уголовного судопроизводства, противоправное поведение которых или реальная возможность такого поведения создает или может создать препятствие производству по делу.

1. Манова, Н. С. Уголовный процесс. Краткий курс лекций / Н.С. Манова, Ю.В. Францифоров. – М. : Юрайт, 2019. – С. 27.

2. Рыжаков, А.П. Уголовный процесс России : курс лекций / А.П. Рыжаков. – СПб. : Питер, 2009. – 432 с.

3. Васильева, Е.Г. Проблемы ограничения неприкосновенности личности в уголовном процессе : дис. ... канд. юрид. наук : 12.00.09 / Е.Г. Васильева. – Уфа : Башкир. гос. ун-т, 2002. – Л. 26.

4. Кучинский, В.А. Личность, свобода, право / В.А. Кучинский. – М. : Юрид. лит., 1978. – С. 49.

5. Мальков, А.В. Ограничения в праве: проблемы теории, практики, политики / А.В. Мальков // Юрид. техника. – 2018. – № 12. – С. 238–241.

6. Смирнов, А.В. Уголовный процесс : учебник / А.В. Смирнов, К.Б. Калиновский ; под общ. ред. А.В. Смирнова. – 7-е изд., перераб. – М. : Норма : ИНФРА-М, 2019. – 752 с.

УДК 343.14 + 343.985

О.А. Слащинин

ПРОБЛЕМА ИСПОЛЬЗОВАНИЯ «УТЕЧЕК ДАННЫХ» В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ

Динамичная цифровизация общественных отношений с их постепенным переходом в глобальную компьютерную сеть Интернет (далее – сеть Интернет) приводит к закономерному расширению международного информационного пространства. Так, переход от традиционных носителей информации (бумага, фотоматериал, пластмасса, магнитная лента) на их электронные аналоги имеет следующие преимущества: 1) сокращение временных и материальных затрат, связанных с поиском, получением, передачей, сбором, обработкой, накоплением, хранением, распространением и предоставлением информации, а также ее использованием и защитой; 2) повышенная доступность «оцифрованной» информации. Но упомянутая доступность информации имеет и свою обратную сторону: высокие риски в сфере кибербезопасности.

Кибербезопасность – это состояние защищенности информационной инфраструктуры (ИИ) и содержащейся в ней информации от внешних и внутренних угроз согласно ст. 8 Концепции информационной безопасности Республики Беларусь [1]. Основными субъектами угрозы кибер-

безопасности (далее – исполнители) выступают специалисты в сфере высоких технологий, совершающие посредством сети Интернет умышленные противоправные действия против объектов ИИ и обслуживающих их операторов. Среди них можно выделить: хакеров, имеющих корыстную или иную личную заинтересованность, а также хактивистов, преследующих при осуществлении своей деятельности общественные или политические цели. Не имея допуска к информации, содержащейся в ИИ и представляющей интерес для хакеров и хактивистов, последние планируют и проводят целевые кибератаки на тот или иной объект ИИ. Цель проведения указанных атак: нарушение систем защиты объекта ИИ и осуществление к нему несанкционированного доступа с последующим неправомерным завладением содержащейся в ИИ информацией. В результате возникшего киберинцидента исполнители также могут завладеть данными, которые в соответствии со ст. 17 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон «Об информации, информатизации и защите информации») могут признаваться информацией, распространение и предоставление которой ограничено [2], а также в соответствии со ст. 1 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон «О защите персональных данных») – персональными данными физических лиц [3]. Наиболее популярными объектами ИИ, которые подвергаются кибератакам, являются базы и банки данных торговых сетей [4, 5], сервисов доставки товаров [6], информационные системы предприятий, организаций и государственных органов [7], банковских и иных коммерческих учреждений [8]. Осуществив несанкционированный доступ к информации, содержащейся в ИИ, исполнители до обнаружения оператором объекта проведенной кибератаки должны успеть ее скопировать. Одним из наиболее популярных и быстрых способов копирования информации при осуществлении кибератаки является создание «дампа» (англ. dump – сбрасывать), представляющего собой полное или частичное содержание компьютерной информации, аккумулируемой в ИИ. Рассмотренный типовой пример киберинцидента, обязательным результатом которого является завладение информацией лицом, не имеющим к ней допуска, квалифицируется в сфере кибербезопасности как «утечка данных» [9].

