Д. Н. Рудов,
кандидат юридических наук, доцент,
Юридический институт Белгородского государственного национального исследовательского университета

К ВОПРОСУ О ПРЕДУПРЕЖДЕНИИ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Аннотация. В статье рассматривается проблема противодействия и пресечения цифровой преступности, порождаемой непрерывной глобализацией и модернизацией современных IT-технологий. Определены основные направления системы предупреждения цифровых преступлений, анализирован практический опыт по противодействию данного вида преступности. Особое внимание уделено профилактическим мерам преступности в рассматриваемой сфере. В заключении автор отметил основные недостатки системы предупредительных мер в сфере борьбы с цифровыми преступлениями.

Ключевые слова: право, цифровизация, цифровые преступления, цифровые технологии, предупреждение преступности

ON THE PREVENTION OF DIGITAL CRIME: THEORETICAL AND PRACTICAL ISSUES

Abstract. The article deals with the problem of countering and suppressing digital crime generated by continuous globalization and modernization of modern IT-technologies. The main directions of the system for the prevention of digital crimes have been determined, practical experience in countering this type of crime has been analyzed. Particular attention is paid to preventive measures of crime in this area. In conclusion, the author noted the main shortcomings of the system of preventive measures in the field of combating digital crimes.

Keywords: Law, Digitalization, Digital crimes, Digital technologies, Crime prevention

Современные цифровые технологи активно входят в нашу жизнь. При этом помимо положительного эффекта в промышленности, торговле, и других сферах жизни указанные технологии способствовало созданию в России нового вида преступности – цифровой преступности. С учетом неготовности ряда слоев населения к быстроменяющейся системе жизнедеятельности цифровизация помимо положительного эффекта в экономике и других сферах жизни несет в себе и ряд угроз, прежде всего, для категории лиц которые более медленно адаптируются современным цифровым технологиям. При этом предупреждение преступлений совершенных с применением цифровых технологий представляет сложную задачу, которая в первую очередь ложится на сотрудников органов внутренних дел и службы безопасности соответствующих структур вовлеченных в деятельность с использованием цифровых технологий. При этом из собственного практического опыта работы в территориальном органе МВД России (СУ УМВД России по г. Белгороду) автору статьи известно о технических сложностях возникающих при предупреж-

дении, раскрытии и расследовании преступлений совершенных с использованием цифровых технологий.

Повышение уровня деятельности сотрудников органов внутренних дел по предупреждению и профилактики преступлений совершенных с применением цифровых технологий влечет за собой повышение затрат государства на техническое оснащение сотрудников полиции и привлечение на работу специалистов высокого уровня. При этом минимальные затраты возможны только при организации повышения квалификации сотрудников органов внутренних дел и соответствующих работников организаций использующих в своей детальности цифровые технологии.

Предупреждение преступлений, совершаемых с использованием высоких технологий (цифровых технологий), является одним из приоритетных направлений деятельности органов внутренних дел [1. С. 60].

Применительно к системе предупреждения высокотехнологичной цифровой преступности можно выделить несколько направлений.

Ни для кого не секрет, что важным направлением противодействия цифровым преступлениям являются социальные меры, так, например, профилактика цифровых преступлений может и должна начинаться с пожилыми лицами, которые только начинают осваивать некоторые виды деятельности с использованием цифровых технологий. Так, в деятельности правоохранительных органов неплохо зарекомендовала себя работа по разъяснению пожилым людям действий при обращении к ним мошенников в рамках «телефонного мошенничества». Здесь необходимо сказать и положительной реакции руководства банковских структур, которые осознают, что массово совершаемые преступления с использованием цифровых технологий подрывают доверие населения и к их деятельности, так как фактически хищения, как правило, совершаются с использованием банковских переводов. Подготовка различных информационных стендов и размещением информации о способах совершения цифровых преступлений, а также бесед сотрудников банковских структур в офисах банковских организаций важный элемент профилактики цифровых преступлений.

Отдельно стоит отметить и способы воздействия на «незащищенные» слои населения при профилактике преступлений совершенных с использованием цифровых технологий, которые предусматривают осуществлением разъяснительной работы во взаимодействии со средствами массовой информации (телевидение, радио, печатные издания).

На наш взгляд, важным элементом предупреждения и профилактики цифровых преступлений будут являться научно-технические меры профилактики преступлений совершенных с использованием цифровых технологий, которые включали бы в себя формирование и государственную поддержку системы целевых фундаментальных и прикладных научных исследований как необходимого элемента научного обеспечения деятельности по профилактики указанного вида преступлений. Система государственной поддержки научных исследований в данном направлении по нашему мнению являлась бы наиболее эффективной формой способствовавшей профилактике и предупреждению преступлений совершенных с использованием цифровых технологий.

