

**БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И.Д. ПУТИЛИНА**

Проблемы информационного обеспечения деятельности правоохранительных органов

**Сборник статей
10-й Всероссийской научно-практической конференции
19 мая 2023 года**

**Белгород
Белгородский юридический институт МВД России
имени И.Д. Путилина
2023**

УДК 351.74:002
ББК 67.401.114
П 78

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России имени
И.Д. Путилина

Выпускается с 2015 года.

П 78 Проблемы информационного обеспечения деятельности правоохранительных органов : сборник статей 10-й Всероссийской научно-практической конференции, 19 мая 2023 года. – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. – 205 с.
ISBN 978-5-91776-513-6

Редакционная коллегия:

Александров А.Н., начальник института, кандидат юридических наук, доцент (председатель);

Дизер О.А., заместитель начальника института (по научной работе), доктор юридических наук, доцент (заместитель председателя);

Ковалева Е.Г., доцент кафедры информационно-компьютерных технологий в деятельности ОВД, кандидат технических наук (ответственный секретарь);

члены редакционной коллегии:

Меняйло Д.В., начальник кафедры информационно-компьютерных технологий в деятельности ОВД, кандидат юридических наук, доцент;

Дрога А.А., заместитель начальника кафедры информационно-компьютерных технологий в деятельности ОВД.

В сборнике 10-й Всероссийской научно-практической конференции представлены научные статьи, в которых исследуются проблемы противодействия компьютерным преступлениям и обеспечения информационной безопасности.

Предназначен для курсантов, слушателей, адъюнктов, профессорско-преподавательского состава образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 351.74:002
ББК 67.401.114

ISBN 978-5-91776-513-6

© Белгородский юридический институт
МВД России имени И.Д. Путилина, 2023

СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМА ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА НЕЗАКОННОЙ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ АЗАРТНЫХ ИГР

Аветисян К.Р.

(Московский университет МВД России имени В.Я. Кикотя);

Аветисян Б.Р.

(Научно-исследовательский институт образования и науки)

Аннотация: развитие общественных отношений и достижение науки и техники формирует новые механизмы взаимодействия в социуме, предопределяя принятие организационно-технических и правовых мер необходимых в конъюнктуре цифрового общества как эффективную меру обеспечения экономической безопасности государства. Своевременное выявление угрозы и есть критерий эффективности работы подразделений правоохранительных органов, только такой подход позволит применять превентивные меры и исключить реализацию потенциального ущерба в отношении личности, общества и государства.

Ключевые слова: информационное противоборство, интеллектуальные системы, азартные игры, детерминирующие признаки, совершенствование механизма.

IMPROVING THE MECHANISM OF INFORMATIONAL CONFRONTATION OF ILLEGAL ORGANIZATION AND CONDUCT OF GAMBLING

Avetisyan K.R.

(Kikot Moscow University of the Ministry of Internal Affairs of Russia);

Avetisyan B.R.

(Institute of Education and Science)

Abstract: the development of public relations and the achievement of science and technology forms new mechanisms of interaction in society, predetermining the adoption of organizational, technical and legal measures necessary in the conjuncture of digital society as an effective measure to ensure the economic security of the state. Timely detection of a threat is the criterion for the effectiveness of the work of law enforcement agencies, only such an approach will allow to apply preventive measures and exclude the realization of potential damage to individuals, societies and the state.

Keywords: informational confrontation, intelligent systems, gambling, deterministic signs, improvement of the mechanism.

Как правило, в результате формирования новых форм общественных отношений, сопряженных с применением информационных технологий и, в частности, искусственного интеллекта (автоматизированных и интеллектуальных

информационных систем, архитектурно представленных и обладающих по своей технической природе такими атрибутами как язык программирования, фреймворки, библиотеки и прочими компонентами, основанными на методах машинного обучения) изменяются и механизмы совершения преступлений.

С развитием цифровых технологий игорное оборудование стало управляться программными методами, а устройства приобрели адаптивный для восприятия интерфейс [1]. Установление лиц¹ организатора или пособника незаконной организации и проведения азартных игр реализуется подразделениями органов внутренних дел, как правило, через обращение к провайдерам, с требованием о последующей блокировке доступа к рассматриваемым в рамках производства ресурсам; в случае если информационный ресурс и/или его содержание запрещено Российским законодательством. Вместе с тем операторам и провайдерам поступают требования на представление достаточных сведений об активности пользователей сети и логов их сетевого оборудования, с представлением их идентификаторов: сопоставлением «статических» и «динамических» IP-адресов и их физических адресов – MAC-адресов.

Стоит отметить, что в соответствии с ч. 4 ст. 21 Уголовно-процессуального кодекса Российской Федерации «Требования, поручения и запросы прокурора, руководителя следственного органа, следователя, органа дознания и дознавателя, предъявленные в пределах их полномочий, установленным настоящим Кодексом, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами», а также по основаниям п. 4, ч. 1 ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» возможно «...запрашивать и получать на безвозмездной основе по мотивированному запросу уполномоченных должностных лиц полиции от государственных и муниципальных органов, общественных объединений, организаций, должностных лиц и граждан сведения, справки, документы (их копии), иную необходимую информацию, в том числе персональные данные граждан...».

Ввиду чего специфика механизма предупреждения незаконной организации и проведения азартных игр предусматривает не только анализ норм права, регулирующих данную отрасль, но технические возможности по получению установочной информации о потенциальном лице или группе лиц, что эффективно реализуемо в сегодняшних реалиях лишь при анализе больших ненормализованных массивов данных и корреляционном анализе идентифицирующих признаков как из открытых источников, так и из Deep Web платформ [3], но и в качестве одного из организационно-технических решений – ведение журналирования об активности тех узлов в Сети, пользователи которых представляют оперативный интерес (только совокупность факторов, включающие в себя использование анонимайзеров и/или технологии VPN, наличие недеklarированного дохода и анализа его динамики, связи лица с криминогенным контингентом и др.).

¹ Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс».

Целесообразно исследовать незаконную организацию и проведение азартных игр в виде совокупности детерминант [4], с их категоризацией по группам (см. рис. 1).

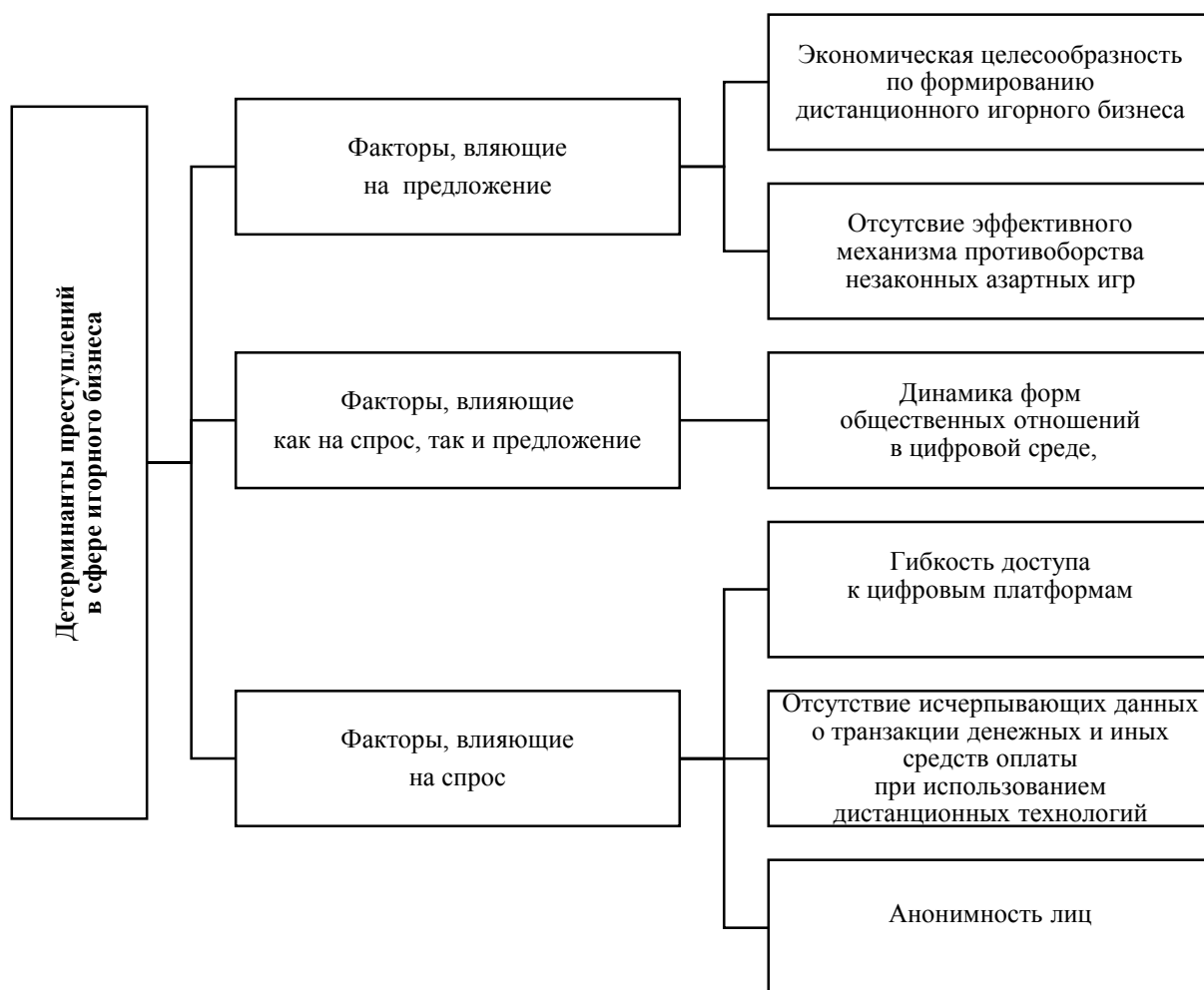


Рисунок 1. Детерминанты преступлений в сфере игорного бизнеса

В связи с «... экономической природой...» [5] азартных игр наиболее профильными мерами противодействия преступности в сфере незаконной организации и проведения азартных игр выступает взаимодействие органов государственной власти при осуществлении контроля игорной деятельности с защитой всех форм собственности в области незаконной организации и проведения азартных игр.

Изучение закономерностей и особенностей предупреждения преступности в игорной среде направлено на формирование практического подхода, включающего:

- разработки мер по выявлению инцидентов организации и проведения незаконных азартных игр, контактного, дистанционного и смешанного типов;
- выявление схемы и установление всех участников и формы их взаимодействия в рамках организации и проведения незаконных азартных игр;

– определение квалификации по всем исследуемым событиям в отношении установленных лиц, а также причастных к организации и проведения незаконных азартных игр;

– разработка оперативно-тактического плана мероприятий, в системе мер по развитию и обеспечению экономической безопасности государства.

Библиографический список

1. Аветисян Б.Р. Игрное оборудование: реальность и метаморфозы // Образование. Наука. Научные кадры. 2015. № 6. С. 72–75.

2. Аветисян Б.Р. Инструментальные сервисы предиктивной криминологии. – Москва: Патентное ведомство: Россия, 2020.

3. Аветисян Б.Р. Игровой бизнес как криминальный рынок услуг // Общество и право. 2015. № 4(54). С. 176–179.

4. Аветисян Б.Р. Использование экономического подхода при исследовании криминального рынка услуг игрового бизнеса // Экономика, педагогика и право. 2016. № 3. С. 1–6.

5. Крупенникова К.К., Меняйло Д.В. Правовое регулирование информационного пространства в современной России / Право в эпоху информационных технологий: проблемы и пути решения: сборник материалов Международной научно-практической конференции среди студентов, магистрантов и аспирантов (Пермь, 24 декабря 2021 г.). – Пермь, 2021. Т. 2. С. 129–132.

МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Акапьев В.Л.,

кандидат педагогических наук;

Горбатовская М.С.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в течение последних десятилетий во всем мире наблюдается значительный рост информационно-технологического прогресса. Данный процесс развивается не только в глобальных масштабах, но и затрагивает каждую сферу жизни обычного человека. Однако подобное развитие способствует как значительному росту уровня жизни населения, так и зарождению новых, а также модернизации уже известных видов преступлений, что способствует увеличению процента нераскрытых преступлений. Следовательно, необходимо детальное изучение имеющихся в настоящее время методик, направленных на расследование преступлений в сфере информационных технологий, с целью их дальнейшего развития и поддержания их эффективности в борьбе с указанным видом преступлений. Актуальность выбранной нами темы, прежде всего, опре-

делена интенсивным развитием преступной деятельности, в связи с ее переходом в информационно-технологическую среду, а также проблематикой раскрытия и расследования подобных преступлений.

Ключевые слова: информационные технологии, органы внутренних дел, преступление, расследование преступления, информационное пространство, сеть Интернет.

MODERN METHODS OF INVESTIGATION OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Akapev V.L.,

Candidate of Pedagogical Sciences;

Gorbatovskaya M.S.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: over the past decades, there has been a significant increase in information technology progress around the world. This process is developing not only on a global scale, but also affects every sphere of society. However, such development contributes to a significant increase in the standard of living of the population, as well as the emergence of new, as well as the modernization of already known types of crimes, which contributes to an increase in the percentage of unsolved crimes. Therefore, it is necessary to study in detail the currently available methods aimed at investigating crimes in the field of information technology, in order to further develop them and maintain their effectiveness in combating this type of crime. The relevance of the topic we have chosen is primarily determined by the intensive development of criminal activity, in connection with its transition to the information technology environment, as well as the problems of disclosure and investigation of such crimes.

Keywords: information technologies, internal affairs bodies, crime, crime investigation, information space, Internet.

Преступления в сфере информационных технологий предполагают такие действия, как взлом паролей, предоставляющих доступ к защищенной информации, кражу и последующее распространение подобной информации, создание и распространение вирусов и иных вредоносных программ, незаконное получение номеров банковских карт и иных реквизитов, при помощи которых осуществляется получение доступа к денежным средствам их владельцев. При этом перечисленные выше действия не являются исчерпывающим перечнем, а представляют собой примеры противоправной деятельности, осуществляемой посредством информационных технологий.

При этом, имеется ряд факторов, которые влияют на сложность расследования информационных преступлений:

– во-первых, подобные преступления чаще всего совершаются на просторах информационного пространства, которое обеспечивает своего рода ано-

нимность действий преступных элементов, что позволяет им оставаться незамеченными для правоохранительных органов;

– во-вторых, на просторах сети Интернет, существует огромное количество видеороликов, которые содержат инструкции по созданию собственных информационных ресурсов, что позволяет человеку, обладающему минимальными познаниями в сфере информационных технологий, реализовать свои противоправные действия в Интернете;

– в-третьих, существуют информационные сети, которые позволяют с определенной периодичностью изменять IP-адреса устройств, при помощи которых осуществляется доступ к сети Интернет, что также препятствует определению местоположения источника передачи и приема данных. Подобным информационным ресурсом является DarkNet, который служит основной платформой, используемой лицами для реализации своей преступной деятельности [1, с. 303].

