ARTICLE HISTORY: Received: September 13, 2021 Accepted: November 5, 2021 Published: November 13, 2021

ИНФОРМАЦИОННОЕ ОБЩЕСТВО: ВЛИЯНИЕ НА ОПЕРАТИВНО-СЛУЖЕБНУЮ ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ПЕРСПЕКТИВЫ ИХ РАЗВИТИЯ

Грибков Сергей Сергеевич,
Академия управления МВД России

Gribkov Sergey Sergeevich
Academy of Management of the Ministry of Internal Affairs of Russia

Аннотация. В статье рассматриваются вопросы влияния информационных технологий на социальную и экономическую сферы, а также оперативно-служебную деятельность органов внутренних дел, в частности. Затрагивается проблематика выявления, расследования и учета преступлений, сопряженных с использованием информационно-телекоммуникационных технологий. Предлагаются перспективные решения обозначенных вопросов.

Resume. The article examines the impact of information technologies on the social and economic spheres, as well as the operational and service activities of the internal affairs bodies, in particular. The problems of detection, investigation and registration of crimes associated with the use of information and telecommunication technologies are touched upon. Prospective solutions to these issues are proposed.

Ключевые слова: информационные технологии, органы внутренних дел, информационные системы.

Key words: information technology, internal affairs bodies, information systems.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы определяет в качестве приоритетов формирование цифровой экономики, а фактически констатирует принципы сохранения традиционных и привычных для граждан форм получения товаров и услуг, наряду с повсеместной интеграцией информационных технологий во все сферы жизнедеятельности.

Указанные процессы проводятся в соответствии с паспортом национальной программы «Цифровая экономика Российской Федерации».

Предполагается создание «интернета вещей» и обеспечение доступа к сети «Интернет» практически для 100% домохозяйств.

В свою очередь, столь стремительное развитие информационных технологий имеет свои негативные последствия, связанные в том числе с ростом количества совершенных преступлений в указанной сфере.

Актуальность статьи характеризуется необходимостью анализа предпосылок и условий, способствующих возникновению и росту преступных деяний в сфере высоких технологий, для выработки стратегических решений в данной области.

Данные криминальные деяния составляют все большую долю в общей структуре преступности. В 2020 году она достигла двадцати пяти процентов. Динамика ежегодного прироста фиксируется последние несколько лет. При этом в суд удается направить сравнительно небольшое количество уголовных дел о таких преступлениях (16% в 2020 году). Одной из причин тому является отсутствие достаточных оперативных возможностей по документированию фактов преступной деятельности.

Одним из распространенных и тиражируемых в СМИ противоправных деяний являются преступления, сопряженные со звонками «банковских специалистов», так называемые телефонные мошенничества. Указанные деяния осуществляются, в том числе, в результате «цифровой неграмотности».

Как я отмечал выше, развитие информационных технологий приходит практически в каждую сферу жизнедеятельности, в том числе финансовую. Это в свою очередь ведет к повышению уровня комфорта людей. Например, не выходя из дома можно осуществлять покупки, получение медицинских услуг или финансовые транзакции. Практически все финансовые организации могут оказывать услуги без посещения отделения банков – посредством использования сервисов «мобильный банк».

Стоит отметить, что процесс осуществления преступлений постоянно совершенствуется, так распространение получили случаи телефонных мошенничеств, совершенные от лица «сотрудников полиции».

Схема мошенничества заключается в следующем. Гражданину звонит незнакомец, представляясь сотрудников банка, и сообщает, что мошенники хотят оформить на него онлайн-кредит. Чтобы предотвратить эти действия, человека убеждают в необходимости оформить онлайн-кредит на ту же сумму, а затем обналичить деньги с карты и перечислить на указанный злоумышленниками счет.

Через несколько минут жертве звонит соучастник преступной схемы, который представляется сотрудником полиции и рекомендует следовать инструкциям представителей службы безопасности банка, которые звонили

ранее. При этом злоумышленники используют современную технологию подмены телефонных номеров, которая позволяет в точности повторить контакты правоохранительных органов, указанные на официальном сайте.

С сентября 2020 года по настоящее время выявлено более 20 фактов подобных мошенничеств, в результате которых у граждан похищено более 6,7 млн рублей[1].

Вопросы выявления, фиксации и учета цифровых мошенничеств также вызывают определенный резонанс, освещаемый в средствах массовой информации. Имеется проблематика сопоставления статистических учетов киберпреступлений со стороны Генеральной прокуратуры Российской Федерации, МВД России, Банка России и иных ведомств.

В качестве проблемного вопроса при документировании преступлений рассматриваемой категории отмечены случаи использования в противоправной деятельности так называемых «удаленных рабочих столов», которые расположены на серверах, в том числе находящихся за пределами Российской Федерации либо в «облачном хранилище данных».

В ходе изучения данного вопроса установлено, что в случае изъятия в рамках проведения оперативно-розыскных мероприятий средства коммуникации, информация из облачного хранилища (удаленного сервера), доступ к которой обеспечивается посредством данного устройства, может быть дистанционно уничтожена иными участниками противоправной деятельности, что часто приводит к утрате части доказательной базы и влечет затруднения в доказывании в судебном процессе.

