заключить, что ОРХ – это информационная модель, использующая значимые в оперативно-розыскной деятельности сведения с целью определения наиболее оптимальных направлений противодействия отдельным видам преступлений с учетом особенностей оперативно-розыскных сил, средств и методов, основанная на анализе негласной и гласной информации о подготавливаемых, совершаемых и совершенных преступлениях и причастных к ним лицах.

Любая ОРХ отдельного вида преступлений имеет отличительные по качеству и количеству показатели от частично сходных характеристик других видов преступлений. С учетом таких различий и специфики решаемых на практике задач по выявлению, раскрытию и предупреждению преступлений посредством использования оперативно-розыскных сил, средств и методов целесообразно использовать и разные подходы к разработке рассматриваемых характеристик.

В настоящее время ОРХ НДКИ еще не разработана. Тем не менее в отдельных публикациях криминалистической характеристики НДКИ фрагментарно указываются элементы, которые могут использоваться при построении ОРХ НДКИ [4, 5].

Анализ мнений исследователей относительно содержания ОРХ позволяет акцентировать внимание на том, что в состав ОРХ входит оперативная информация, не всегда выступающая в качестве доказательства в уголовном деле, к которой относятся подтвержденные в ходе ОРД сведения о преступной деятельности и данные о периоде подготовки к совершению преступления.

Для детальной разработки ОРХ НДКИ логично и обоснованно выбрать элементный подход построения. При этом важно учитывать все особенности такой характеристики: эффективность анализа оперативной и иной информации, выдвижение версии для раскрытия указанного вида преступления, планирование, совершенствование организации и тактики ОРД. ОРХ НДКИ, как единый комплекс, должна быть практически ориентирована, когда установлены и типизированы непосредственные и опосредованные связи и зависимости между ее элементами. В целом критерии отбора элементов ОРХ НДКИ должны включать в себя их закономерную повторяемость (устойчивость), научную обоснованность, практическое применение.

Анализ оперативно-розыскной практики показывает, что из всех возможных структурных элементов ОРХ целесообразно рассмотреть особенности предмета преступного посягательства, обстановку и место совершения НДКИ, следы преступления и их локализацию, способ совершения НДКИ, орудия совершения преступления, особенности личности преступника и особенности личности потерпевшего.

Структурные элементы ОРХ НДКИ «личность преступника», «способ совершения НДКИ», «орудия преступления», «обстановка совершения преступления», «следы преступления» находятся в зависимости друг от друга и во взаимосвязи. Способ совершения НДКИ предопределяет применение орудия преступления, вид и назначение которого устанавливают особенности и вид следов преступления. По специфике обнаруженных следов преступления выявляются качественные характеристики совершенного НДКИ и примененного при этом орудия преступления: аппаратного, программного или их в комплексе. Совершение НДКИ с использованием рассматриваемого способа и орудия преступления характерно для преступников с определенными ха-

рактеристиками личности (наличие специальных знаний, профессиональных навыков, умений по изготовлению технических устройств для совершения НДКИ и т. д.). Взаимосвязь указанных структурных элементов ОРХ НДКИ позволяет с помощью сведений об одном из элементов (например, о способе совершения) установить содержание и характерные свойства неизвестных элементов (личность преступника, орудия преступления, следы преступления).

Особенность предмета преступного посягательства, указанного в ст. 349 УК, составляет компьютерную информацию, понятие которой закреплено в п. 18 ч. 5 ст. 4 УК. Под таковой понимается информация, хранящаяся в компьютерной системе, сети или на машинных носителях, обрабатываемая компьютерной системой либо передаваемая в пространстве с помощью любых программно-технических средств. Анализ Закона Республики Беларусь «Об оперативно-розыскной деятельности» показывает, что важнейшим атрибутом КИ является ее существование в форме, доступной для получения, передачи, сбора, обработки, накопления, хранения, распространения или предоставления КИ системой, информационной сетью или машинным носителем, а также для обеспечения защищенности и подлинности этой информации. Ученые Республики Беларусь и зарубежных стран приводят различные авторские дефиниции термина «компьютерная информация» [6, 7]. Большинство авторов склоняется к тому, что КИ – это сведения, хранящиеся в памяти средств компьютерной техники (СКТ) или на машинных носителях [6, 7]. На наш взгляд, указанный подход обоснован, так как КИ не может существовать вне СКТ или машинного носителя. Более того, ее обработка (создание, редактирование, хранение) производится исключительно в СКТ при помощи программных продуктов, которые также не могут существовать вне СКТ или машинных носителей информации. Соответственно, сам программный продукт есть набор команд, хранящихся в памяти СКТ или на машинном носителе, который является КИ.