Однако, несмотря на защищенность информационного пространства и существования подобных уловок, современные технологии, стоящие на вооружении правоохранительных органов, позволяют обеспечить эффективное расследование подобных преступлений.

Рассмотрим основные методики, при помощи которых происходит расследование той или иной преступной деятельности, осуществляемой посредством использования информационных технологий:

1. Функционал технологий информационных подразделений правоохранительных органов позволяет отслеживать изменение IP-адресов, устройство, при помощи которых осуществляется доступ в сеть Интернет, а также определять их точное местоположение, что способствует обнаружению лиц, занимающихся преступной деятельностью.

2. Оперативные подразделения, в соответствии со п. 11 и п. 15, ст. 6 Федерального закона «Об оперативно-розыскной деятельности» № 144-ФЗ от 12 августа 1995 года, имеют возможность проводить оперативно-разыскные мероприятия, позволяющие получить доступ к информационно-технологическим устройствам¹. Однако данная деятельность возможна лишь по решению суда, во избежание нарушения ст. 23 Конституции Российской Федерации².

Данные мероприятия позволяют получить информацию, хранящуюся на персональных компьютерах, а также иных устройствах хранения, передачи и получения информации, которая может повлиять на расследование того или иного преступления.

3. Информационными подразделениями органов внутренних дел для расследования преступлений в сфере информационных технологий, связанных с

¹ Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 30 декабря 2020 г.) (принят Государственной Думой 5 июля 1995 года) // Российская газета. 1995. № 160.

² Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: <http://www.pravo.gov.ru>

кражами денежных средств с банковских счетов и банковских карт, довольно эффективно используются блокчейн-технологии, а также проводятся биллинговые мероприятия. Данный метод наиболее эффективен при использовании двух упомянутых элементов совместно.

Так, блокчейн-технологии используются прежде всего для отслеживания транзакций, которые производятся между банковскими счетами, что позволяет определить конечный банковский или иной счет, на который были начислены украденные денежные средства [2, с. 7]. Далее производятся биллинговые мероприятия, которые позволяют определить геолокацию банковской карты, а также телефонного номера, на который она зарегистрирована, посредством отслеживания IMEI-номера мобильного устройства или последней активности банковской карты [3, с. 46].

Следует отметить, что вышеперечисленные методы также не являются исчерпывающими, а представляют лишь ряд методов, которые используются правоохранительными органами для расследования преступлений в сфере информационных технологий.

Согласно официальной статистике, которая предоставлена МВД России, в период за январь – февраль 2023 года количество совершенных преступлений в сфере информационных технологий, возросло на 17,1% относительно показателей прошлых лет. При этом наибольшую долю подобных преступлений составили мошенничества в сфере информационных технологий. Это 40,1% совершенных преступлений, а также кражи в той же сфере, показатель которых достиг 10,9%. Следовательно, опираясь на статистические показатели, можно сделать вывод о недостаточной эффективности современных методов борьбы с данными видами преступности [1].

Для того чтобы понять, в чем же заключаются данные пробелы, рассмотрим процесс раскрытия мошенничеств в сфере информационных технологий.

Итак, структурно данный процесс, как правило, включает в себя целый ряд звеньев, каждое из которых выполняет свои функции. Как и в любой преступной группе, во главе данной структуры стоит организатор – лицо, которое непосредственно сформировало преступную группу и ведет прямое руководство каждым из его звеньев, совершая преступные действия по заранее продуманному плану.

Таковыми лицами часто бывают люди, осужденные за совершение мошенничества, но при этом необязательно в сфере информационных технологий.

Это связано прежде всего с тем, что процесс получения знаний в области информационных технологий доступен абсолютно для всех, вне зависимости от возраста и уровня образования. Однако данные лица лишь организуют преступную деятельность, но не участвуют в его реализации путем непосредственного вмешательства.

Следующим звеном в подобной преступной иерархии является хакер или лицо, обладающее определенными познаниями в сфере информационных технологий. Данный человек не только следит за движением денежных средств, в его обязанности также входит рассылка спам СМС-сообщений, создание ложных ссылок и вирусных программ, выборка лиц, являющихся потенциальными

жертвами, а также создание подставных счетов для обеспечения конспирации в ходе перевода денежных средств с одного банковского счета на другой.

И, наконец, еще одним звеном в данной структуре является посредник. Однако его участие в схемах с мошенничеством в сфере информационных технологий не всегда необходимо.

Оно происходит лишь в тех случаях, когда жертвой преступления выбирается лицо, не имеющее доступа к сети Интернет, пользующееся лишь мобильной связью. Как правило, в роли посредников выступают лица, не имеющие постоянного дохода, целью которых является получение быстрых и легких денег.

Алгоритм совершения преступлений с участием посредников включает в себя следующую последовательность действий. Сначала производится отбор потенциальной жертвы, которыми, как правило, являются пожилые люди, проживающие отдельно от своих детей. При подборе жертвы преступниками учитываются район проживания человека, а также путем несанкционированного доступа к информации с банковских счетов и карт жертвы производится сбор информации о наличии на них денежных средств в том или ином размере.

Далее происходит звонок на номер мобильного телефона жертвы, при этом хакером производится замена голоса на голос, схожий с близкими родственниками лица, в ходе переговоров с которым сообщаются данные, которые заранее подготавливают почву для психологического воздействия на жертву.

Во время звонка преступники представляются родственниками и просят перевести определенную сумму денежных средств под предлогом несчастного случая, при этом настаивая не отключаться и не сообщать о звонке кому-либо из соседей.

Затем при достижении определенной договоренности в дело вступает посредник, жертва должна будет передать ему денежные средства для «оказания помощи» родственникам. Получив деньги, преступник сразу же покидает здание. После чего осуществляется сброс телефонного звонка, и лишь в этот момент человек осознает, что его обманули.

Сложность раскрытия данного преступления заключается в его анонимности. Для совершения махинаций используются подставные банковские счета, а также номера телефонов, зарегистрированные на иных лиц.

Примечательно то, что несмотря на казалось бы хорошую конспирацию и реализацию преступного замысла, в максимально короткие промежутки времени все же существуют способы, которые обеспечивают раскрытие данных видов преступлений.

Одним из самых важных качеств, которое способствует раскрытию подобного преступления, является оперативность. В зависимости от того, как быстро сотрудники полиции прибудут на место происшествия, может определяться скорость и масштабность дальнейшего расследования.

При своевременном прибытии оперативной группы на свои места есть вероятность организации поиска преступника по горячим следам, а также составление фоторобота по методу словесного портрета. Кроме того, внезапное прибытие сотрудников полиции может заставить преступника мешкать и

оставлять следы, которые несут в себе достаточно полезную для всего расследования в целом оперативно значимую информацию. В противном случае расследованием занимаются подразделения по борьбе с информационной преступностью.

Во-первых, в соответствии с Федеральным законом «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ проводится оперативно-розыскное мероприятие «Прослушивание телефонных переговоров» с целью недопущения рецидива преступления, а также определения местоположения лица, с телефона которого осуществлялся звонок¹.

При этом важно получить судебное разрешение на проведение данного мероприятия во избежание нарушения конституционных прав и свобод граждан. После чего, возможны проведения биллинговых мероприятий².

Во-вторых, в случае перечисления денежных средств на банковскую карту или банковский счет, при реагировании в максимально короткий промежуток времени имеется возможность отследить движение денежных средств путем выявления транзакций, произведенных между теми или иными счетами, с установлением их конечного места хранения.

После чего устанавливаются данные хозяина банковского счета или банковской карты, а также номер мобильного телефона, на который она зарегистрирована, и при помощи проведения биллинговых мероприятий устанавливается местоположения мобильного телефона и, соответственно, владельца карты, а также лица, которое непосредственно занимается преступной деятельностью [5, с. 9].

Положительным примером из практики можно считать раскрытие преступления по делу совершения мошеннических действий на сумму 1 550 000 рублей.

Согласно данному делу преступниками совершался обзвон абонентской базы того или иного мобильного оператора с целью сообщения заведомо спланированных ложных данных о том, что родственники того или иного лица, получили травмы определенной степени тяжести в результате дорожно-транспортного происшествия, и им необходима платная медицинская помощь, либо же родственники жертвы «являлись» виновником случившегося дорожно-транспортного происшествия, в результате которого пострадали люди и, чтобы избежать уголовной ответственности, необходимо внести определенную сумму денежных средств³.

Однако расследование данных преступлений не всегда происходит удачно. Все зависит от подготовленности и профессионализма лиц, которые совершают преступление.

¹ Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 30 декабря 2020 года) (принят Государственной Думой 5 июля 1995 г.) // Российская газета. 1995. № 160.

² Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: <http://www.pravo.gov.ru>, 04.07.2020.

³ Приговор Ленинского районного суда г. Пензы (Пензенская область) от 20.09.2021 по делу № 1-234/2021.

Чем быстрее произойдет внедрение в доверие к жертве преступника, тем больше вероятности провести денежные средства по подставным счетам и при помощи замены IP-адреса, «замести следы», что значительно повысит уровень конспирации преступников и практически лишит правоохранные органы возможности отследить передвижение денежных средств, а соответственно, и выявить преступника.

Еще одной причиной, из-за которой растет число совершения преступлений в сфере информационных технологий, является недоверие граждан к сотрудникам органов внутренних дел.

Во-первых, из-за нестабильного уровня раскрываемости данного вида преступления многие граждане зачастую просто не хотят сообщать о совершении подобных преступлений, что приводит к их переходу в разряд латентной преступности.

Во-вторых, недостаточно серьезное отношение граждан к проведению профилактических мероприятий, направленных на минимализацию возможности совершения данных видов преступления.

Так, известно множество случаев когда, буквально через несколько часов после проведения сотрудниками органов внутренних дел профилактических бесед об увеличении случаев мошенничеств в сфере информационных технологий, а также о способах, позволяющих избежать подобную ситуацию, граждане получают звонок с неизвестного номера с требованием о переводе денежных средств под тем или иным предлогом, лишь потом осознавая, что связались с мошенниками.

В-третьих, существуют пробелы в нормативно-правовом регулировании, не позволяющие оперативно действовать при совершении преступления в сфере информационных технологий, что в последующем приводит к утрате ценного времени, а также отрицательной динамике раскрытия данного рода преступлений. При этом технологический процесс не стоит на месте, а значит, зарождаются все новые виды, а также происходит массовая информатизация и компьютеризация уже имеющихся преступлений.

Следовательно, методики их раскрытия правоохранными органами также должны претерпевать своевременную модернизацию, чтобы увеличить эффективность предупреждения подобных преступлений и обеспечить их дальнейшее расследование.

Это должно проявляться в первую очередь в обеспечении правоохранных органов новейшей информационной техникой, которая позволит обеспечить скорость обнаружения и раскрытия преступлений в сфере информационных технологий.

Помимо того, сотрудники правоохранных органов, занимающиеся расследованием преступлений в сфере информационных технологий, должны проходить ежегодную переподготовку с целью получения информации о последних достижениях информационно-технологического прогресса, а также их использования для преступных целей.

Для того чтобы повысить уровень раскрываемости информационных преступлений, необходимо прежде всего решить вопрос с доступом в DarkNet,

а также разработать алгоритм, который смог бы отслеживать IP-адреса устройств, при помощи которых производится выход в Сеть с целью совершения противозаконных действий, даже с учетом их смены через определенный промежуток времени, а также разработать программу, которая смогла бы дистанционно блокировать повторный доступ в сеть для устройства, через которое осуществляется преступная деятельность.

Но возможно ли это с учетом развития технологий и образования граждан на территории нашей страны? Разработка подобных методов для борьбы с преступностью вполне реальна при соответствующем финансировании.

Достаточно обратиться к произошедшему в 2022 году случаю, когда российские хакеры Killnet смогли дестабилизировать работу хакеров Североатлантического альянса из группы Anonymus. Данный пример ярко показывает, что на территории России есть люди, которые могут обеспечить информационную безопасность страны, а соответственно, есть средства и техника, которые могут позволить это сделать.

Мы считаем, что если подобные люди появились бы и в рядах органов внутренних дел, то это способствовало бы резкому росту раскрываемости информационных преступлений, а также повышению уровня доверия к правоохранительным органам со стороны граждан.

Библиографический список

1. Ерошенков Н.В., Цветов В.И. Справочные интернет-ресурсы в раскрытии преступлений, связанных с хищением денежных средств с банковских счетов граждан // Вестник Белгородского юридического института МВД России. 2019. С. 29–35.
2. Краткая характеристика состояния преступности в Российской Федерации за январь – февраль 2023 года // Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: <https://xn--b1aew.xn--p1ai/reports/item/36479770/> (дата обращения: 04.04.2023).
3. Кумышева М.К., Федина Л.М. Актуальные проблемы противодействия преступлениям в сфере информационно-коммуникационных технологий // Образование и право. 2022. № 8. С. 301–306.
4. Ладухин О.В. Получение правоохранительными органами биллинговой информации / О.В. Ладухин, С.А. Невский, М.Н. Пендюрин // Гуманитарные, социально-экономические и общественные науки. 2015. № 1. С. 42–48.
5. Федотова В.В., Емельянов Б.Г., Типнер Л.М. Понятие блокчейн и возможности его использования // European science. 2018. № 1(33). С. 40–48.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ В МЕРОПРИЯТИЯХ ПО ОБНАРУЖЕНИЮ НАРКОТИЧЕСКИХ ВЕЩЕСТВ

Акапьев В.Л.,

кандидат педагогических наук;

Кнутарев А.В.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: одной из отличительных черт трансформации незаконного оборота наркотических веществ как в Российской Федерации, так и во всем мире в настоящее время является его переход в виртуальное пространство, в глобальную сеть Интернет, что вынуждает перестраивать всю систему противодействия наркотрафику со стороны правоохранительных органов. Для снижения количества совершаемых преступлений в данной сфере необходимо безотлагательное внедрение в практику органов внутренних дел специальных информационных технологий, а также реформирование системы подготовки кадров для правоохранительных органов.

Ключевые слова: незаконный оборот наркотических средств, информационно-телекоммуникационная среда, сеть Интернет, наркопреступность.

USE OF INFORMATION TECHNOLOGIES AND SYSTEMS IN DRUG DETECTION ACTIVITIES

Akapev V.L.,

Candidate of Pedagogical Sciences;

Knutarev A.V.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: one of the distinctive features of the transformation of illicit drug trafficking both in the Russian Federation and around the world at present is its transition to the virtual space, to the global Internet, which forces the entire system of countering drug trafficking by law enforcement agencies to be rebuilt. In order to reduce the number of crimes committed in this area, it is necessary to immediately introduce special information technologies into the practice of the Department of Internal Affairs, as well as reform the training system for law enforcement agencies.