Кроме того, в целях изучения компьютерной информации, обнаруженной в результате проведения оперативно-розыскного мероприятия «получение компьютерной информации», в том числе с привлечением лица, обладающего специальными познаниями, представляется целесообразным проведение ее исследования.

Дополнительно хочется отметить, что на долю службы экономической безопасности и противодействия коррупции МВД России приходится может и не самое большое количество киберпреступлений, но стоит признать, вероятно, наиболее вредоносных, как для государства, так и для граждан.

Это финансовые пирамиды в сети, «фальшивки», азартные игры «онлайн», незаконные сделки с использованием криптовалют, махинации с электронными цифровыми подписями (которые в свою очередь используются в криминальных схемах уклонения от уплаты налогов и в деятельности так называемых «обнальных площадок»).

В настоящее время МВД России осуществляется поступательная работа по разработке проекта нормативно-правового акта, предусматривающего корректировку положений Федерального закона «Об оперативно-розыскной деятельности», в части дополнения его новым оперативно-розыскным мероприятием по исследованию компьютерной информации, в том числе с привлечением квалифицированных специалистов, в целях документирования (фиксации) «электронных» следов преступления.

В этой связи, вероятно, следует заблаговременно предусмотреть возможность обучения и дополнительной подготовки для сотрудников органов внутренних дел по данному направлению.

Затрагивая вопросы выявления и фиксации киберпреступлений, целесообразно обозначить основные способы получения первичной информации о преступлении – непосредственно от заявителей или в ходе осуществления оперативно-розыскной деятельности.

Для получения доказательной базы в виртуальном пространстве сотруднику необходимо простроить цепочки оперативно-значимых событий, на основании сведений из различных ведомств и организаций.

Безусловно, процесс взаимодействия МВД России с федеральными органами исполнительной власти и банковскими организациями имеет четкую и логичную правовую основу. Однако, направление запросов в банки и интернет-провайдеры имеет свои негативные стороны, выражающиеся в частности, в несвоевременном поступлении оперативно-значимой информации на запросы.

Сейчас данная проблематика разрешается, путем заключения дополнительных соглашений о взаимодействии, регламентирующих фактор оперативности в ходе предоставления справочной информации.

Совместными усилиями МВД России и Росфинмониторинга в настоящее время проводится апробация информационного ресурса «Личный кабинет правоохранительного органа».

Использование указанного ресурса предполагает направление запросов в Росфинмониторинг в режиме «онлайн», что фактически позволит взглянуть на оперативную обстановку с другой стороны, а также оперативно обмениваться информацией с помощью так называемого «одного окна»[2].

Общаясь с коллегами из подразделений оперативного блока, отмечу явную заинтересованность сотрудников в таком взаимодействии. Подразделения Росфинмониторинга обладают обобщенной и емкой информацией о движении денежных средств, «подсвеченных» в ходе совершения преступлений. При этом остается открытым вопрос корректной «легализации» полученной информации.

---

[1] Пресс-релиз «МВД России предупреждает: мошенники используют технологию подмены телефонных номеров», https://мвд.рф/news/item/23115917.

[2] Пресс-релиз «О заседании коллегии Росфинмониторинга», https://www.fedsfm.ru/releases/4768.

Имея в распоряжении сведения о перемещении денежных средств, возможно отследить финансовые цепочки, вплоть до снятия денег из банкоматов.

Таким образом, возможно констатировать, что в ходе выявления и раскрытия киберпреступлений все большие требования предъявляются к аналитическим способностям правоохранителей.

Справедливости ради, стоит отметить и постоянно развивающиеся способности и навыки аналитиков преступного мира. Первоначально, для совершения большинства киберпреступлений злоумышленниками проводится аналитическая разведка, на основе сведений, полученных противоправным путем из государственных, банковских и иных информационных ресурсов. Речь идет о персональных данных граждан.

Прошедший год показал нам, что форсирование цифровизации общества может привести к многочисленным неконтролируемым утечкам персональных данных, в том числе из банковского сектора и цифровых онлайн-сервисов. Попадая к злоумышленникам, эти сведения, массивы больших данных, анализируются и систематизируются.

На текущий момент организациям и подразделениям, обрабатывающим персональные данные, особо внимательно стоит отнестись к периоду плавного возвращения работников в «оффлайн». Зачастую, отправляя работников на удаленную работы создавались предпосылки для халатного и небрежного обращения с «чувствительными» данными. Рабочие места организовывались впопыхах, без соблюдения элементарных процедур по обеспечению информационной безопасности.

Сотрудники, работая на «удаленке», могут и не догадываться, что их идентификаторы скомпрометированы, а рабочее место может иметь интегрированное вредоносное программное обеспечение.

Эти факторы в будущем могут способствовать росту числа фиксируемых противоправных деяний, связанных со сферой информационных технологий.