Факт происшедшей утечки данных может держаться в тайне от общественности как исполнителями проведенных кибератак в целях тайного использования полученной информации, так и операторами объекта ИИ для защиты своей деловой репутации. Часто о возникшей утечке данных хакеры и хактивисты могут сами публично сообщить

в сети Интернет, размещая созданный ими дамп ИИ на специализированных «теневых» интернет-ресурсах. Вышеуказанный дамп может размещаться в сети Интернет фрагментарно в качестве рекламы для последующей продажи его полной версии всем заинтересованным и готовым за это платить лицам. Информационное содержание дампа той или иной ИИ может анализироваться и использоваться органом уголовного преследования в качестве доказательства по уголовному делу, несмотря на противоправную сущность его создания и размещения. Обнаружение в сети Интернет указанных дампов и их последующий осмотр может иметь существенное значение для установления ранее неизвестных обстоятельств уголовного дела, которые в соответствии со ст. 89 Уголовно-процессуального кодекса (УПК) Республики Беларусь подлежат доказыванию при производстве дознания, предварительного следствия и судебного разбирательства [10]. Информационную значимость дампа ИИ как доказательства для целей уголовно-процессуального доказывания можно оценить лишь при детальном рассмотрении его формы и содержания.

Дамп по своей форме представляет собой электронный файл (далее – файл) или группу файлов, содержащий (-е) в себе преимущественно текстовую или гипертекстовую компьютерную информацию. Содержание файла дампа зависит от типа скопированной ИИ и вида аккумулируемой в ней компьютерной информации. Так, социальные сети, интернет-мессенджеры, сервисы электронной почты, интернет-форумы, интернет-сайты банковских или иных коммерческих учреждений, интернет-магазины, иные интернет-ресурсы и удаленные серверы, а также банки и базы данных внутренних серверов организаций и государственных органов, будут иметь разные системы и виды хранимой компьютерной информации. Но независимо от используемых в дампе систем и видов, интерес для органов уголовного преследования представляют две условные группы сведений: идентификаторы учетных записей, в том числе персональные данные физических лиц, а также внутренние файлы ИИ, в том числе документированная информация (контент).

К первой группе сведений можно отнести следующие компоненты будущей доказательственной базы: логин, пароль, адрес электронной почты, абонентский номер, сетевое имя, регистрационное описание или подпись учетной записи, реквизиты привязанных банковских платежных карточек, электронных счетов или кошельков, секретные ключи или мнемонические фразы восстановления кошелька криптовалюты, IP-адреса и иные маркеры интернет-браузера или компьютерной техники, а также иные персональные данные физических лиц.

Ко второй группе, в свою очередь, можно отнести: списки транзакций, системные логи, содержание публикаций, записей, комментариев, личных сообщений, электронных писем и вложений к ним, а также файлы архива и иной документированной информации органов иностранных государств и организаций.

Ценность и уникальность сведений, содержащихся в дампе той или иной ИИ, подкрепляется возможными проблемами их правового получения без непосредственного взаимодействия с содержанием дампа. Во-первых, оператор ИИ и (или) сам объект ИИ могут располагаться на территории иностранного государства, с которым не заключен международный договор о правовой помощи по уголовным делам, где производство выемки сведений на объекте ИИ не представляется возможным. Во-вторых, сроки получения и исполнения направленного в иностранное государство поручения (просьбы) об оказании правовой помощи могут превышать максимальные сроки хранения запрашиваемой компьютерной информации. В-третьих, в качестве операторов интересующего объекта ИИ могут выступать киберпреступники, а также иные лица, связанные с профессиональной преступностью и не сотрудничающие с правоохранительными органами, например, администраторы «теневых» интернет-форумов и специализированных торговых площадок, серверов обмена файлами и сообщениями. В-четвертых, операторы коммерческих объектов ИИ и органы иностранных государств по направленным запросам могут предоставлять недостоверные сведения или заявлять об их отсутствии. Это может быть связано с их возможной заинтересованностью в исходе уголовного дела или в целях сокрытия запрашиваемых сведений, которые признаются последними коммерческой или государственной тайной.

В случае обнаружения в сети Интернет размещенных дампов ИИ, содержащих фактические данные об обстоятельствах, имеющих значение для правильного разрешения уголовного дела, орган уголовного преследования описывает их в протоколе осмотра компьютерной информации. Далее, в соответствии с ч. 2 ст. 100 УПК Республики Беларусь осмотренные дампы ИИ, в том числе скопированные органом уголовного преследования на электронный носитель информации, могут признаваться такими источниками доказательств, как другие носители информации и (или) вещественные доказательства [10].