Keywords: illicit drug trafficking, information and telecommunication environment, Internet, drug crime.

В настоящее время ведется активное противодействие незаконному сбыту наркотических средств и психотропных веществ. Данная борьба затрагивает все слои общества, и в первую очередь правоохранительные органы Российской Федерации. Распространение наркотических средств и психотропных веществ оказывает негативное влияние на жизнь и здоровье человека и представляет

большую опасность как для самого гражданского общества, так и для всего государства в целом [1, с. 14].

Именно поэтому сейчас противодействие ему входит в число приоритетных задач, стоящих перед органами внутренних дел. Достижения в области информационных технологий дали шанс преступникам создать более легкий бесконтактный способ сбыта наркотических средств с использованием сети Интернет.

Одним из признаков нашего времени является тот факт, что у каждого человека есть смартфон, планшет, компьютер и другие гаджеты, открывающие прямую дорогу в Интернет. Многие граждане имеют аккаунт в таких социальных сетях, как «Одноклассники», «ВКонтакте», Facebook, Instagram, мессенджерах Telegram, WhatsApp, Viber. Все это является определяющим фактором, который дает преступникам возможность привлекать клиентов путем рассылки сообщений с предложениями приобрести запрещенные вещества в виртуальном пространстве [2, с. 206].

Пропаганда наркотических средств и их аналогов, запрещенная на территории Российской Федерации, в настоящее время является одной из основных угроз национальной безопасности по той простой причине, что распространение в сети Интернет данных видов запрещенных средств может вызвать интерес не только у полностью дееспособных лиц, но и у лиц частично дееспособных, например подростков. Тинейджеры, не имеющие жизненного опыта и лишённые контроля со стороны родителей и школы, могут стать легкой добычей для наркодельцов.

В распоряжении преступников для сохранения их анонимности находится широкий арсенал различных средств, приемов и отработанных механизмов. В частности, широкое распространение получили специальные приложения, одним из которых является Changing number – приложение для подмены телефонного номера, которое позволяет сохранить анонимность благодаря вымышленным номерам [3, с. 13].

Конечно, для противодействия наркобизнесу в виртуальном пространстве можно использовать отработанные на практике традиционные оперативно-разыскные методы. Например, метод опроса различных участников чатов, бесед, групп в различных социальных сетях с целью получения необходимой оперативной информации непосредственно из сети Интернет и выявления участников и организаторов преступного бизнеса.

Другим способом может являться метод «наблюдения». Его может реализовывать специально обученный сотрудник правоохранительных органов под вымышленным аккаунтом. Он будет являться активным участником данных сайтов или чатов, где, предполагается, производится сбыт и приобретение наркотических и психотропных веществ для фиксации контактов и следов.

Но при этом необходимо учитывать снижение эффективности данного метода в связи с тем, что информационное пространство – это новый мир со своей спецификой, условностями и участниками, к которому нужен свой особый подход.

Кроме того, в этом пространстве создано огромное количество сайтов и форумов, где люди пытаются сбыть или приобрести наркотические и психотропные вещества, что также затрудняет проведение классических оперативно-разыскных мероприятий [4, с. 27].

Поэтому для борьбы на этом фронте правоохрнительным органам также нужно использовать требуемые информационные технологии и системы, адаптированные к этому направлению деятельности. Поскольку современные способы совершения данного вида преступлений связаны с использованием IT-технологий, то и способы и методика расследования таких преступлений должны быть модернизированы и опираться на соответствующий инструментарий.

Помимо этого необходимо сконцентрировать усилия на создании безопасного интернет-пространства. Одним из возможных вариантов решения данной проблемы видится создание специального подразделения в правоохрнительных органах, которое который будет заниматься «присмотром» за сайтами и их легализацией. В его функционал будет входить обязанность прекращения деятельности тех сайтов, чья активность вызывает подозрения или требует постоянного контроля. Тем самым запускается механизм очистки интернет-пространства от тех участников, чьи мотивы были направлены на преступную деятельность [5, с. 47].

Также необходимо расширить обязанности провайдеров по контролю за участниками интернет-сообществ, в частности по IP-адресам устройств, подключенных к Сети. Или, например, если распространитель наркотических средств осуществляет свою преступную деятельность через сайт, можно попытаться установить владельца домена, которому он принадлежит [6, с. 10].

Каждый из доменов регистрируется в официальных компаниях, которые имеют право на его продажу, и данные о владельцах в настоящее время получить несложно.

Другим направлением борьбы с противоправными действиями в интернет-пространстве является повышение соответствующей информированности населения. Данный способ представляется достаточно эффективным, так как предполагает прямой контакт граждан и сотрудников правоохрнительных органов. Квалифицированный сотрудник, который напрямую работает в данном направлении, будет с помощью официальных сайтов правоохрнительных органов выкладывать информацию, направленную на обеспечения безопасности граждан в сети Интернет, организовывать взаимодействие с другими государственными и образовательными структурами, проводить беседы со школьниками и их родителями, а также реализовывать другие различные и многоплановые мероприятия.

Повышение уровня взаимодействия с населением по вопросам распространения наркотических средств может стать крайне эффективным оружием в руках правоохрнителей.

Анализируя современные информационные методы противодействия незаконному обороту наркотических средств, следует отметить, что необходимо усовершенствование законодательной базы, регулирующей данный вопрос.

Следует перевести на принципиально более высокий уровень техническое оснащение правоохранительных органов, которое позволит использовать в повседневной деятельности новейшие информационные технологии на базе нейросетей, искусственного интеллекта, систем распознавания образов и др.

Все вышеуказанное предъявляет к сотрудникам правоохранительных органов более жесткие требования в части необходимости формирования у них информационно-технологической компетентности соответствующего уровня.

Библиографический список

1. Морозов А.В. Особенности борьбы с наркопреступностью в сфере информационно-телекоммуникационных технологий // Профессионал. 2018. № 4. С. 14–18.

2. Решняк О.А., Ковалев С.А. Проблемы расследования преступлений, совершенных с использованием современных компьютерных технологий // Обеспечение прав и законных интересов граждан в деятельности органов предварительного расследования: сборник статей межведомственного круглого стола (19 октября 2017 г., Орел); под ред. А.В. Булыжкина [и др.]. – Орел: Орловский юридический институт МВД России им. В.В. Лукьянова, 2017. С. 206–208.

3. Усманов И.М. Противодействие преступной деятельности организованных преступных групп, связанных с бесконтактным сбытом наркотических средств: учебное пособие. – Казань: КЮИ МВД России, 2016. – 90 с.

4. Решняк О.А., Лихолетов А.А. Противодействие новым потенциально опасным психоактивным веществам: проблемы правоприменения // Наркоконтроль. 2015. № 2 (39). С. 26–30.

5. Решняк О.А. О некоторых вопросах расследования незаконного сбыта синтетических наркотиков, совершенного бесконтактным способом // Вестник Волгоградской академии МВД России. 2019. № 2 (49). С. 45–50.

6. Билоус Е.Н., Кублова М.Г. Некоторые вопросы деятельности подразделений по контролю за незаконным оборотом наркотиков органов внутренних дел по выявлению сбыта наркотических средств, совершенных бесконтактным способом: сборник научных статей по итогам Недели Российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя. – Рязань: Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2020. С. 9–13.

**УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ
ПРОИЗВОДСТВА ДОПРОСА ПУТЕМ ИСПОЛЬЗОВАНИЯ
СИСТЕМ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ
(СТАТЬЯ 189.1 УГОЛОВНО-ПРОЦЕССУАЛЬНОГО КОДЕКСА
РОССИЙСКОЙ ФЕДЕРАЦИИ)**

Александров А.Н.,

кандидат юридических наук

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются важные вопросы реализации в досудебном производстве по уголовному делу положений уголовно-процессуального законодательства, регламентирующего порядок проведения отдельных следственных действий с применением систем видео-конференц-связи. Обращается внимание на принятие законодателем давно ожидаемого, важного и необходимого решения о дополнении закона соответствующей нормой, которая положительно скажется на эффективности деятельности органов предварительного расследования в ходе производства одного из основных следственных действий – допроса. Приводятся примеры правоприменительной практики и формулируются важные аспекты производства названного следственного действия с применением ведомственной системы видео-конференц-связи. Обращается внимание читателя на важные аспекты фактической реализации законодательных нововведений, соблюдение которых следователем и дознавателям будут способствовать формированию необходимой следственной практики. Формулируются выводы об ожидаемом положительном эффекте применения современных средств связи при производстве отдельных следственных действий по уголовному делу в аспекте повышения эффективности предварительного расследования и обеспечения соблюдения гарантированных конституционных прав граждан на доступ к правосудию.

Ключевые слова: следственные действия, допрос, видео-конференц-связь, следователь, дознаватель, уголовное дело, досудебное производство, эффективность предварительного расследования.

**CRIMINAL PROCEDURAL AND ORGANIZATIONAL ASPECTS
OF INTERROGATION BY USING VIDEO CONFERENCING SYSTEMS
(ARTICLE 189.1 OF THE CODE OF CRIMINAL PROCEDURE
OF THE RUSSIAN FEDERATION)**

Alexandrov A.N.,

Candidate of Law

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article deals with important issues of implementation in pre-trial proceedings in a criminal case of the provisions of the criminal procedure legislation

regulating the procedure for conducting individual investigative actions using video conferencing systems. Attention is drawn to the adoption by the legislator of a long-awaited, important and necessary decision to supplement the law with an appropriate norm, which will have a positive impact on the effectiveness of the activities of the preliminary investigation bodies during the production of one of the main investigative actions - interrogation. Examples of law enforcement practice are given and important aspects of the production of the named investigative action using the departmental video conferencing system are formulated. The reader's attention is drawn to important aspects of the actual implementation of legislative innovations, the observance of which by the investigator and the interrogators will contribute to the formation of the necessary investigative practice. Conclusions are formulated about the expected positive effect of the use of modern means of communication in the production of individual investigative actions in a criminal case, in terms of improving the effectiveness of the preliminary investigation and ensuring compliance with the guaranteed constitutional rights of citizens to access justice.

Keywords: investigative actions, interrogation, video conference call, investigator, inquirer, criminal case, pre-trial proceedings, effectiveness of preliminary investigation.

10 января 2022 г. в законную силу вступил Федеральный закон от 30 декабря 2021 г. № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» (далее – УПК РФ), который ввел в УПК РФ статью 189.1, предусматривающую возможность проведения допроса, очной ставки, опознания путем использования систем видео-конференц-связи (далее – ВКС) по правилам, предусмотренным главой 26, статьями 164, 166–170, 189.1 УПК РФ.

Перед принятием данного закона представителями научной среды и практическими сотрудниками органов предварительного расследования неоднократно высказывались убеждения о необходимости дополнения уголовно-процессуального закона нормой, предусматривающей возможность проведения отдельных следственных действий, и особенно допроса с применением современных технологий различных видов связи [1].

Соответствующие предложения ученых-процессуалистов периодически появлялись в научных публикациях на протяжении более 10 последних лет. В числе таковых высказывали свои мнения С.П. Щерба и Е.А. Архипова, которые предлагали дополнить УПК РФ отдельной нормой, регламентирующей общие правила применения ВКС при производстве следственных действий [2]. Некоторые авторы высказывали мнение о том, что использование ВКС при производстве следственных действий с участием несовершеннолетних лиц позволит им в психологически комфортной обстановке дать показания об известных обстоятельствах [3]. Другие ученые полагали, что использование ВКС в досудебном производстве позволит решить проблему невозможности допроса лиц, находящихся на самоизоляции [4].

Кроме того, в обоснование необходимости включения в УПК РФ нормы об использовании ВКС в досудебном производстве назывался опыт бывших союзных Республик: Беларуси, Казахстана и Украины, в которых действующий уголовно-процессуальный закон позволяет с использованием ВКС допрашивать, проводить очные ставки, предъявлять для опознания [5, 6, 7].

Безусловно, что такие разговоры были основаны на реалиях сегодняшнего времени, явно свидетельствующих о потребностях следственной практики в принятии соответствующих законодательных изменений (дополнений) в целях повышения эффективности деятельности уполномоченных должностных лиц в досудебном производстве по уголовному делу. При этом необходимо отметить, что эти чаяния и ожидания возникли потому, что законодательная регламентация и практическое применение ВКС в российском уголовном процессе, а именно в судебном производстве, существовала на протяжении длительного времени с момента вступления в силу УПК РФ 2001 года. На период принятия законодателем вышеуказанного федерального закона использование современных технологий связи в ходе проведения судебных заседаний по уголовным делам сформировало достаточно внушительную практику, о чем свидетельствовали данные Судебного департамента при Верховном суде Российской Федерации [8].

В пояснительной записке к проекту Федерального закона «О внесении изменений и дополнений в УПК РФ» проблема несвоевременности явки (доставки) свидетелей в установленное судом время признается одной из основных причин увеличения сроков рассмотрения дела, волокиты, нарушения прав и интересов всех участников процесса.

Отмечалось, что для практических работников возможность использования систем ВКС в уголовном судопроизводстве – очевидный плюс. Прежде всего это сокращение сроков следствия (соблюдение положений ст. 6.1 УПК РФ) и уменьшение финансовых затрат на обеспечение процесса расследования. Отмечалось также, что возможность использования ВКС на следствии особенно актуальна для отдаленных регионов страны. В качестве примера приведен опыт следственной практики Следственного управления СК России по Хабаровскому краю, который показал, что по определенной категории дел следователю приходится выезжать в центральные районы России для производства допросов по 4–5 раз, каждый продолжительностью на 2–3 дня [9].

Итак, внесение вышеуказанных дополнений в УПК РФ явилось логичным и ожидаемым решением законодателя для достижения целей качества и эффективности деятельности органов предварительного расследования в досудебном производстве по уголовному делу.

Формирование правоприменительной практики применения вышеуказанной нормы, конечно же, будет сопровождаться определенными организационными сложностями, которые никак не могут повлиять на ожидаемую активизацию использования ВКС при производстве следственных действий уполномоченными должностными лицами.