Выделение КИ в качестве самостоятельного предмета обусловлено ее специфическими характеристиками. Она не может существовать в материальном мире, вне компьютера, компьютерной сети, машинного носителя информации; при ее потреблении не исчезает и не подвержена никакому износу; может быть растиражирована в неограниченном количестве, а также создана и изменена только при помощи СКТ; проста в создании и обработке; легко удаляется при помощи СКТ и передается по компьютерным сетям в рекордно короткие сроки на неограниченные расстояния. При всем указанном наиболее специфическим свойством КИ является то, что при ее изъятии она сохраняется в первоисточнике, и доступ к ней могут иметь одновременно неограниченное число пользователей из любой точки мира без учета географических и административных границ, например, при работе с информацией, содержащейся в одном файле. При этом изъятая КИ в виде файла на машинном носителе будет определена СКТ, как вновь созданная.

Немаловажным фактором НДКИ является и то, что он должен сопровождаться нарушением системы защиты КИ, как указанно в ст. 349 УК. В данную систему защиты входят правовые, организационные и технические средства защиты информации. Несанкционированным будет признан доступ к КИ, связанный с нарушением хотя бы одного из средств системы защиты КИ, а также совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда, а также повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия.

Обстановка совершения НДКИ – совокупность условий и обстоятельств совершения преступления – существенно значима для раскрытия преступления, имеет ряд отличительных особенностей, не свойственных для большинства иных преступлений. Обычно ее определяют обстоятельства, характеризующие пространственные, временные, вещественные, технические, психологические особенности события рассматриваемого преступления.

Согласно сведениями информационного центра МВД Республики Беларусь (далее – ИЦ МВД Республики Беларусь)[1], подавляющее большинство НДКИ совершено путем удаленного доступа с использованием сети Интернет. При этом преступному посягательству в основном подвергаются персональные страницы пользователей популярных социальных сетей и мессенджеров

[1] Здесь и далее приводятся сведения информационного центра МВД Республики Беларусь за 2018–2023 гг. о зарегистрированных на территории Республики Беларусь преступлениях, предусмотренных ст. 349 УК.

(например, Viber, Instagram, vk.com), а также программное обеспечение автоматизации и оптимизации организационных и производственных процессов индивидуальных предпринимателей и юридических лиц (например, семейства «1С» (Бухгалтерия, Руководитель)). Встречаются также единичные случаи НДКИ дисконтных программ сети продовольственных магазинов. При этом установление злоумышленников по таким преступлениям имеет ряд трудностей, что обусловлено тем, что при совершении НДКИ кроме удаленного доступа, чаще всего осуществляемого за пределами Республики Беларусь, преступники скрывают идентификаторы присутствия в сети и возможности различных современных устройств для доступа к интернету во время перемещения. Для этого используются подменные IP-адреса, VPN-серверы, общественные места с подключением по технологии Wi-Fi либо (приобретенные в теневой части сети Интернет «Даркнет») пароли доступа к сетям частных лиц или компаний. При этом при выявлении незаконных действий в сети отобразятся идентификационные данные лиц, не причастных к совершенному НДКИ. Возможности современных устройств доступа к интернету (в частности их мобильность) позволяют злоумышленникам осуществлять противоправные действия даже в движении (например, в общественном транспорте), и данный фактор вызывает трудности при определении места совершения преступления.

Само совершение НДКИ достаточно специфично, как и его следовая картина. Для последней характерно нахождение следов в разных местах одновременно и на большом расстоянии друг от друга. Под следами совершения НДКИ преимущественно понимаются цифровые следы – КИ о факте совершения НДКИ, занимающие промежуточное звено между идеальными и материальными следами с учетом специфики их природы. Любые действия с КИ оставляют цифровые следы, т. е. информацию о событиях или действиях, отраженную в материальной среде в процессе ее возникновения, обработки, хранения и передачи. Цифровые следы аналогично КИ не могут существовать вне среды оборота КИ и также подвержены способам обработки (копированию, удалению, удаленному доступу) КИ. Для человека такая информация доступна только при использовании специализированных программных и аппаратных средств, осуществляющих декодирование и визуализацию в привычной графической, текстовой или звуковой форме. Здесь важно отметить, что из-за своей подвижности и сложной структуры хранения подобного рода данные могут быть получены и интерпретированы в полном объеме и без изменения содержания только с использованием специальных знаний, так как это журналы доступа к операционной системе, дампы[1] памяти машинных носителей информации, где она представлена в не привычном для обычного пользователя, не обладающего специальными знаниями, виде [8].