Стоит отметить, что в настоящее время проводится комплекс мероприятий по совершенствованию информационной безопасности в государственном секторе. Прорабатываются перспективы развития ситуационных центров, а также совершенствование взаимодействия в рамках ГосСОПКА.

Особое место в сфере информационных технологий занимают искусственный интеллект и робототехника.

В перспективе обработка большого количества информации о событиях и инцидентах потребуют работы значительного штата специалистов в соответствующих областях. Однако, описанные процессы уже сегодня возможно автоматизировать посредством использования технологий искусственного интеллекта.

В свою очередь, на крупных предприятиях промышленности и производства в России все чаще применяется робототехника. Роботы, как и любые высокотехнологичные устройства, планируется интегрировать в структуру «интернета вещей». Данный термин еще мало используется в повседневной деятельности, но мы все чаще наблюдаем создание «умных систем», в том числе в своих домах.

В будущем, в процессе эксплуатации «интернета вещей» мы можем столкнуться с результатами деятельности узкопрофильных компьютерных специалистов – хакеров. Взлом, нарушение функционала и вывод из строя робототехники может привести к совершению более тяжких преступных деяний, способных нанести ущерб не только экономике, но и жизни и здоровью людей.

Перспективным видится вопрос организации расследования указанных противоправных деяний, ведь на текущий момент специалистов, способных провести качественный криминалистический компьютерный анализ можно пересчитать по пальцам.

Учитывая всю изложенную проблематику, целесообразно предложить следующие перспективные варианты решения:

– для позитивного разрешения вопроса учета преступлений в сфере высоких технологий предлагается разработать отдельный перечень преступлений, совершаемых в информационно-телекоммуникационной сфере, а также соответствующих методических рекомендаций;

– с целью систематизации и унификации информационного пространства предлагается форсировать процессы централизации информационных систем, а также организовать проведение комплексных ревизий в информационной среде;

– для дополнительного повышения уровня «цифровой грамотности» сотрудников органов внутренних дел предлагается разработать систему оценки знаний основ информационной безопасности;

– учитывая перспективы развития и интеграции технологий искусственного интеллекта и робототехники в повседневную жизнь предлагается рассмотреть вопрос создания соответствующих специализированных подразделений, на которые будут возложены функции по выявлению и расследованию преступлений, сопряженные с использованием указанных технологий.

И последнее, но не менее важное предложение – это улучшение межрегионального и международного взаимодействия по данным вопросам. Ведь по своей сути совершение преступлений в виртуальном пространстве не имеет такого понятия как граница. Только вместе сконцентрировав усилия и организовав непрерывный обмен опытом возможно противостоять современным вызовам в информационном пространстве.

Список литературы.

1. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс]: Доступ из СПС «Консультант Плюс».
2. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]: Доступ из СПС «Консультант Плюс».
3. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ [Электронный ресурс]: Доступ из СПС «Консультант Плюс».
4. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утверждена президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) [Электронный ресурс]: Доступ из СПС «Консультант Плюс».
5. Пинкевич Т.В., Смольянинов Е.С. Международный опыт противодействия преступной деятельности с использованием криптовалюты // Академия управления МВД России. 2021.
6. Аносов А.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий // Академия управления МВД России. 2019.
7. Пресс-релиз «МВД России предупреждает: мошенники используют технологию подмены телефонных номеров», https://мвд.рф/news/item/23115917.
8. Пресс релиз «О заседании коллегии Росфинмониторинга», https://www.fedsfm.ru/releases/4768 // 2020.

References:

1. Decree of the President of the Russian Federation dated 09.05.2017 No. 203 «On the Strategy for the Development of the Information Society in the Russian Federation for 2017 – 2030» [Electronic resource]: Access from the PCA "Consultant Plus".
2. Decree of the President of the Russian Federation dated 05.12.2016 No. 646 «On the approval of the Doctrine of information security of the Russian Federation» [Electronic resource]: Access from the SPS "Consultant Plus".
3. Federal Law «On Operational Investigative Activities» from 12.08.1995 N 144-FZ [Electronic resource]: Access from the SPS "Consultant Plus".
4. Passport of the national project «National Program» Digital Economy of the Russian Federation (approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects, minutes of 04.06.2019 No. 7) [Electronic resource]: Access from the SPS" Consultant Plus ".
5. Pinkevich T.V., Smolyaninov E.S., Mejdunarodnii opit protivodeistviya prestypnoi deyatelnosti s ispolzovaniem kriptovaluti. Academy of Management of the Ministry of Internal Affairs of Russia, 2021 (in Russian).
6. Anosov A.V. and others. Deyatelnost organov vnytrennix del po bor'be s prestypleniyami, sovershennimi s ispolzovaniem informacionnix, kommynikacionnix i visokix tekhnologii. Academy of Management of the Ministry of Internal Affairs of Russia, 2019 (in Russian).
7. Press release «The Ministry of Internal Affairs of Russia warns: scammers are using technology to substitute phone numbers», https://мвд.рф/news/item/23115917 (in Russian).
8. Press release «On the meeting of the Rosfinmonitoring board», https://www.fedsfm.ru/releases/4768 // 2020 (in Russian).