В настоящий период отмечается положительная практика реализации ст. 189.1 УПК РФ в ряде территориальных органов МВД России. К примеру, уже 19 января 2022 года сотрудниками Управления по организации дознания МВД России по Мурманской области по уголовному делу успешно проведен допрос свидетеля Х. путем использования ведомственной системы ВКС. В ходе допроса установлена личность свидетеля путем сличения документа, удостоверяющего личность, после чего в соответствии с требованиями ст. 164 УПК РФ ему разъяснен порядок проведения следственного действия, а также применяемые при этом технические средства. Дознаватель, находясь в помещении своего рабочего кабинета, при помощи ведомственной системы ВКС создал конференцию в режиме «Все на экране», при которой каждый из участников имел возможность видеть и слышать друг друга в режиме реального времени. Непосредственно после проведения допроса и составления протокола дознавателем оглашены показания свидетеля, о чем в протоколе допроса также сделана отметка. Созданный видеофайл с записью допроса скопирован на оптический диск CD-R, который упакован в бумажный конверт и приобщен к протоколу допроса, о чем в протоколе сделана соответствующая отметка. Сотрудник органа дознания по месту нахождения допрашиваемого свидетеля, находясь с ним в одном помещении, вносил в бланк подписки к протоколу допроса записи и удостоверял их подписями свидетеля. В частности, подписями свидетеля удостоверяются факты: установление его личности, применение видеозаписи следственного действия, разъяснение порядка проведения следственного действия и применяемых технических средств, разъяснение его прав и обязанностей, предупреждение об уголовной ответственности, а также отсутствие замечаний и дополнений к протоколу следственного действия. Подписка к протоколу допроса в течение суток направлена дознавателю посредством ведомственной электронной почты [10].

Внимательный анализ положений ст. 189.1 УПК РФ позволяет выделить важные элементы для их реализации в практической деятельности сотрудников подразделений дознания.

Во-первых, указанные следственные действия должны проводиться только с использованием ведомственной системы ВКС.

Во-вторых, по смыслу части 2 рассматриваемой статьи письменное поручение об организации участия допрашиваемого лица в следственном действии направляется должностным лицом, проводящим предварительное расследование, с учетом его принадлежности к соответствующему органу предварительного расследования. То есть следователь (дознаватель) направляет поручение на имя начальника соответствующего органа дознания с просьбой поручить «своему коллеге – следователю или дознавателю», а при невозможности иному сотруднику органа дознания организацию участия допрашиваемого лица в следственном действии.

Несомненно, что конкретного исполнителя поручения будет определять начальник подразделения дознания и руководитель следственного органа в отношении подчиненных им сотрудников.

Тем не менее целесообразно в поручении акцентировать просьбу о назначении исполнителем именно следователя (дознателя), поскольку он более компетентен в процессуальных вопросах производства допроса, очной ставки или предъявления для опознания, в сравнении с оперуполномоченным или участковым уполномоченным полиции.

В-третьих, протокол следственного действия составляется должностным лицом, в производстве которого находится уголовное дело. При этом необходимо учитывать, что положения ст. 163 «Производство предварительного следствия следственной группой» и ст. 223.1 УПК РФ «Производство дознания группой дознавателей» позволяют следователю и дознавателю, входящему в такую группу, лично производить следственные действия (допрос, очную ставку, предъявление для опознания) с использованием систем ВКС и составлять соответствующий протокол следственного действия. Однако, как нам представляется, само поручение об организации участия допрашиваемого лица в следственном действии должно быть подписано руководителем следственной группы или группы дознавателей, поскольку он в целом организует их работу и руководит их действиями.

В-четвертых, в протоколе допроса указываются дата, место и время не только по месту производства следственного действия, но и по месту нахождения допрашиваемого лица. При этом следователю (дознателю) – инициатору допроса необходимо учитывать часовые пояса в нашей стране, чтобы время проведения следственного действия не пришлось на ночной период (с 22:00 до 6:00) по месту нахождения допрашиваемого лица. Соответственно, в протоколе допроса должны указываться оба варианта.

Таким образом, законодательная регламентация возможности использования ВКС при производстве одного из основных следственных действий, такого как допрос, на стадии предварительного расследования несомненно является верным шагом навстречу ожиданиям и потребностям следственной практики. Активное применение следователями дознавателями положений ст. 189.1 УПК РФ при расследовании уголовных дел позволит сократить не только временные и материальные, но и фактические трудозатраты в досудебном производстве. А самое главное, это положительно отразится на повышении качества и эффективности деятельности органов предварительного расследования, в том числе обеспечении конституционных прав граждан, потерпевших от преступлений, на доступ к правосудию в разумные сроки.

Библиографический список

1. Гаас Н.Н. Использование видео-конференц-связи при производстве следственных действий в стадии предварительного расследования: изменения, в которых нуждается практика // Российский следователь. 2021. № 12. С. 11–15.
2. Щерба С., Архипова Е. Правовые основы применения видео-конференц-связи в уголовном судопроизводстве России и перспективы их совершенствования // Уголовное право. 2014. № 4. С. 109–117.

3. Пашутина О.С., Алымов Д.В. Очная ставка: проблемные аспекты уголовно-процессуального регулирования // Российский следователь. 2020. № 6. С. 13–16.
4. Буфетова М.Ш., Кобзарь Д.Н. Применение систем видео-конференц-связи в уголовном судопроизводстве: перспектива изменения законодательства // Адвокатская практика. 2021. № 1. С. 14–18.
5. Уголовно-процессуальный кодекс Республики Беларусь от 16 июля 1999 г. № 295-3 [Электронный ресурс]. – URL: <https://etalonline.by/document/?regnum=hk9900295> (дата обращения: 18.05.2023).
6. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V [Электронный ресурс]. – URL: <https://online.zakon.kz/Document/?doc> (дата обращения: 18.05.2023).
7. Уголовный процессуальный кодекс Украины от 13 апреля 2012 г. № 4651-VI [Электронный ресурс]. – URL: <http://continent-online.com/Document/?doc> (дата обращения: 18.05.2023).
8. Официальный сайт Судебного департамента при Верховном Суде Российской Федерации [Электронный ресурс]. – URL: <https://www.cdep.ru/index.php?id=79> (дата обращения: 18.05.2023).
9. Официальный сайт Системы обеспечения законодательной деятельности Российской Федерации [Электронный ресурс]. – URL: <https://sozd.duma.gov.ru/bill/112417-5> (дата обращения: 18.05.2023).

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Беспалова А.О.;

Челядинов Д.В.,

кандидат технических наук

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в данной статье рассматриваются некоторые особенности производства следственных действий в ходе расследования преступлений, совершенных с использованием сети Интернет. Актуальность статьи обусловлена тем, что киберпреступность представляет собой серьезную проблему для общества, поскольку ее результатом выступает большой материальный, а также моральный ущерб для граждан. Анализируются варианты способов совершения киберпреступлений, в статье формируются организационные подходы по повышению эффективности проведения первичных следственных действий и оперативно-разыскных мероприятий. Высказываются предложения по совершенствованию деятельности органов внутренних дел по данному направлению оперативно-служебной деятельности.

Ключевые слова: киберпреступность, Интернет, цифровые технологии, средства защиты компьютерной информации, преступление, следственные действия.

FEATURES OF THE INVESTIGATION OF CRIMES COMMITTED USING THE INTERNET

Bespalova A.O.;
Chelyadinov D.V.,

Candidate of Technical Sciences

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: this article discusses some features of the production of investigative actions during the investigation of crimes committed using the Internet. The relevance of the article is due to the fact that cybercrime is a serious problem for society, since its result is a large material, as well as moral damage to citizens. The variants of ways of committing cybercrimes are analyzed, organizational approaches are formed in the article to improve the effectiveness of primary investigative actions and operational investigative measures. Proposals are made to improve the activities of the internal affairs bodies in this area of operational and service activities.

Keywords: cybercrime, Internet, digital technologies, computer information protection tools, crime, investigative actions.

Киберпреступность представляет собой угрозу для современного интернет-зависимого общества и огромную растущую проблему. Исследования показывают, что люди используют онлайн-банкинг, онлайн-покупки и онлайн-социальные сети. Цифровые технологии дают преимущества и создают богатую среду для преступной деятельности – от кражи личных данных, до кражи секретной государственной информации.

Интернет – это самая быстрорастущая инфраструктура в повседневной жизни, а новейшие технологии меняют лицо человечества. Но из-за этих новых технологий мы крайне трудно защитить личную информацию, и, следовательно, количество киберпреступлений в наши дни растет день ото дня. Поскольку большинство коммерческих транзакций совершаются в Интернете, то, соответственно, требуется высокий уровень безопасности.

Повышение безопасности Интернета является решающим фактором для развития общества. Борьба с киберпреступностью требует масштабного и углубленного подхода. Используя только технические меры безопасности, предотвратить преступления в сети Интернет невозможно, поэтому правоохранительные органы должны иметь возможность эффективно расследовать киберпреступления и формировать доказательную базу для дальнейшего предъявления обвинения злоумышленнику [3].

Особенность расследования преступлений, совершенных с использованием сети Интернет, заключается в сборе соответствующих доказательств, что в криминалистическом плане выражается в фиксации и изъятии информации, свидетельствующей о фактах совершения преступления и подтверждающих определенные следственные версии.

Как отмечает А.В. Аносов, информационная сущность фиксации информации, которая относится к числу доказательств совершения преступлений с использованием сети Интернет, заключается в следующем:

- компьютерная информация, содержащаяся на электронном носителе, перекодируется в доступную для человека форму, затем информация изымается вместе с носителем, на котором она содержится. Если изъятие носителя по какой-либо причине невозможно или нецелесообразно, информация будет скопирована;

- принимаются меры по обеспечению безопасности изъятой информации;

- устанавливаются обстоятельства, входящие в предмет доказывания при расследовании данной категории уголовных дел. Примерами являются дата и время совершения преступления, адрес электронной почты, номер абонента сети оператора связи, физический адрес, где находится оборудование;

- оформляются соответствующие протоколы следственных действий, подтверждающие возможность использования изъятой информации в качестве доказательств по уголовному делу [1].

В процессе производства следственных действий необходимо учитывать ряд обстоятельств, оказывающих непосредственное влияние на характер их проведения:

1. Состав информационной системы, а также ее конфигурация. Кроме того, необходимо учитывать количество компьютеров, находящихся в помещении, где планируется расследование.

2. Использование средств защиты компьютерной информации от несанкционированного доступа и их специфика.

3. Способы размещения информации на электронных носителях, а также способы их обработки и форматы представления.

В процессе расследования преступлений, совершенных с использованием сети Интернет, производятся следующие следственные действия:

- следственный осмотр, включающий осмотр места происшествия, предметов и документов;

- поиск, включающий в себя обследование предприятий различных форм собственности, в том числе в жилище, а также личный обыск;

- выемка, под которой понимается изъятие информации, представляющей ценность по данной категории уголовных дел, с носителем или без такового, а также изъятие компьютерной техники;

- назначение экспертизы. При этом на экспертизу направляются технические средства, технологии, сообщения и другие электронные устройства, с помощью которых было совершено расследуемое преступное деяние.

Как отмечает Р.О. Баландюк, методика расследования преступлений, совершенных с использованием сети Интернет, полностью зависит от вида конкретного преступления [2].

На примере расследования преступлений, связанных с несанкционированным доступом к компьютерной информации, на начальном этапе расследования необходимо будет вынести постановление о назначении программно-технической криминалистической экспертизы для определения места, откуда

был совершен несанкционированный доступ к компьютерной информации. Кроме того, данная проверка позволит выявить и другие аспекты совершенного преступления [4].

Следующий этап предполагает выдвижение следственных версий. Например, одной из таких версий является осуществление несанкционированного доступа к компьютерной информации из хулиганских побуждений. Проработка этой версии включает в себя проверку состояния компьютеров, компьютерных сетей и носителей информации, допросы лиц и т.д. Результатом этого этапа расследования должна стать идентификация подозреваемого.

Логичным продолжением проведения мероприятий является сбор доказательств, подтверждающих вину подозреваемого. На данном этапе осуществляются такие следственные действия, как допрос подозреваемого, свидетелей и потерпевших, производство следственных экспериментов, назначение необходимых экспертиз.

Рассмотрим некоторые виды преступлений, совершаемых с использованием сети Интернет.

Киберпреследование – это преступление, в котором используются электронные средства для преследования, беспокойства и жестокого обращения с одним человеком, преследуемым конкретно по причинам гнева, мести или ярости.

Взлом – это преступление, связанное со взломом систем и получением несанкционированного доступа к данным. Многие хакеры пытаются получить доступ к ресурсам с помощью программного обеспечения для взлома паролей для доступа к компьютеру.

Фишинг – это действие, направленное на то, чтобы обмануть людей, чтобы получить финансовые данные, личную информацию, такую как имя пользователя, пароль для доступа к своей учетной записи.

Вишинг – это электронная стратегия введения в заблуждение, при которой людей обманывают, заставляя раскрывать основные денежные или личные данные неутвержденным элементам [3].

Таким образом, глобальная сеть Интернет связана с национальной безопасностью, поскольку компьютеры исполняют роль службы экстренной помощи, правительственных операций, банковского дела, транспорта, энергетики и телекоммуникаций. Несмотря на то, что данные предоставляют пользователям бесчисленные возможности, эти преимущества могут быть использованы в преступных целях. Для борьбы с киберпреступностью необходимы меры безопасности, предназначенные для защиты данных и конфиденциальности пользователей. Преступления, совершенные с использованием сети Интернет, увеличиваются с каждым днем, и их необходимо своевременно раскрывать [5].

При расследовании конкретных видов преступлений характер и методика подлежат уточнению с учетом специфики деяния. Необходимо определить особенности проведения следственных действий для каждого вида преступления и разработать определенный алгоритм действий для сотрудников органов внутренних дел, осуществляющих выявление, пресечение и раскрытие преступлений рассматриваемой категории.

Библиографический список

1. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие. В 2 ч. – Москва: Академия управления МВД России, 2019. Ч. 1. – 208 с.
2. Баландюк О.Р. Методика расследования отдельных видов преступлений, совершаемых в сфере интернет-технологий // Вестник Белгородского юридического института МВД России. 2015. № 2. С. 96–99.
3. Малыхина Н.И., Кузьмина С.В. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети интернет // Вестник Томского государственного университета. 2021. № 462. С. 238–247.
4. Смушкин А.Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. № 3. С. 102–111.
5. Газимуллин И.Ю. Некоторые организационно-тактические особенности противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Право: ретроспектива и перспектива. 2022. № 1. С. 50–54.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В СИСТЕМЕ КИБЕРБЕЗОПАСНОСТИ

Борисенко А.В.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в данной статье поднимаются вопросы информатизации общества, уделяется особое внимание обеспечению кибербезопасности пользователей. Рассматриваются инциденты в сфере информационной безопасности, возможности утечки информации при работе пользователя в Сети. Кибератаки со стороны злоумышленников, в том числе и служб иностранных разведок, становятся все более масштабными, что заставляет уделять особое внимание вопросам кибербезопасности.

Ключевые слова: кибербезопасность, инциденты, информационная безопасность; методы социальной инженерии.