Применительно к социальным сетям в случае несанкционированного доступа при условии сохранения возможности доступа потерпевшего к своему аккаунту существует техническая возможность получить сведения о дате доступа к нему, имени устройства и его IP-адресе. Указанные цифровые следы хранятся на серверах социальных сетей достаточный период времени, что позволяет их получить и использовать при раскрытии преступления.

В случае НДКИ юридических лиц (обычно программное обеспечение семейства 1С, дисконтные программы торговых сетей) цифровые следы находятся на сторонних серверах и фрагментарно в физической памяти СКТ, осуществляющих управление указанным программным обеспечением. В данном случае цифровые следы изымаются и исследуются при проведении компьютерной технической экспертизы. Во-первых, это могут быть IP-адреса СКТ, использованные для НДКИ, которые обычно хранятся в журналах доступа к информационным ресурсам в рабочем браузере; web-версии программного обеспечения, журналы доступа к электронной почте юридического лица (на которых также могут сохраниться цифровые следы НДКИ: IP-адрес устройства, с которого осуществлен вход в почтовый ящик, время и регистрация провайдера в момент входа).

Учитывая двойственность природы компьютерной программы (инструмент для работы с КИ, в то же время программа сама по себе есть КИ), следует иметь в виду, что вариантов следов совершения НДКИ может быть несколько: цифровые следы, оставленные на стороннем ресурсе или СКТ, оставленные при подготовке к совершению несанкционированного доступа, т. е. исходные коды и файлы для написания вредоносного программного обеспечения, а также програм-

[1] Снимок информации о состоянии компьютерной системы.

мы для подбора идентификаторов доступа в закрытые сети, социальные сети или к КИ, доступ к которой ограничен паролем доступа. Программные продукты для подбора идентификаторов доступа представляют собой программу с алгоритмом действия, которая при НДКИ остается только в памяти СКТ злоумышленника. При этом при установлении и задержании преступника, совершившего НДКИ, в первую очередь необходимо изъять устройства хранения информации СКТ, а также все устройства для доступа к сети Интернет, используемые злоумышленником. В таком случае даже при условии уничтожения следов написания вредоносного ПО, самого вредоносного ПО, которое использовалось преступником для совершения НДКИ, а также идентификаторы доступа к облачным хранилищам, где возможно хранение информации о противоправной деятельности (вредоносное ПО, исходные коды такого ПО), будет возможность зафиксировать и изъять для последующего исследования в рамках компьютерной технической экспертизы и использования в качестве доказательств.

К способам совершения НДКИ относится взлом системы защиты КИ (состоит из комплекса правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации), на что указанно в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, устанавливающие условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

К организационным мерам по защите информации относятся процедура обеспечения особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации); разграничение доступа к информации по кругу лиц и характеру информации.

При нарушении организационных средств защиты информации преступники чаще всего, используя служебное положение и имеющиеся у них идентификаторы доступа, осуществляют доступ к конфиденциальной КИ или к машинным носителям информации, копируют, изменяют или похищают конфиденциальные сведения полностью либо идентификационные данные для доступа к таким сведениям. Чаще всего такой вид НДКИ преступники осуществляют по вине потерпевших, например, в случае увольнения сотрудника либо его перемещении внутри организации, когда не производится процедура смены идентификаторов доступа к электронной почте, программному обеспечению автоматизации и оптимизации организационных и производственных процессов.

К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации и контролю защищенности информации. Анализ сведений ИЦ МВД Республики Беларусь показывает, что большинство НДКИ преступники совершают, нарушая технические средства защиты информации.

При НДКИ, сопряженном с нарушением технических мер по защите КИ, преступники используют средства социальной инженерии, когда необходимые идентификаторы для доступа в закрытые сети передачи информации либо к персональным страницам в социальных сетях получают непосредственно у потерпевших, применяя психологические приемы воздействия.