При этом мы можем говорить и о расширение сети научно-исследовательских и образовательных учреждений, обеспечивающих разработку научных исследований в сфере высоких технологий и подготовку соответствующих специалистов, а также «целевом» наборе студентов (магистрантов, аспирантов) на соответствующие специальности (направления подготовки).

Необходимо отметить и положительные наработки правоохранительных органов и заинтересованных коммерческих организаций по противодействию преступлениям, совершенным с использованием цифровых технологий.

Так, в целях быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по уголовным делам принимаются меры по совершенствованию механизма взаимодействия следственных органов с оперативными подразделениями, заинтересованными ведомствами и представителями бизнес-сообщества, предусматривающие возможность оперативной блокировки сайтов интернет-пирамид (хайд-проектов), фишинговых сайтов и мошеннических Колл-центров, а также номеров мобильных телефонов, с использованием которых осуществляются хищения денежных средств. В связи этим были заключены соответствующие соглашения с ПАО «Сбербанк» (23.10.2017), Банк ВТБ (ПАО) (25.12.2017) и ПАО «МТС» (30.08.2019), с ПАО «ВымпелКом» (05.12.2019)[1, С. 60].

В целях сокращения фактов цифровых преступлений корыстной направленности, в МВД России создана специализированная база данных «Дистанционное мошенничество», где аккумулируется информация о зарегистрированных IT-преступлениях и устройствах, с помощью которых осуществляются хищения денежных средств. В указанный модуль сотрудниками территориальных органов внутренних дел на региональном уровне вносится актуальная информация о вновь выявленных фактах IT- преступлений.

Однако на данный момент имеются проблемные вопросы ее функционирования, а именно она сформирована не в полной мере.

Согласно сведениям, представленным УОРИ МВД России, массив учтенной информации содержит 141 950 записей о фактах противоправных деяний (номера КУСП или уголовных дел), а также сведения о 166 970 используемых при этом устройствах мобильной связи и 48 647 банковских счетах. К данному массиву имеют доступ более 6 тыс. региональных пользователей, которыми в 2019 г. выявлено 7 603 совпадения по номерам телефонов, фигурирующим в 28 530 уголовных делах, в том числе 296 совпадений по 1 035 банковским счетам и 1 393 совпадения по 3 373 банковским картам [2. С. 12].

Важное значение придается профилактике преступности в рассматриваемой сфере. В рамках профилактической работы особое внимание следует уделять наименее защищенным слоям населения. Целесообразно применять для этого различные способы распространения информации (в органах власти, муниципальных образованиях, государственных, медицинских, образовательных и других учреждениях, на объектах торговли и массового пребывания граждан). Транслировать через СМИ сообщения об успешном расследовании цифровых преступлений, проводить брифинги и пресс-конференции.

На практических примерах разъяснять работу мобильных банковских приложений, предотвращающих дистанционное подключение сторонних лиц путем блокировки возможности восстановления логина и пароля онлайн.

В целях повышения уровня профилактической работы управления общественных связей МВД России разработан, утвержден и реализуется План внешних коммуникаций МВД России и Банка России по противодействию кибер-мошенничеству на 2020 год [3. С. 10]. В нем предусмотрено проведение ряда мероприятий по информированию населения о преступлениях рассматриваемой категории и способах противодействия им, с привлечением ведомственных, региональных и федеральных средств массовой информации.

В качестве положительного примера можно привести опыт деятельности МВД по Республике Башкортостан, где в целях профилактики преступлений и дополнительного информирования населения о новых способах совершения хищения имущества и денежных средств в 2019 г. на региональном сайте МВД размещено 352 материала, интернет-изданиями и интернет-порталами опубликовано 368 материалов, в печатных изданиях – 37, региональными СМИ выпущено 57 видеосюжетов [3.С. 10]. Разработан и утвержден план дополнительных профилактических мероприятий, в рамках исполнения которого на территории республики проводилась соответствующая работа с максимальным привлечением сотрудников территориальных органах внутренних дел.

Таким образом, можно говорить о том, что правоохранительными органами осуществляется достаточно обширный перечень мероприятий, направленный на борьбу с преступлениями, совершаемыми с использованием цифровых (информационно-телекоммуникационных) технологий. Однако задачи, поставленные перед государством по совершенствованию указанного противодействия, решены не в полной мере.

Список литературы

1. Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие. – Москва: Академия управления МВД России, 2019. С. 60.

2. Анализ практики расследования преступлений, совершенных в сфере телекоммуникаций и компьютерной информации: учебное пособие / В. В. Гончаров, В. Ю. Иванов, К. Р. Аветисян, Д. В. Гусев. – Москва: Московский университет МВД РФ им. В. Я. Кикотя, 2020. С. 12.

3. Анализ практики расследования преступлений, совершенных в сфере телекоммуникаций и компьютерной информации: учебное пособие / В. В. Гончаров, В. Ю. Иванов, К. Р. Аветисян, Д. В. Гусев. – Москва: Московский университет МВД РФ им. В. Я. Кикотя, 2020. С. 10.