THE HUMAN FACTOR IN THE CYBERSECURITY SYSTEM

Borisenko A.V.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: this article raises issues of informatization of society, pays special attention to ensuring the cybersecurity of users. Incidents in the field of information security, the possibility of information leakage when a user is working on the network are considered. Cyber attacks by malefactors, including foreign intelligence services, are becoming more and more large-scale, which forces us to pay special attention to cybersecurity issues.

Keywords: cybersecurity, incidents, information security; social engineering methods.

В последние десятилетие всеобщая информатизация общества, развитие информационных технологий и глобальной сети Интернет оказывают сильное влияние на повседневную жизнь граждан Российской Федерации. В ходе открытия XII Российского форума по управлению Интернетом были приведены следующие сведения по статистике пользования им: в России насчитывается около 130 млн интернет-пользователей, что составляет практически 90% населения страны. Таким образом, доступ в Интернет есть практически в каждой российской семье.

Однако не все пользователи Сети задумываются об обеспечении кибербезопасности своих устройств и мерах по защите своей конфиденциальной информации. Помимо этого, в современных условиях критическая инфраструктура Российской Федерации подвергается кибератакам со стороны иностранных государств, а ее безопасность и надежность функционирования является ключевым моментом в вопросе стабильности и процветания страны.

Интенсивный рост числа кибератак заставляет задуматься о создании эффективной системы кибербезопасности. В создании такой системы должен быть применен комплексный подход, учитывающий не только развитие информационных технологий и защиту терминального оборудования программными средствами, но и уровень информационной грамотности пользователей конечных устройств [1, 5].

Любые действия, производимые с информацией (создание, обработка, передача и удаление) осуществляются пользователями, которые становятся частью информационной системы.

По сведениям компании Group-IB, 94% всех совершаемых кибератак происходит из-за человеческого фактора. Основные способы совершения атак на частных лиц представлены на рисунке 1 [8].



Рисунок 1. Основные способы совершения кибератак на частных лиц

Наиболее распространенным способом совершения кибератак является фишинг, т.е. вид интернет-мошенничества, используемого для получения конфиденциальных данных пользователя путем распространения вредоносных электронных писем, ссылок для скачивания вредоносного программного обеспечения или перехода на сайты мошенников [2, 3]. Небрежность и халатность в действиях пользователей приводят к осуществлению злоумышленником несанкционированного доступа к информации, обрабатываемой автоматизированными системами или средствами вычислительной техники. Пренебрегая основными принципами информационной гигиены, пользователь Сети подвергает риску кибератаки не только свою личную конфиденциальную информацию, но и информационную структуру предприятий и государственных органов, являясь сотрудником этих организаций. Другими словами, пользователь становится слабым звеном в системах кибербезопасности.

Поэтому, принимая во внимание поэтапное совершенствование технических и программных средств защиты информации (далее – СЗИ), злоумышленник будет направлять свои усилия по преодолению СЗИ на авторизированных пользователей – персонала организации [6]. Применяя различные сочетания методов социальной инженерии, психологии, человеческих потребностей и нужд, злоумышленник получает возможность доступа к конфиденциальной информации и другим охраняемым ресурсам с помощью непосредственного оператора информационной системы.

По данным МВД России, показатели киберпреступности за 2022 год в целом остались стабильными относительно 2021 года. Каждое четвертое преступление в Российской Федерации совершается с использованием высоких технологий. Обращаясь к статистике за январь – февраль 2023 года, можно отметить значительный рост числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий на 17,1% – этот показатель наглядно демонстрирует активность действий злоумышленников в IT-сфере [7].

Для предотвращения попыток получения конфиденциальной информации необходимо проводить систематические занятия с сотрудниками о способах и методах, применяемых злоумышленниками для достижения корыстных целей, регулярно информировать сотрудников о степени ущерба вследствие необдуманных действий и личной ответственности каждого. Одним из способов «профилактики» может быть попытка воссоздания действий злоумышленников. Необходимо организовать проведение так называемой ложной атаки с целью проверки пользователей на бдительность [8, 9]. Например, осуществляется рассылка сообщений на электронную почту пользователей с недостоверного аккаунта. После чего анализируются действия пользователей с данным сообщением, указываются ошибки и предоставляются алгоритмы правильных действий в подобных случаях.

Грамотное администрирование и настройка прав доступа являются залогом безопасности данных, хранящихся на устройствах [4]. Установка пользователями стороннего нелицензионного программного обеспечения может привести к утечке информации и осуществлению злоумышленниками кибератаки. Обязательное использование антивирусных программ и сетевых фильтров, а также использование безопасного пароля и его периодическая смена повышают надежность системы в целом.

Таким образом, одним из самых уязвимых звеньев в системе кибербезопасности является человеческий фактор. Для предотвращения атак методами социальной инженерии необходимо проводить информационную работу с пользователями оконечных устройств и акцентировать особое внимание на информационной гигиене при использовании сетевых ресурсов. Контроль и мониторинг установленного программного обеспечения, использование только лицензионного программного обеспечения и регулярное обновление операционной системы позволят снизить риски совершения удачной кибератаки злоумышленником. Применение продуманной политики безопасности позволит сохранить конфиденциальную информацию в целостности, а установленная антивирусная программа – выявить и устранить угрозы безопасности информации.

Библиографический список

1. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник. – Москва: РИОР: ИНФРА-М, 2022. – 202 с.
2. Белоус А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – Москва; Вологда: Инфра-Инженерия, 2020. – 692 с.

3. Диогенес Ю., Озкая Э. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д.А. Беликова. – Москва: ДМК Пресс, 2020. – 326 с.
4. Ищейнов В.Я. Информационная безопасность и защита информации: теория и практика: учебное пособие. – Москва; Берлин: Директ-Медиа, 2020. – 270 с.
5. Сэрра Э. Кибербезопасность: правила игры: Как руководители и сотрудники влияют на культуру безопасности в компании / пер. с англ. – Москва: Альпина ПРО, 2022. – 189 с.
6. Шаньгин В.Ф. Информационная безопасность и защита информации. – Москва: ДМК Пресс, 2017. – 702 с.
7. Официальный сайт МВД России [Электронный ресурс]. – URL: <https://мвд.рф>
8. Официальный сайт компании «Лаборатория Касперского» [Электронный ресурс]. – URL: <https://www.kaspersky.ru>
9. Официальный сайт компании «Мобильный криминалист» [Электронный ресурс]. – URL: <https://mko-systems.ru/mobile-kriminalist>

КИБЕРБЕЗОПАСНОСТЬ. ПРОБЛЕМЫ МОТИВАЦИИ ОБУЧЕНИЯ

Гаврющенко А.П.,

кандидат технических наук

(Белгородский юридический институт МВД России имени И. Д. Путилина)

Аннотация: в статье рассмотрены проблемы мотивации познавательной деятельности обучающихся, в том числе дистанционно. Предложены решения, включающие использование в учебном процессе научно-популярных статей ведущих банков, посвященных обеспечению кибербезопасности клиентов.

Ключевые слова: кибербезопасность, информационная безопасность, финансовая безопасность, мотивация.

CYBERSECURITY. PROBLEMS OF LEARNING MOTIVATION

Gavryushchenko A.P.,

Candidate of Technical Sciences

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the problems of motivation of cognitive activity of trainees, including those studying remotely, are considered. Solutions are proposed that include the use in the educational process of popular science articles by leading banks dedicated to ensuring the cybersecurity of customers.

Keywords: cybersecurity, information security, financial security, motivation.

Дисциплина «Основы кибербезопасности» была введена в Бел ЮИ МВД России имени И.Д. Путилина для обучения курсантов по всем специальностям, а также для изучения ее слушателями на курсах профессиональной подготовки. Пандемия коронавируса Covid-19, а затем проведение специальной военной операции повлекло значительные изменения в методике обучения в Белгородской области. В основном применяются дистанционные методы получения знаний, в рамках которых стало сложнее мотивировать слушателей и курсантов.

В данной статье для стимулирования познавательной деятельности по направлению «Кибербезопасность» и повышения интереса к изучению разделов курса «Основы кибербезопасности» предлагается использовать наработки специалистов-профессионалов в области информационной безопасности. Как известно, наиболее квалифицированными службами безопасности обладают ведущие банки России, так как информационная безопасность тесно связана с финансовой безопасностью данных организаций.

На сайтах многих банков имеется раздел, посвященный кибербезопасности клиентов. Как правило, в нем представлены статьи, посвященные вопросам финансовой и информационной безопасности, в которых в доступной форме разъясняют многие положения по безопасности в киберсфере. В результате анализа содержания статей можно сделать вывод, что их тематика охватывает свыше 50% материала курса «Основы кибербезопасности», который преподается в Бел ЮИ МВД России имени И.Д. Путилина.

Таким образом, эти материалы способствуют развитию положительной мотивации, повышению уровня учебно-познавательного интереса курсантов, результативности учебного процесса по данному курсу, так как характеризуются использованием различных форм подачи информации, в том числе и игровых технологий, простотой и доступностью изложения, исключающей избыток технических терминов и понятий, что наиболее подходит для специалистов в области юриспруденции.

В данной статье на примере крупнейшего банка Российской Федерации – Сбербанка демонстрируется имеющаяся библиотека статей, посвященных обеспечению кибербезопасности, и форма представления материала.

Ниже представлены наименования статей и их краткое содержание.

В библиотеке знаний по кибербезопасности – «Кибрарий» находится важная информация о кибербезопасности, чтобы облегчить защиту от мошенников своих личных данных, паролей и денег [1].

Двухфакторная аутентификация. В этой статье мы разберем, что такое двухфакторная аутентификация, где и для чего она используется и гарантирует ли стопроцентную защиту.

Как мошенники оформляют кредиты на других людей. Каждый банковский клиент рискует стать жертвой кредитных преступников. Третьи лица могут завладеть его персональными данными и использовать их для получения займов. Предотвратить проблему поможет бдительность и специализированные сервисы.

Оценка риска от разглашения КИ в источниках данных с интеллектуальным анализом. Степень развития методов, позволяющих оценить уровень риска от распространения конфиденциальной информации в источниках, не предназначенных для этого, достаточно низкая.

Обзор технологий выявления модифицированного контента класса DeepFake. В работе приводится обзор публикаций об основных технологиях выявления модифицированного контента класса DeepFake.

Доверяй, но проверяй: как распознать фейк и защитить деньги. Прародительница сегодняшних фейковых сообщений – «газетная утка» – появилась более трехсот лет назад.

Использование технологий искусственного интеллекта в построении режима КТ. До сих пор остается нерешенной задача надежного выявления в информационном потоке актуальных сведений, составляющих коммерческую тайну.

Прогноз влияния перспективных технологий на ландшафт угроз кибербезопасности. Лаборатория кибербезопасности Сбербанка выпустила аналитический отчет «Прогноз влияния перспективных технологий на ландшафт угроз кибербезопасности».

Мошенники обманывают юридических лиц. Описываются самые распространенные схемы и объясняется, как действовать, чтобы бизнес не пострадал.

Телефонный развод. В борьбе с «звонарями» необходим комплексный подход. Россияне все чаще жалуются на звонки от неизвестных, которые представляются сотрудниками различных банков и рассказывают о компенсациях и подозрительных операциях.

Помоги себе сам. Как пенсионеру защититься от мошенников. Иногда кажется, что мошенники точно не смогут обмануть.

Как искусственный интеллект защищает данные клиентов Сбера. Часть 2. Речь пойдет о процессе защиты от утечек информации и системах DLP (Data Leakage Prevention).

Угрозы и риски утечки персональных данных. Как часто, регистрируясь на каком-либо сайте или взаимодействуя в социальных сетях, мы задумываемся о том, какой цифровой след мы оставляем после себя? Почему мы не должны игнорировать безопасность персональных данных?

Тайны и опасности социальных сетей. Социальные сети могут быть небезопасны, особенно если не знать о некоторых их особенностях.

Как безопасно пользоваться картами. Несколько советов по безопасному использованию банковских карт.

Процессный подход в управлении кибербезопасностью. Высокий уровень технологий требует регулирования и координации на всех уровнях управления действиями организации и особенно при обеспечении кибербезопасности.

Сохрани свою уникальность: как защитить персональные данные от утечки. Каждый день, делая покупки в Интернете, заходя в соцсети, переписываясь в мессенджерах, пользуясь мобильным банком, мы оставляем цифровой след.

Как искусственный интеллект защищает данные клиентов Сбера. Часть 1. Оперативный обмен большими объемами данных и их обработка стали необходимым условием для успешного ведения бизнеса.

Что такое Threat Intelligence и как его применять? Организации нуждаются в информации и знаниях об актуальных киберугрозах, техниках и тактиках злоумышленников, а также выявляемых критических уязвимостях ИТ-систем.

Предотвращение утечек информации с помощью DLP-системы. Информация – ценнейший актив любого современного предприятия. Бизнес многих компаний основан на обладании информацией, которой нет у конкурентов.

Какие угрозы могут содержаться в обычном письме. При поиске товаров, услуг или развлечений в Интернете каждый рискует попасть на фишинговую страницу. Чтобы отличить фейковый сайт от настоящего, важно знать признаки подделок злоумышленников.

Почему социальные сети знают о нас больше, чем друзья и родные. В Интернете мы делаем практически все: учимся, развлекаемся, общаемся, покупаем и продаем. Но, несмотря на это, важная информация о нас и о нашей жизни все-таки должна оставаться в офлайне.

Pentest как метод оценки безопасности организации и сервисов. Тестирование на проникновение (англ. *pentest*) — вид работ по выявлению уязвимостей, основанный на моделировании действий потенциального нарушителя.

Меры защиты от вредоносного ПО. Каждый день обнаруживается 300 тыс. новых вредоносных программ. Как защитить компанию от вредоносного заражения? В разделе – описание мер защиты и обзор классов решений для эффективной защиты от вредоносных.

Спам – сколько его в твоём ящике? К сожалению, не все емейлы полезны: технологическими возможностями электронной переписки пользуются и недобросовестные люди.

Подключай с умом. Как защитить устройства интернета вещей? Если в доме установлены умные колонки, автоматические умные термостаты и пр., то технологии, используемые у вас дома, не должны подвергаться риску.

Это должен знать каждый. Правила удаленной работы. Удаленной (дистанционной) работой называется такой режим труда, при котором рабочим местом признается личное жилище работника.

Как перевести офис на удаленную работу: основные этапы. Чек-лист основных этапов безопасной удаленной работы офиса поможет организовать или проверить кибербезопасность «удаленки» в офисе.

Как определить фишинговый сайт. Фишинг является наиболее популярным на сегодняшний день видом атак, потому что он не требует специальной подготовки, знаний или затрат мошенников, но в то же время прост в реализации.