Вторым, не менее распространенным способом совершения НДКИ, является использование специально созданного программного обеспечения по подбору паролей для несанкционированного доступа к информационному ресурсу. Программный продукт для подбора паролей имеет определенный алгоритм действия, несложен в изготовлении при наличии соответствующих навыков.

Способ совершения НДКИ детерминирует выбор преступником определенного орудия противоправного деяния. При НДКИ это СКТ и программные продукты (специально созданные или приспособленные).

Специально созданные программы способны из заданного пользователем диапазона символов подобрать в максимально короткие сроки пароль доступа к сведениям ограниченного доступа или сети, где такие сведения циркулируют. Данная технология взлома системы защиты получила название «Брутфорс» (от англ. brute force – грубая сила), когда преступник получает

доступ к информации ограниченного доступа или закрытой сети путем подбора идентификаторов. Преимущественно такое ПО представляет собой единичный файл небольшого объема (от нескольких килобайт до одного гигабайта), не отличающийся разнообразным и понятным интерфейсом. Наиболее распространенным является ПО с интерфейсом командной строки, вредоносное воздействие которого заключается в быстром (до нескольких сотен в секунду) вводом паролей из заданного диапазона символов. При этом установленные программные средства защиты информации не фиксируют НДКИ, так как доступ осуществляется с использование зарегистрированных в системе идентификаторов.

При построении ОРХ основным наиболее рациональным критерием классификации личности преступников будет уровень владения СКТ. По этому критерию можно выделить две группы преступников. К первой группе будут относиться преступники высокого уровня владения СКТ, обладающие навыками написания кодов программных продуктов, способные на сокрытие своего сетевого присутствия путем уничтожения всевозможных следов противоправной деятельности, другими словами, способные оказывать активное противодействие раскрытию совершенного преступления. Такого рода преступники действуют либо в одиночку, когда преследуют определенные личные цели, либо группой, когда их цель НДКИ – большая материальная выгода.

Ко второй группе будут относиться преступники, обладающие минимальными знаниями уровня базового пользователя СКТ, способные использовать приемы социальной инженерии либо получать в теневом сегменте «Даркнет» необходимые сведения, такие как идентификационные данные и пароли владельцев банковских карт, специально разработанное программное обеспечение для подбора идентификационных данных потенциальной жертвы, преследующие цель получить незначительные материальные блага от НДКИ. Такие преступники редко обладают навыками противодействия раскрытию совершенного преступления, оставляют цифровые следы своей противоправной деятельности, не прикладывая особых усилий для их сокрытия. Как правило, они реализуют свой преступный умысел исключительно ради получения материальных благ, мести и др.

Потерпевшим сегодня может стать любой человек, использующий СКТ в своей повседневной жизни, а также организация или юридическое лицо, использующее в своей хозяйственной деятельности программные продукты для частичной автоматизации и оптимизации процесса хозяйственной деятельности с помощью СКТ и специально созданных для таких целей соответствующих программных продуктов. По сведениям ИЦ МВД Республики Беларусь, интерес с целью совершения НДКИ в отношении физических лиц у преступников представляют персональные страницы наиболее популярных социальных сетей, а юридические лица и индивидуальные предприниматели наиболее часто подвергаются НДКИ, содержащейся в программном обеспечении семейства «1С».

Преступный умысел злоумышленников часто реализовывается из-за низкого уровня цифровой грамотности потерпевших, использующих простые пароли с минимальным количеством символов, легкие для запоминания и быстрого ввода. При повседневном использовании они часто пересылают или сохраняют в памяти СКТ без какого-либо шифрования фотоизображения или записи идентификаторов доступа к интернет-банкингу, идентификаторы доступа к персональной странице в социальных сетях (более того, одинаковые либо максимально сходные по содержанию и количеству символов для разных страниц), реквизиты банковской платежной карты (БПК) и т. д. Анализ сведений ИЦ МВД Республики Беларусь и оперативно-розыскной практики позволяет выделить еще один аспект в определении потерпевших, представляющих интерес для преступников, по рассматриваемому виду преступления. Речь идет о количественном показателе категории «друзья» либо «подписчики» персональной страницы потерпевшего в социальной сети. Преступным посягательствам подвергаются в основном страницы данных социальных сетей, где вышеуказанный показатель находится в пределах до ста человек. Такой аспект преступниками используется с психологической точки зрения. Небольшое количество друзей или подписчиков предполагает более плотное и доверительное общение в сети пользователей – потенциальных жертв, когда в случае совершения в отношении их страницы НДКИ и рассылки сообщении с просьбой о помощи в виде перевода безналичным путем на БПК или электронный кошелек незначительной суммы денег, что не вызовет подозрений. Расчет пре-

ступников в данном случае направлен не на достижение максимально возможной суммы материальной выгоды, а на гарантированный успех совершения НДКИ с возможностью реализации материальной выгоды.