Несмотря на то что у органа уголовного преследования отсутствуют какие-либо правовые ограничения на собирание подобных доказательств, не исключена возможность возникновения в процессе уголовно-процессуального доказывания проблем с их последующей проверкой и оценкой. Следует отметить, что на основании ст. 6 Закона «О защите

персональных данных» обработка персональных данных, в том числе содержащихся в обнаруженных дампах ИИ, в целях ведения уголовного процесса может производиться без согласия субъектов этих персональных данных [3]. Однако сам факт обнаружения в открытом доступе в сети Интернет утечки данных в виде дампа ИИ не освобождает органы уголовного преследования от соблюдения ими правового режима осмотра компьютерной информации, распространение и предоставление которой ограничено в соответствии со ст. 17 Закона «Об информации, информатизации и защите информации» [2]. На основании вышеуказанного следует, что рассматриваемые доказательства будут признаваться допустимыми лишь с соблюдением в процессе их собирания требований ч. 2 ст. 204^1 УПК Республики Беларусь, а именно: их осмотр лишь по постановлению следователя, органа дознания с санкции прокурора или с согласия обладателя информации и в его присутствии [10].

Если вести речь о необходимости проведения всесторонней, полной и объективной проверки обнаруженных утечек данных, следует упомянуть о возможности заинтересованных лиц разместить в сети Интернет подложного (наполненного сходным, но неподлинным содержанием) дампа той или иной ИИ в целях дискредитации ИИ или субъектов, чьи данные содержатся в дампе. В целях признания обнаруженных доказательств достоверными, последние должны быть сопоставлены с другими полученными доказательствами, которые подтвердят или опровергнут проверяемую в «утечках данных» информацию.

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : в ред. Закона Респ. Беларусь от 10.10.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

3. О защите персональных данных [Электронный ресурс] : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З : в ред. Закона Респ. Беларусь от 01.06.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

4. Национальный центр защиты персональных данных Республики Беларусь: Установлен факт «утечки» персональных данных в одной из торговых сетей [Электронный ресурс]. – Режим доступа: cpd.by/ustanovlen-fakt-utechki-personalnyh-dannyh-v-odnoj-iz-torgovyh-setej. – Дата доступа: 09.11.2022.

5. Национальный центр защиты персональных данных Республики Беларусь: Произошла «утечка» персональных данных клиентов торговой сети «Остров чистоты и вкуса» [Электронный ресурс]. – Режим доступа: cpd.by/proizoshla-utechka-personalnyh-dannyh-klientov-torgovoj-seti-ostrov-chistoty-i-vkusa. – Дата доступа: 09.11.2022.

6. Национальный центр защиты персональных данных Республики Беларусь: Подтвержден факт «утечки» персональных данных в одном из сервисов доставки еды [Электронный ресурс]. – Режим доступа: cpd.by/podtverzhden-fakt-utechki-personalnyh-dannyh-v-odnom-iz-servisov-dostavki-edy. – Дата доступа: 09.11.2022.

7. Национальный центр защиты персональных данных Республики Беларусь: Из-за несанкционированного доступа к информационным системам организации были распространены персональные данные 55 тысяч граждан [Электронный ресурс]. – Режим доступа: cpd.by/vnimanie-vazhnaja-informacija. – Дата доступа: 09.11.2022.

8. МТБанк признает вину за утечку данных о потенциальных кредитополучателях [Электронный ресурс] / SB.BY / БЕЛАРУСЬ СЕГОДНЯ. – Режим доступа: www.sb.by/articles/mtbank-priznaet-vinu-za-utechku-dannykh-o-potentsialnykh-kreditopoluchatelyakh.html. – Дата доступа: 09.11.2022.

9. Лаборатория Касперского: Что такое кража данных и как ее избежать [Электронный ресурс]. – Режим доступа: cpd.by/vnimanie-vazhnaja-informacija. – Дата доступа: 09.11.2022.

10. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 20.07.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

УДК 343.132

А.Ю. Теслёнок

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ ПОРЯДОК ОФОРМЛЕНИЯ ОСМОТРА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ ПО СОВЕРШЕНИЮ ОРГАНИЗАЦИИ НЕЗАКОННОЙ МИГРАЦИИ

Совершение противоправных деяний на современном этапе, как правило, носит латентный характер, а информация, содержащая следы преступления, в том числе в ходе совершения организации незаконной миграции, может храниться в компьютерных устройствах, автоматизированных информационных системах и сетях, в том числе сети Интернет, которая может быть получена в ходе проведения процессуальных действий и в перспективе может являться доказательством по уголовным делам. Вместе с тем необходимо отметить, что до 2003 г.