Твой мобильный телефон – опасный враг или верный помощник? Смартфон в руках каждого современного человека – это большое количество рисков и «слепых зон», через которые к нему могут подобраться мошенники.

Как пользоваться умной техникой, чтобы не стать жертвой мошенников. Опросы показывают, что почти 70% россиян хотели бы жить в доме со

специальными датчиками, реагирующими на голос, свет или прикосновение, и с работающими в паре с ними приборами.

Чем опасен фишинг? Мы ежедневно получаем большое количество сообщений в свои электронные ящики. И часть из них может быть фишинговыми письмами.

Вся правда о паролях. Любой аккаунт от онлайн-банка, почтовой службы и даже социальной сети хранит важную информацию, которая является желанной целью злоумышленников.

Номер школы и геолокация: что нельзя выкладывать в Интернет. В Интернете много мошенников, которые вымогают у детей и взрослых их личные данные. О чем не стоит рассказывать?

Как уберечь ребенка от вредного контента в Сети. Дети могут случайно (или неслучайно) найти и посмотреть запрещенные для их возраста и даже незаконные сайты.

Вишинг. Как защититься от телефонных мошенников. В России бум телефонного мошенничества. За последние два года злоумышленники звонят своим жертвам в 11 раз чаще, чем раньше.

Вредоносное программное обеспечение. Классификация вредоносного ПО, способы распространения и целевой функционал вредоносов. Практические рекомендации и методы защиты компьютеров от заражения вредоносным ПО.

Приложения и программы для родителей и детей, которые помогут защитить ребенка в Сети. Чтобы и ребенку, и взрослому было спокойнее погружаться в онлайн-мир, выделено 5 основных направлений в защите данных для тех, кто хочет безопасно пользоваться Интернетом и гаджетами.

СберБанк предупредит: как узнать, что вам звонят жулики. Только за прошлый год мошенники позвонили жителям России 15 млн раз. Рассказывается о том, как не поддаться на их уловки.

Телефонное мошенничество – виды и схемы обмана. Сегодня злоумышленники пользуются разнообразными способами обмана пользователей телефонов. Есть несколько популярных способов обмана, которые рекомендуется запомнить.

Конкурсы, в которых побеждают только мошенники. Жулики любят прикрываться именами знаменитостей, чтобы выманить деньги. Особенно активно этот вид мошенничества используют в соцсетях.

Правила защиты ребенка в Интернете. Пять правил, которые помогут создать доверительные отношения между ребенком и родителями, и при этом соблюсти все требования кибербезопасности.

Как мошенники выводят деньги с украденных телефонов. Тот, кто лишился смартфона, почти всегда звонит на него в надежде вернуть назад [1].

Далее приводится содержание одной из статей.

Двухфакторная аутентификация

Что такое двухфакторная аутентификация, где и для чего она используется и гарантирует ли стопроцентную защиту?

Двухфакторная аутентификация (2FA, two-factor authentication) – это наиболее часто используемый тип многофакторной аутентификации (MFA),

требующий дополнительный (второй) фактор аутентификации к паролю (первый фактор).

Двухфакторная аутентификация является дополнительной защитой и используется при входе в различные онлайн-сервисы – электронную почту, социальные сети, мессенджеры, онлайн-банкинг и т.д. В настоящее время все больше компаний внедряют поддержку 2FA на своих ресурсах [1].

Зачем нужна двухфакторная аутентификация?

У многих может возникнуть вопрос: «Зачем нужна двухфакторная аутентификация, когда есть надежный пароль»? Важно понимать, что двухфакторная аутентификация не заменяет пароль, а дополняет (усиливает) его. Например, когда приложение для онлайн-банкинга требует от клиента ввести пароль и отправленный на телефон в виде СМС-сообщения проверочный код, это означает, что оно использует 2FA.

Благодаря двухфакторной аутентификации вы выстраиваете дополнительную линию защиты своего аккаунта и персональных данных. Включая 2FA, вы защищаете информацию надежнее и эффективнее, чем при классическом подходе с одним паролем.

Если пароль можно подобрать или скомпрометировать в ходе утечки, то для взлома второго фактора аутентификации требуется гораздо больше усилий. Соответственно, 2FA повышает безопасность аккаунта и лучше защищает организацию и ее пользователей от несанкционированного доступа.

Еще одним преимуществом 2FA является то, что данный метод способен предупреждать пользователя о попытках взлома аккаунта. Например, если на ваш телефон приходит сообщение с одноразовым кодом для входа в аккаунт, а вы никаких подобных попыток не предпринимали, то это может означать, что ваш аккаунт пытаются взломать – самое время менять пароль на более сложный!

Как работает двухфакторная аутентификация:



Как показано на схеме, сначала нужно ввести свой логин и пароль от учетной записи – 1-й фактор (фактор знания). Затем на мобильный телефон поступает push-уведомление в виде одноразового кода. Мобильное устройство – 2-й фактор (фактор владения) – то, что есть, и для завершения аутентификации нужно доказать факт владения им [1].

К многофакторной аутентификации относят 3 категории факторов:

1. **Знание** – информация, которая известна пользователю. Например, пароль, ПИН-код, контрольное слово и т.д.

2. **Владение** – вещь, которой обладает пользователь. Например, смартфон, пластиковая карта, токен и т.д.

3. **Свойство** – уникальные биометрические данные. Например, отпечатки пальцев, радужная оболочка глаз, распознавание лица, последовательность ДНК [1].



Комбинации 2FA могут быть разными, например:

- пароль + sms/push-уведомление;
- пароль + сертификат;
- отпечаток пальца + ОТР (одноразовый пароль);
- PIN-код + лицевая биометрия.

Стоит обратить внимание, что правильная двухфакторная аутентификация – это подтверждение личности с помощью двух **разных** факторов (знание, владение, свойство). Например, комбинация «Пароль + PIN-код» не будет являться 2FA, так как данные относятся к одному фактору (фактор знания). Данная комбинация подходит под определение 2SV (two-step verification) – двухшаговая верификация [1].

Может ли 2FA заменить традиционные пароли?

При помощи беспарольной 2FA можно забыть о паролях в принципе, так как пароли имеют ряд недостатков: теряются, забываются, подбираются (взламываются). Также не стоит забывать, что количество паролей стремительно увеличивается по мере роста количества онлайн-сервисов. Многие организации внедряют аутентификацию без пароля с помощью двухфакторной аутентификации, которая опирается на факторы владения, свойства и поведенческие факторы для проверки личности. Аутентификация без пароля снижает уязвимость к атакам, направленным на пароли (например, фишинговым), и решает проблемы, связанные с утечками баз данных. Например, можно попасть в личный кабинет, приложив отпечаток пальца и магнитный ключ. Этого будет достаточно для авторизации, пароль не потребуется.

Как включить двухфакторную аутентификацию?

Для начала нужно определиться, на каком ресурсе требуется включить 2FA, и проверить, есть ли такая возможность. Многие онлайн-сервисы пока не предоставляют такой поддержки [1].

В зависимости от онлайн-сервиса дополнительная защита может включаться и работать по-разному. Как правило, в разделе «Помощь» или «Настройки» можно найти подробную информацию об активации 2FA. Будьте готовы, что названия данной настройки могут отличаться (например, «Двухфакторная аутентификация», 2FA, «Подтверждение входа» и т.д.) [1].

Таким образом, собрав базу соответствующих ссылок на статьи, размещенные на сайтах таких банков, как «Сбербанк» [1], «Открытие» [2], «Россельхозбанк» [3] и др., предлагается их включить в список дополнительной литературы для самостоятельного изучения курсантами и слушателями. В ходе ознакомления с указанной для самостоятельной работы статьей обучаемые непроизвольно знакомятся и с другими материалами, касающимися информационной безопасности, повышая свою эрудицию, в том числе и по вопросам кибербезопасности. Это подтверждено результатами успеваемости в различных группах разных потоков.

Библиографический список

1. Сбербанк // Официальный сайт [Электронный ресурс]. – URL: <http://www.sberbank.ru/ru/person/cybersecurity>
2. Банк «Открытие» // Официальный сайт [Электронный ресурс]. – URL: https://www.open.ru/security?from=main_footer
3. Россельхозбанк // Официальный сайт [Электронный ресурс]. – URL: <https://www.rshb.ru/security>

ДЕАНОНИМИЗАЦИЯ ПРАВОНАРУШИТЕЛЕЙ В СЕТИ: ПРОБЛЕМЫ И ОТДЕЛЬНЫЕ ПУТИ РЕШЕНИЯ

Гончар В.В.,

кандидат юридических наук, доцент;

Аветисян К.Р.

(Московский университет МВД России имени В.Я. Кикотя);

Аветисян Б.Р.

(Научно-исследовательский институт образования и науки)

Аннотация: в статье рассматриваются основные теоретические, юридические и технические аспекты установления лиц, совершающих преступления в сфере информационных технологий. Особое внимание уделено описанию механизмов маскирования передачи данных и установлению ключевых элементов модели противодействия анонимной работе правонарушителей, построенной на основе SDN (Software Defined Networking), DXE (Decentralized Exchange), DPI (Deep Packet Inspection), AML (Anti-Money Laundering), KYC (Know your Customer/Client) и KYT (Know your Transaction) технологий.

Ключевые слова: противодействие киберпреступности, деанонимизация, логирование удаленного управления, эвристические методы анализа трафика, децентрализованные криптобиржи.

DEANONYMIZATION OF OFFENDERS ONLINE: PROBLEMS AND INDIVIDUAL SOLUTIONS

Gonchar V.V.,

Candidate of Law, Associate Professor;

Avetisyan K.R.

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Avetisyan B.R.

(Research institute of Education and Science)

Abstract: the article discusses the main theoretical, legal and technical aspects of identifying persons who commit crimes in the field of information technology. Special attention is paid to the description of the mechanisms of masking data transmission and the establishment of key elements of the model of countering the anonymous work of offenders, based on technologies: SDN (Software Defined Networking), DXE (Decentralized Exchange), DPI (Deep Packet Inspection), AML (Anti-Money Laundering), KYC (Know your Customer/Client) and KYT- (Know your Transaction).

Keywords: countering cybercrime, deanonymization, remote control logging, heuristic methods of traffic analysis, decentralized crypto exchanges.

Контроль цифрового пространства со стороны государственных органов является обязательным элементом безопасности личности, общества и государства. Этот механизм можно представить в виде процессуального, технического и силового элементов. Взаимодействие вышеуказанных элементов будет определять эффективность контроля информации, в частности на Deep-Web-платформах [1, 2]. На территории России выход в открытую сеть реализован через национальный домен .ru [3].

Регистрируясь в доменных именах домена .ru, необходимо предоставить соответствующую установочную информацию [4] о лице и заполнить обязательную документацию, в том числе заполнить анкету владельца домена, где необходимо указать паспортные данные [5], и при обнаружении следов организации незаконной деятельности на доменном имени, зарегистрированном в домене .ru, правоохранительным органам представляется возможным установить владельца данного ресурса, на основании подпункта 2 пункта 1 статьи 64 ФЗ № 126 от 7 июля 2003 г. «О связи», который обязывает операторов связи хранить информацию на территории Российской Федерации до шести месяцев. Данный фактор существенно ограничивает время хранения оперативно значи-

мых сведений, посредством которых возможна реализация мероприятий по обнаружению искомого лица [6].

Зарегистрированное доменное имя ресурса выступает одним из идентификаторов, позволяющих установить владельца хоста (персональный компьютер, сервер, локальная сеть и т.д. – устройства с предустановленным сетевым оборудованием либо устройства с модульно интегрированным сетевым интерфейсом), а именно лицо, на которое оно зарегистрировано. При анализе сетевого трафика следует понимать, что наряду с IPv4 – интернет-протоколом четвертой версии необходимо обратить внимание и на MAC-адрес исследуемых узлов [7]. Уникальными идентификаторами в глобальной сети выступают «белые» IP-адреса.

На каждом устройстве с сетевым интерфейсом существует ряд идентификаторов (IP-адрес и MAC-адрес), посредством которых оператор реализует целевую активность в глобальной сети.

В большинстве локальных сетей предусмотрен выход в глобальную сеть через сетевое оборудование MAN (Metropolitan Area Network) [8]. На внутренний сервер с настроенным DHCP (Dynamic Host Configuration Protocol) [9], позволяющим в автоматическом режиме присваивать подключаемым сетевым узлам IP-адреса из диапазона, определенного маской сети, существует сетевой кабель. Выход в Интернет пользователями данной сети, обслуживаемыми вышеуказанным сервером, независимо от топологии сети: кольцо, шина, звезда, древо, и т.д. – реализован посредством сетевого протокола NAT [9]. При наличии соответствующих сведений за интересующий период времени, производится корреляция – сопоставляются внутренние (локальные) IP-адреса с внешними IP-адресами (глобальными), посредством которых узлы локальной сети взаимодействовали с ресурсами глобальной сети, туннелируемыми узлами (например, облачными хранилищами) и др.

Одним из наиболее важных компонентов при анализе активности сетевых узлов, наряду с сопоставлением белых и серых IP-адресов исследуемых объектов (лиц и их активности в сети), выступают директории хранения журналов активности узлов, условно называемые «время их жизни» (сколько времени до перезаписи данных в рамках центров обработки данных (ЦОД)), а также таблицы маршрутизации, обеспечивающие корректную маршрутизацию пакетов данных по обслуживаемым сервером узлам [10].

Представляя глобальную сеть в виде единой магистральной транснациональной сети по всему миру с различными уровнями доступа ее пользователей, введем понятие цифровой юрисдикции, которую следует понимать как контролируемый государством индексируемый сегмент глобальной сети. Неиндексируемые, постоянно мигрирующие сегменты в глобальной сети (Deep-Web платформы), представляют собой платформы с наивысшим уровнем приоритета к их исследованию и получению актуальной, оперативно значимой информации.

Использование вышеуказанными лицами технологии VPN [11] регистрации в доменном имени .com в рамках сетевой инфраструктуры недружественных государств при организации незаконной деятельности снижает эффективность контроля, а именно: получение информации посредством запросов провайдером на предоставление сведений об искомом объекте (сетевой интерфейс,

его активность, домен и установочные данные лица при регистрации, и т.д.), определяет рудиментарность векторных ограничений (целевых, направленных на конкретное лицо) в отношении организаторов противоправной деятельности.

Копиями ранее заблокированных сайтов «на территории Российской Федерации» выступают зеркала интернет-ресурсов. При создании зеркала, владельцы сайта фактически меняют доменное имя, причем участники web-ресурса оперативно уведомляются об актуальной, вновь «поднятой» цифровой платформе. Оперативность миграции серверной части, отсутствие ограничений на количество зеркал определяет низкую эффективность противодействия данным ресурсам. Для блокировки такого ресурса, мигрировавшего на новое доменное имя, правоохранительным органам необходимо повторно формировать и реализовывать перечень процессуальных действий по результатам которого Роскомнадзор [12] проведет процедуру блокировки.