В отношении предпринимателей и юридических лиц при совершении атаки на используемый ими программный продукт семейства «1С» преступники в качестве жертвы чаще выбирают небольшую частную компанию или государственную организацию, обладающую средними по объему материальными активами, для которой важен в первую очередь рейтинг на рынке предоставляемых услуг. Алгоритм действий преступников при совершении НДКИ в отношении таких организации также направлен на подбор пароля доступа к системе, его изменение с целью исключения возможности для жертвы дальнейшего использования в повседневной деятельности заблокированного программного продукта с последующим вымогательством денежных средств за возвращение доступа к заблокированному программному продукту. Такой НДКИ может остаться латентным из-за отказа от обращения юридического лица в правоохранительные органы для сохранения рейтинга на рынке предоставляемых услуг и исключения огласки наступления негативных для организации последствий.

Таким образом, личность потерпевшего как элемент ОРХ имеет значение для раскрытия и предупреждения НДКИ, так как при изучении этой личности можно с большой долей вероятности определить способ совершения, орудия совершения НДКИ, так как указанные элементы ОРХ НДКИ находятся в непосредственной причинно-следственной взаимосвязи. Это способствует построению и проверке оперативно-розыскных версий относительно различных обстоятельств подготавливаемого либо совершенного НДКИ, наиболее качественному планированию отдельных оперативно-розыскных мероприятий, а также повышению эффективности их проведения и ОРД в целом.

Установление связи между признаками элементов ОРХ НДКИ позволяет определить оптимальную структуру практически значимых элементов, без знания которых процесс раскрытия преступления будет значительно затруднен как на первоначальном этапе, так и на последующих. При этом установление хотя бы одного элемента и его свойств способствует установлению остальных, ранее неизвестных элементов ОРХ НДКИ, входящих в ее структуру. В таком случае данные об элементах и связях между ними ориентируют сотрудников оперативных подразделений на выдвижение наиболее вероятных версий при раскрытии рассматриваемого преступления, содействуют определению задач по раскрытию НДКИ и установлению лица, его совершившего.

Итак, предложенная ОРХ НДКИ обеспечит получение более точных знаний о НДКИ, повысит качество анализа возможного преступного поведения и развития динамики преступности в сфере НДКИ, для своевременного реагирования на изменение оперативной обстановки с целью его прогнозирования. Предложенная ОРХ НДКИ также поможет разработке методических рекомендаций по оперативному обслуживанию объектов и систем, которые могут быть подвергнуты НДКИ и реализации оперативными сотрудниками подразделений ПК криминальной милиции организационно-тактических форм ОРД. ОРХ НДКИ может также быть использована для: дальнейшего построения и развития ОРХ конкретных видов преступлений, совершенных в различных сферах компьютерных преступлений, а также устранения возникших и недопущения прогнозируемых негативных последствий наступления какого-либо вреда для общества и государства при НДКИ в целом.

**Список использованных источников**

1. Абрамов, А. М. К вопросу о содержании оперативно-розыскной характеристики вида преступлений / А. М. Абрамов, И. А. Климов // Актуальные вопросы борьбы с преступностью и проблемы их преподавания : сб. науч. тр. – М. : Моск. юрид. ин-т МВД России, 1996. – С. 83–84.

2. Басецкий, И. И. Квартирные кражи: теория и практика борьбы : моногр. / И. И. Басецкий, В. Ч. Родевич ; под ред. И. И. Басецкого. – Минск : Акад. МВД Респ. Беларусь, 1999. – 297 с.

3. Гребельский, Д. В. О соотношении криминалистических и оперативно-розыскных характеристик преступлений / Д. В. Гребельский // Криминалист. характеристика преступлений : сб. науч. тр. / под ред. Л. Н. Викторова, В. А. Образцова, А. А. Эйсмана. – М., 1984. – С. 70–73.