Примечание

Обращаясь к зарубежной практике, а именно к ужесточению ответственности за подобную противоправную деятельность, формируется основа к нейтрализации клиентской базы и, как следствие, снижению прибыли владельцев незаконных интернет-ресурсов. На сегодняшний день Китай контролирует деятельность зарубежных компаний в своем сегменте информационно-телекоммуникационных сетей. Однако данный путь имеет и обратную – негативную сторону, а именно цифровую изоляцию, что сомнительно в современном мире.

Рассмотрим еще один аспект заявленной темы, а именно транзакции в финансовой сфере. Данные операции реализуются через банки, сведения, обрабатываемые в банках, относятся к категории информации ограниченного доступа [13].

В случае если банки осуществляют свою деятельность на территории России и/или в рамках ее цифровой юрисдикции в соответствии с Федеральным законодательством обязанности на предоставление соответствующих сведений распространяются на все виды транзакций.

Примечание

В настоящее время предоставление правоохранительным органам, в частности субъектам оперативно-разыскной деятельности, сведений о транзакциях российских банков может составлять несколько месяцев, а запрос, направленный в адрес иностранного банка, может остаться без ответа. Таким образом, правоохранительные органы имеют возможность отследить только «национальную ветвь» всей транзакционной цепи. И если речь о криптовалюте, то предоставленные сведения будут отражать использование лишь «холодных криптокошельков»¹, – временных хранилищ, как правило ис-

¹ Cold Storage – холодное хранение, то есть криптокошелек, который не имеет постоянного подключения к сети Интернет. Подразумевает хранение валюты офлайн под защитой персонального ключа. К таковым относят, например, аппаратный криптокошелек, хранящийся на отдельном устройстве, внешне похожем на флеш-накопитель [Электронный ресурс]. – URL: <https://profinvestment.com/cold-hot-cryptocurrency-wallets/> (дата обращения: 19.09.2023).

пользуемых для одноразовой пересылки денежных средств или цифровых активов. Исходя из выше рассмотренных аспектов, напрашивается ряд решений в правовом плане: установить ограничение на взаимодействие отечественных и иностранных банков? На сегодняшний день, с учетом многоуровневых связей и форм взаимодействия, в частности в сфере экономики, реализовать инициативу по изоляции зарубежного банковского сегмента маловероятно.

Для совершенствования противодействия легализации (отмыванию) доходов [14] необходимо совершенствование нормативной правовой базы, в частности международной, регламентирующей формы взаимодействия. Приказом Генпрокуратуры России № 511, Росфинмониторинга № 244, МВД России № 541, ФСБ России № 433, ФТС России № 1313, СК России № 80 от 21 августа 2018 г. «Об утверждении Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем» государственных органов по контролю «межгосударственного, транснационального» закреплена межведомственная Инструкция по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем.

В рамках государственной политики совершенствования национальной «антиотмывочной» системы Федеральной службой по финансовому мониторингу реализован сбор и анализ информации, в частности о криптовалютных транзакциях. К вопросу эффективности – исключительно в рамках цифровой юрисдикции государства и дружественных стран. Имеют место лишь частные случаи установления владельца криптокошелька в случаях:

- самоличного отключения VPN и взаимодействие с к «контролируемым» правоохранительными органами сетевым оборудованием;
- многократного изменения сетевого интерфейса за единицу времени, признак использования VPN;
- произведение реверса анализируемой транзакции в обе стороны, с выявлением «миксеров»¹, после чего редукцией приведение в линейный вид, объединив все разветвления цифровых активов в блок, тем самым получив начальные и окончательные хеш-суммы транзакции конкретной криптовалюты.

Исследование технической природы анонимизации действий пользователя определяет наличие и/или использование следующих технологий: городской сетевой инфраструктуры – MAN; в рамках которой функционирует виртуальной сервер – VPS (Virtual Private Server) провайдера, сетевая инфраструктура и оборудование которого находятся в контролируемой государственными органами цифровой юрисдикцией; где «поднята и развернута» виртуальная частная сеть – VPN; посредством протокола сетевого уровня – NAT реализована процедура преобразования IP-адреса(ов) узла(ов) локальной сети – LAN (Local Area

¹ Сервис, который позволяет пользователям скрывать происхождение и назначение транзакций. Пользователи отправляют криптовалюту в сервис, смешивают эту криптовалюту с другими монетами или токенами, а затем отправляют эквивалентное количество «смешанных» монет на адрес получателя, скрывая связь между отправителем и получателем.

Network), беспроводной локальной сети – WLAN (Wireless Local Area Network) либо удаленного туннелируемого узла.

Анализ активности пользователей Сети позволят идентифицировать лицо и его активность на конкретном хосте (сетевом узле), в том числе окончечном.

Первым компонентом к изучению выступает технология проверки данных в сетевых пакетах – DPI (Deep Packet Inspection), предоставляющая возможности изучения накопленных статистических данных и его фильтрации. Провайдер как координатор «отслеживает» весь трафик, по всем уровням модели OSI (Open Systems Interconnection) обслуживаемых им хостов. Представляющий оперативный интерес «аномальный трафик», в соответствии с руководящей документацией и внутренними инструкциями, в целях эргономичности обращения к нему в сегменте базы данных и последующим его анализе записывается в отдельные «логи» (журналы событий).

В случаях если по исследуемому сетевому узлу будет установлен дата-центр, следует предположить использование VPN-сервера. При использовании на хосте технологии VPN (оборудование, выход в сеть которого реализован с контролируемой территории) – изменение IP-адреса, DNS, и т.д. следует воспользоваться утилитой IP lookup, посредством которой установить организацию, иерархию подсетей и диапазон обслуживаемых хостов.

Блокировка VPN-сервера при наличии достоверных идентифицирующих сведений с «наблюдением» за активностью IP-адреса (поиск и обращение по принципу процесса DORA (Discovery-Offer-Request-Acknowledge) в протоколе DHCP к иным, доступным для хоста VPN-серверам).

Блокировка провайдером «эталонных» портов VPN:

- 1194 (OpenVPN),
- UDP-порты 500 и 4500 (протокол IPSec & протокол IKEv2),
- 1701 (протокол L2TP).

Примечание

Важно отметить, порт 443 заблокировать при анализе активности не представится возможным, так как данный порт используется при передаче трафика по протоколу HTTPS (Hyper Text Transfer Protocol Secure) (предназначен для безопасной передачи данных в сети Интернет).

Нередко правонарушители используют механизм маскирование протокола OpenVPN на стек протоколов TCP/UDP в целях анонимизации и легализации трафика. Шифрование OpenVPN имеет отличительную подпись, отличительный маркер которой отслеживается посредством DPI. Функция VPN, позволяющая скрыть зашифрованный трафик OpenVPN, имитируя его в обычный интернет-трафик, именуется «обфускацией». Реализуется путем удаления связанных с VPN данных из пакета OpenVPN и назначения ему порта 443, изначально предназначенного для передачи трафика по протоколу HTTPS.

Анализ активности узла и установление протоколов передачи данных:

- IKEv2 (Internet Key Exchange Version 2),
- WireGuard, SSTP (Secure Socket Tunneling Protocol),
- PPTP (Point-to-Point Tunneling Protocol), выявление маркеров инкапсуляции сетевых пакетов GRE (Generic Routing Encapsulation).

Использование `pf` – (идентификации удаленных систем); анализ трафика позволяет установить:

- ОС (операционную систему);
- MTU (Maximum transmission unit – максимальный размер полезного блока данных одного пакета);
- используемый браузер.

Добавив экспорт MTU через API (Application Programming Interface) и обновив сигнатуры, появляется возможность установить пользователей VPN-протоколов, проху (сетевой «посредник» между узлами), а также выявить смену User-Agent (идентификатор браузера).

Далее рассмотрим механизм деанонимизации через преднамеренный вызов утечки VPN-трафика. Провайдер может вызвать подключение по протоколу IPv6 на исследуемом сетевом узле, отправляя поддельные ICMPv6 Router Advertisement сообщения. Подобные пакеты могут быть разосланы при помощи утилит: `rtadvd`, `THC-IPv6`, `SI6 Networks' IPv6 Toolkit` и др.

Важно отметить, что исследуемый узел должен поддерживать обе версии протокола IP: IPv4 и IPv6. Осуществляя рассылку Router Advertisement (сообщение, инициируемое маршрутизатором/роуэтром) сообщений, содержащих соответствующую RDNSS-опцию (рекурсивный DNS-сервер), провайдер имитирует локальный рекурсивный DNS-сервер, после чего производит DNS-спуфинг (переадресацию пользователей с запрошенного им ресурса на указанный инициатором) и изучает сетевой трафик объекта исследования.

В случае если IPv6 VPN-клиентом не поддерживается, реализуется отключение поддержки шестой версии протокола IP на всех сетевых интерфейсах. Таким образом, у приложений, запущенных на компьютере, не будет другого выбора, как использовать IPv4. Если же IPv6 поддерживается, то справедлива версия о том, что весь IPv6-трафик отправляется через VPN.

Требования к гибкости и масштабируемости компьютерных сетей определили государственным структурам приоритетную задачу по обеспечению безопасности элементов сети, в особенности распределенных высокопроизводительных кластеров обработки Больших Данных (BIG DATA) и интеграции технологий виртуализации для предоставления облачных сервисов (Cloud Bursting).

По нашему мнению, модель противодействия анонимизации действий правонарушителей в информационно-телекоммуникационной сети должна состоять из следующих элементов:

I. SDN (Software Defined Networking) – форма виртуализации вычислительных ресурсов с функцией удаленного программного-конфигурирования сети, выполняющей функции: разделения передачи трафика, его контроля и управления; определения единого интерфейса между устройствами управления и передачи данных, оптимизации контроля всех сетевых узлов в структуре сети; объединение управление узлами сети и применение соответствующих политик безопасности между Software Defined Networking («северный мост»); между физическими сетевыми устройствами («южный мост»).

Примечание

Информационный поток «северный мост» реализован на базе протокола REST API – работа с логическими компонентами.

Информационный поток «южный мост» реализован посредством протокола OpenFlow, обеспечивающий взаимодействие контроллера с сетевыми устройствами.

II. DPI (Deep Packet Inspection) – глубокий анализ трафика (пакетов); RDP (Remote Desktop Protocol) – протокол удаленного подключения.

Посредством DPI реализуется:

- контроль и управление аварийными событиями на устройствах;
- сбор логированной информации с устройств;
- опрос характеристик производительности устройств,
- представление информации по нагрузке компонентов ЭВМ.

Анализ эвристической модели исследуемого трафика/протоколов включает:

- структуру передаваемых данных;
- принадлежность передаваемого трафика/пакета к конкретному приложению;
- частоту открытия сессий;
- формат заголовков;
- размер пакета;
- номера портов;
- иную информацию, идентифицирующую исследуемый трафик.

DPI устанавливается на границе сети оператора/провайдера и наиболее эффективен при анализе трафика в симметричных сессиях. В случае же если трафик ассиметричен, нецелесообразно контролировать весь массив данных, анализировать следует лишь метаданные, явно характеризующие исследуемый трафик. Данная процедура может быть реализована при помощи инкапсуляции в broadcast-фреймы, с отправкой на DPI-устройства, находящиеся в едином домене. Далее посредством анализа метаданных исследуемого трафика в логах устанавливаются сессии с аналогичными данными, таким образом, возможно определить источник отправки пакетов данных и установить узлы в рамках национальной «цифровой юрисдикции».

III. AML (Anti-Money Laundering) – противодействие отмыванию денег, полученных преступным путем. В отношении DEX-источников (транзитных адресов, децентрализованных биржевых аккаунтов, зарегистрированных на «третьи» лица) включает в себя KYC (Know your Customer/Client) – принцип деятельности финансовых институтов (банков, бирж, криптобирж и т.п.), обязывающий их идентифицировать личность контрагента, прежде чем проводить финансовую операцию; KYT (Know your Transaction)¹ включает:

¹ KYT – это дополнение к уже известному процессу KYC, который требует от компаний проверки личности своих клиентов для предотвращения мошенничества и других незаконных действий. Основная цель KYT — предотвратить отмывание денег, финансирование терроризма и другие виды преступной деятельности путем обнаружения необычных или подозрительных моделей транзакций.

- историю поступлений на криптовалютный адрес;
- вероятность связи с незаконной деятельностью;
- особенности поведения пользователя;
- иную доступную информацию об адресе и его связях.

Примечание

Следует учитывать готовые программные решения, в рамках которых разработчиком-составителем алгоритмизируются, прописываются все условия в смарт-контрактах. Представляя собой программный код, не исключается наличие стегано- и крипто- контейнеров с дополнительными условиями, джиптр-ов в исполняемом коде, целью которых выступает включение заранее не-декларированных возможностей.

Библиографический список

1. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации // СПС «КонсультантПлюс».
2. ГОСТ Р 58210-2018/ISO/IEC TR 29181-1:2012. Национальный стандарт Российской Федерации. Информационные технологии сети будущего. Формулировка проблем и требования // СПС «КонсультантПлюс».
3. ГОСТ Р ИСО 14813-1-2011. Национальный стандарт Российской Федерации. Информационные технологии сети будущего. Формулировка проблем и требования. Интеллектуальные транспортные системы. Схема построения архитектуры интеллектуальных транспортных систем // СПС «КонсультантПлюс».
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс».
6. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СПС «КонсультантПлюс».
7. ГОСТ Р 53632-2009. Национальный стандарт Российской Федерации. Показатели качества услуг доступа в интернет / Термины и определения // СПС «КонсультантПлюс».
8. ГОСТ 33707-2016. Межгосударственный стандарт. Информационные технологии (ISO/IEC 2382:2015) // СПС «КонсультантПлюс».
9. ГОСТ Р 56045-2021/ISO/IEC TS 27008:2019. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Раздел 13 Безопасность коммуникаций. В.2 Оценка мер обеспечения информационной безопасностью 13.1 Менеджмент информационной безопасности сетей // СПС «КонсультантПлюс».
10. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

11. ГОСТ Р 53729-2009. Национальный стандарт Российской Федерации. Качество услуги «предоставление виртуальной частной сети (VPN)» // СПС «КонсультантПлюс».

12. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс».

13. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

14. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 7 августа 2001 г. № 115-ФЗ // СПС «КонсультантПлюс».

РОЛЬ РЕКЛАМНОГО И PR-ТЕКСТА КАК ФОРМЫ МАССОВОЙ КОММУНИКАЦИИ НА ПРИМЕРЕ КИНОИНДУСТРИИ

Григорусь Л.Н.,

Мамутов Э.Э.