4. Козлов, В. Е. Теоретико-прикладные аспекты первоначального этапа расследования компьютерных преступлений : дис. … канд. юрид. наук : 12.00.09 / В. Е. Козлов ; Акад. МВД Респ. Беларусь. – Минск, 2000. – 96 л.

5. Лепёхин, А. Н. Криминалистическое обеспечение расследования преступлений против информационной безопасности : дис. … канд. юрид. наук : 12.00.09 / А. Н. Лепёхин ; Акад. МВД Респ. Беларусь. – Минск, 2007. – 185 л.

6. Бачила, В. В. Об уголовно-процессуальном аспекте понятия «компьютерная информация» / В. В. Бачила // Вестн. Акад. МВД Респ. Беларусь. – 2022. – № 2. – С. 156–160.

7. Вехов, В. Б. Проблемы определения понятия компьютерной информации в сфере унификации уголовного законодательства стран СНГ / Б. В. Вехов // Уголов. право. – 2004. – № 4. – С. 15–17.

8. Россинская, Е. Р. Концепция цифровых следов в криминалистике / Е. Р. Россинская, И. А. Рядовский // Аубакировские чтения : материалы Междунар. науч.-практ. конф. (Алматы, 19 февр. 2019 г.) / Алмат. акад. М-ва внутр. дел Респ. Казахстан им. Макана Езбулатова. – Алматы, 2019. – С. 6–8.

Дата поступления в редакцию: 28.03.2024

УДК 343.985

***О. Н. Шуляковский***, *начальник управления внутренних дел*
*Брестского областного исполнительного комитета*
*e-mail: UVD_Brest@mvd.gov.by*

## РАЗВИТИЕ ТЕОРЕТИКО-ПРАВОВЫХ ВЗГЛЯДОВ НА ПРОБЛЕМУ ЗАЩИТЫ ГРАЖДАН, ОКАЗЫВАЮЩИХ КОНФИДЕНЦИАЛЬНОЕ СОДЕЙСТВИЕ ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ

*Проанализированы взгляды отечественных и зарубежных ученых по вопросу защиты лиц, оказывающих содействие органам, осуществляющим оперативно-розыскную деятельность, на конфиденциальной основе. Обозначена роль указанного института в теории и практике оперативно-розыскной деятельности. Сделан вывод о необходимости комплексного исследования вопросов защиты конфидентов, определены основные направления научного осмысления указанной проблемы.*

*Ключевые слова: оперативно-розыскная деятельность, оперативно-розыскные мероприятия, конфиденты, защита граждан, оказывающих конфиденциальное содействие, меры по обеспечению безопасности.*

***O. N. Shulyakovsky***, *Head of the Department of Internal Affairs of the Brest Regional Executive Committee*
*e-mail: UVD_Brest@mvd.gov.by*

## DEVELOPMENT OF THEORETICAL AND LEGAL VIEWS ON THE PROBLEM OF PROTECTING CITIZENS PROVIDING CONFIDENTIAL ASSISTANCE

*The views of both domestic and foreign scientists on the protection of persons providing assistance to bodies engaged in detective activities on a confidential basis are analyzed. The role of this institute in the theory and practice of operational investigative activities is outlined. The conclusion is made about the need for a comprehensive study of the issues of protecting confidants, the main directions of scientific understanding of this problem are determined.*

*Keywords: detective activities, detective measures, confidants, protection of citizens providing confidential assistance, security measures.*

Практика государственных органов, осуществляющих оперативно-розыскную деятельность (ОРД), по выявлению и раскрытию преступлений свидетельствует, что использование результатов ОРД при возбуждении уголовных дел и доказывании в ходе их расследования сопряжено с угрозой личной и имущественной безопасности для лиц, непосредственно принимавших участие в подготовке и проведении оперативно-розыскных мероприятий (ОРМ), и для лиц, оказывавших содействие оперативным подразделениям на конфиденциальной основе.

В деятельности оперативных подразделений могут иметь место случаи противоправного воздействия на конфидентов различными способами для причинения вреда их имуществу и здоровью, вплоть до физического устранения. Причиной происходящего выступает именно факт содействия правоохранительным органам. Данные обстоятельства весьма наглядно показывают существующую необходимость обеспечения защиты негласных сотрудников путем выработки и принятия комплекса законодательных и организационных мер, направленных на эффективное обеспечение их личной и имущественной безопасности, безопасности их родственников и близких.