(Краснодарский университет МВД России)

Аннотация: в данной статье поднята проблем использования PR-средств для продвижения в современном информационном обществе. Выявлены основные тенденции использования PR-текстов, определено место пресс-службы в этом процессе. Кроме того, выявлена эффективность массовой коммуникации на современном этапе, а также роль профессиональных журналистов для привлечения внимания к конкретному кинопроизводству. Кратко охарактеризованы PR-инструменты такого продвижения в киноиндустрии и определены наиболее эффективные из них.

Ключевые слова: PR-текст, реклама, киноиндустрия, журналистика, СМИ, информационное общество, коммуникационный процесс, PR-деятельность, связи с общественностью, продвижение, эффект «молвы», медиамероприятия, пресс-релиз, замалчивание информации, создание интриги.

THE ROLE OF ADVERTISING AND PR TEXT AS A FORM OF MASS COMMUNICATION ON THE EXAMPLE OF THE FILM INDUSTRY

Grigorius L.N.,

Mamutov E.E.

(Krasnodar University of the Ministry of the Interior of Russia)

Abstract: this article raises the problem of using PR tools for promotion in the modern information society. The main trends in the use of PR texts are revealed, the place of the press service in this process is determined. In addition, the effectiveness of mass communication at the present stage is revealed, as well as the role of professional journalists to attract attention to a particular film production. The PR tools of such promotion in the film industry are briefly described and the most effective of them are identified.

Keywords: PR-text, advertising, film industry, journalism, mass media, information society, communication process, PR-activity, public relations, promotion, the effect of «rumor», media events, press release, silencing information, creating intrigue.

Постановка проблемы. Развитие общества и его преобразование в информационное общество влечет за собой изменения во многих сферах человеческой жизни. Совместное использование инструментов рекламы и связей с общественностью имеет важное значение для повышения эффективности коммуникации. Сегодняшний рациональный потребитель остается равнодушным ко многим рекламным сообщениям. Поэтому при создании кампании по продвижению необходимо сочетать как PR, так и рекламные технологии, чтобы оказывать всестороннее и, прежде всего, эффективное воздействие на целевую аудиторию.

Цель исследования – исследовать роль рекламного и PR-текста как формы массовой коммуникации на примере киноиндустрии.

Изложение основного материала. Научно-технический прогресс, активное развитие средств массовой информации в к. XIX–XX вв. актуализировали такой феномен, как информационное и речевое воздействие. Увеличение технических возможностей, появление глобальной интернет-сети сделало возможными не только свободу высказывания, но и включение самых широких слоев населения в обсуждение насущных вопросов с возможностью высказать собственное мнение. Огромное разнообразие информации и ее источников приводит к тому, что воздействие на сознание человека все меньше и меньше поддается контролю и осознанию. Остро стоит в наши дни проблема информационного и речевого манипулирования сознанием. К сожалению, приходится констатировать, что критическое восприятие информации в современном обществе находится на крайне низком уровне.

Информационное общество можно определить как «общество, в котором информационные процессы осуществляются в основном на основе использова-

ния информационных технологий, а информационные ресурсы доступны для всех слоев населения». Согласно этой концепции деятельность большинства работающих людей в современном мире связана с производством, хранением, обработкой и распространением информации [2].

В условиях современного информационного общества структура взаимодействия субъекта и объекта информационного воздействия несколько усложнена, в связи с чем появляется необходимость получения актуальной информации и управления ею. Данный процесс способствует образованию специальных структур – пресс-служб, которые осуществляют PR-деятельность с целью правильного воздействия на аудиторию и донесения информации о компании, мероприятии или других объектах [4].

Инструменты по связям с общественностью (PR-инструменты) – это определенные средства и методы, используемые в связях с общественностью для достижения поставленных коммуникативных целей. Инструменты по связям с общественностью следует классифицировать по каналам связи: СМИ, события, Интернет и другие технические средства связи, личные контакты [3].

Люди больше не восприимчивы к прямым пропагандистским действиям, в связи с чем повышается социальная апатия. Становится очевидна необходимость использования связей с общественностью как способа ведения равноправного диалога. Однако процесс становления PR затрудняется из-за многих причин, имеющих объективную и субъективную природу. Главными причинами являются менталитет, социально-экономический застой, отсутствие четкой формулировки национальной идеи и политической стабильности развития России.

И все же, даже с такими трудностями, можно констатировать, что в России функционируют Public Relations как сфера профессиональной деятельности. При этом настоящие специалисты в данной сфере находятся в сложном положении. Они вынуждены работать в нелегких условиях, для того чтобы доказать социуму, что PR – это отрасль, имеющая право на существование. С помощью своей деятельности они хотят поменять сформированное годами отрицательное отношение к Public Relations среди населения, сложившееся по причине множества популярных и «черных» кампаний, так как в процессе пропагандистской деятельности использовались различные компрометирующие факты и незаконные политические технологии [1].

Рассмотрим данный процесс на примере отрасли киноиндустрии.

Инструменты связей с общественностью целесообразно классифицировать по каналам коммуникации: СМИ, события, Интернет и другие технические средства коммуникации, личные контакты. Несомненно, данные инструменты приобретают свои особенности, когда используются для продвижения. Так, например, специальные мероприятия, то есть мероприятия, проводимые для создания положительного имиджа и привлечения внимания общественности к компании, ее деятельности, продуктам и услугам, а в киноиндустрии – для привлечения внимания к конкретному кинопроизводству, могут включать: кинопремии и фестивали, презентации, социально значимые акции, пресс-конференции с актерами и с создателями фильмов, различные конкурсы, розыгрыши призов, кинофестивали, закрытые показы.

Кинопремии и кинофестивали являются эффективным средством продвижения кинопроизводства, поскольку одним из критериев, по которому зрители выбирают фильм для просмотра, является получение награды или номинация самого факта, указывающего на качество фильма, именно так профессионалы кинопроизводства отличают его от других. Чтобы оказать положительное влияние на участие любого кинопроекта в фестивале, необходимо:

- 1) соответствие продвигаемого кино уровню фестиваля;
- 2) доверие зрителей к кинофестивалю [5].

Кроме того, фестивали как мероприятия носят не только прямой, но и косвенный характер: если фильм покори́л жюри или каким-либо образом возбудил общественное мнение, в дальнейшем он будет рассмотрен и описан в печатных изданиях и других средствах массовой информации.

Другим видом деятельности кинофестивалей являются показы фильмов, которые имеют потенциал для связей с общественностью, особенно в профессиональной среде, а также кинорынки – бизнес-ярмарки и ярмарки, темой которых является презентация, покупка и продажа кинопродукции.

Еще одним важным средством продвижения является премьера кинопроекта, специального мероприятия, на котором впервые демонстрируется созданный кинопродукт избранной целевой аудитории. Благодаря широкому освещению премьеры в прессе эти мероприятия значительно повышают интерес публики и напрямую увеличивают количество зрителей. Кроме того, премьерные показы провоцируют эффект «молвы», которая также является чрезвычайно эффективным средством пиар-продвижения. Но стоит отметить, что сегодня такой вид финансирования, как премьера фильма, используется не всегда. Например, когда фильм не имеет большого художественного замысла или когда нет времени на подготовку качественного мероприятия, его не используют, чтобы избежать противоположного негативного воздействия на общественное мнение [3].

Другим важным инструментом PR-продвижения являются так называемые медиамероприятия, которые могут быть всех видов, используемых в других сферах бизнеса: от пресс-конференций, презентаций фильмов и личных встреч до пресс-туров, которые могут проводиться в рамках поездки в места для журналистов, эффект от которых достигается за счет приглашения любителям кино.

Несомненно, наиболее важной частью продвижения является грамотное составление PR-текстов и последующее их распространение в СМИ путем прямой или личной передачи, поскольку для успешной рекламы фильма необходимо постоянно находиться в информационном поле, и желательно в позитивном ключе. Например, при продвижении кинопродукции используются различные традиционные PR-тексты: пресс-релиз, рекламный ролик, различные развлекательные, иллюстративные или авторские статьи, например от имени известного представителя коллективной группы, интервью с создателями фильмов или, наоборот, с критиками; биографии вовлеченных лиц и т.д. Кроме того, важной частью является продуманное написание аннотаций к фильмам, кото-

рые могут быть составной частью PR-текста или отдельным элементом, а также рекламой [5].

При составлении аннотации необходимо исходить из особенностей восприятия целевой аудиторией, а также технических характеристик фильма. Создавая анонс, необходимо заинтересовать зрителя, но не раскрыть интригу фильма.

В настоящее время вышеупомянутые PR-средства используются для большинства фильмов, поэтому становится важным выделиться на их фоне, чего можно достичь не только за счет творческой реализации каждого из них, но и за счет специальных PR-акций, которые не только «пробуждают» публику, но и обладают вирусным потенциалом.

В качестве примера можно привести успешную пиар-акцию фильма «Кредо. Наследие Рокки», когда пропагандировался не только фильм, но и здоровый образ жизни: пассажиры лондонского метро, поднимавшиеся по эскалатору пешком, были встречены на верхнем этаже группой веселых спортсменов и настоящим оркестром, исполнявшим музыкальную тему из фильма «Рокки». Эта акция не только оказала влияние на непосредственных участников мероприятия, но и позже получила широкое распространение в Интернете [6].

Таким образом, одним из основных элементов PR-продвижения является создание информационных площадок, которые постоянно поддерживали бы интерес к кинопроизводству. Прямая реклама может надоесть и невольно вызывать обратный, негативный эффект, а причины, привнесенные в информационную среду, воспринимаются как должное, как нечто интересное и увлекательное, чем можно поделиться с друзьями, проявив свою эрудицию.

Необходимо постоянно быть в курсе производства фильма, а также любых изменений информационного фона, которые могут быть так или иначе связаны с фильмом. Это могут быть: переделка фильма, личная жизнь актеров, события на сцене, праздники и другие события, связанные с темой фильма, и многое другое, что сопровождает кинопроект.

Стоит отметить, что информация может быть не только получена извне, но и быть источником – контекстная среда фильма может быть создана или расширена путем размещения в СМИ информационных тем, которые могут не касаться непосредственно самого кинотеатра.

Причем информационной причиной ее отсутствия может быть намеренное замалчивание информации, создание интриги и ауры мистики вокруг кинопроекта. Это ясно показывает, что в продвижении кинопроизводства важно выходить за рамки кино, фильм должен быть не просто произведением искусства, а событием, дискуссии и споры о котором начнутся еще до выхода на экраны и не прекратятся после выхода в прокат.

Реклама в прессе должна публиковаться в профессиональных изданиях, а также в тех, которые направлены на информирование общественности о возможных развлекательных мероприятиях, поскольку люди получают к ней прямой доступ, чтобы найти приемлемый способ передачи. Кроме того, эффективно инициировать публикации в прессе, в которых заинтересована приоритетная рабочая группа, часто во многих журналах и газетах, которые даже не затраги-

вают тематику досуга или кино, есть разделы, посвященные досугу, искусству и культуре, а также публиковать рекламу напрямую в таких же изданиях. Для повышения эффективности целесообразно использовать фотоматериалы со съемочной площадки, фотографии звезд, участвующих в проекте, плакаты и видеоматериалы.

В заключение стоит упомянуть рекламную мудрость: нет ничего более опасного для плохого продукта, чем хорошая реклама. Решение об использовании определенных инструментов должно быть взвешенным и основываться на результатах тщательной исследовательской работы. PR-сопровождение – это совокупность методов, направленных на установление, поддержание связей с общественностью за счет многократной реализации действий по улучшению взаимоотношений между организацией, индивидуумом и общественностью. Массовая коммуникация является основной средой, в которой функционируют институты PR, которые призваны влиять на общественность прежде всего через каналы коммуникации и с помощью СМИ. Специалисты публичных рилейшнз фактически являются посредниками между организацией и различными группами общественности, с которыми она имеет дело. Они призваны распространять информацию, которая позволяет заинтересованным группам населения осознать политику и деятельность организации.

Библиографический список

1. Дмитриева О.С. Разработка стратегии продвижения кинокартины // Альманах современной науки и образования. 2012. № 6. С. 38–42.
2. Душкина М.Р. PR и продвижение в маркетинге: коммуникации и воздействие, технологии и психология: учебное пособие по специальности «Связи с общественностью». – Санкт-Петербург: Питер, 2010. – 506 с.
3. Кокарев И.Е. Кино как бизнес и политика: современная киноиндустрия США и России: учебное пособие. – 2-е изд., перераб. – Москва: Аспект Пресс, 2009. – 342 с.
4. Кривоносов А.Д. Основы теории связей с общественностью: учебник для студентов вузов, обучающихся по направлению подготовки (специальности) «Связи с общественностью» / А.Д. Кривоносов, О.Г. Филатова, М.А. Шишкина [и др.]. – Санкт-Петербург: Питер, 2012. – 375 с.
5. Михалева Е.П. Маркетинг: конспект лекций. – Москва: Высшее образование, 2008. – 222 с.
6. Ромат Е.В. Реклама. Краткий курс. – 2-е изд. – Санкт-Петербург: Питер, 2008. – 506 с.
7. Сидоренко В.И., Огурчиков П.К. Профессия – продюсер кино и телевидения. Практические подходы: учебник. – Москва: Юнити-Дана, 2010. – 712 с.

ОСОБЕННОСТИ КЛАССИФИКАЦИИ КИБЕРПРЕСТУПЛЕНИЙ

Дрога А.А.,
Горковенко В.С.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: на современном этапе развития наше государство выходит на путь постиндустриального общества, все чаще цифровое право охватывает отрасли российского права, а информационное пространство – все сферы деятельности российского общества. Но при развитии информационной среды появляются все новые возможности по злоупотреблению IT-технологиями в целях совершения новых видов преступлений, направленных против информационных ресурсов. Киберпреступления в настоящее время вышли на новый уровень, что обуславливает необходимость усиления борьбы с ними, а следовательно, и решения проблемы их классификации.

Ключевые слова: киберпреступление, научно-технический прогресс, интернет-мошенничество, информационная безопасность.

FEATURES OF THE CLASSIFICATION OF CYBERCRIMES

Droga A.A.,
Gorkovenko V.S.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: at the present stage of development, our state is entering the path of a post-industrial society; increasingly, digital law covers branches of Russian law, and the information space covers all spheres of activity of Russian society. But with the development of the information environment, new opportunities arise for the abuse of IT technologies in order to commit new types of crimes directed against information resources. Cybercrimes have now reached a new level, which necessitates the need to intensify the fight against them, and, consequently, to solve the problem of their classification.

Keywords: cybercrime, scientific and technological progress, Internet fraud, information security.

В настоящее время с развитием научно-технического прогресса развивается и техника, которая активно внедряется в человеческую жизнь. Недавние изобретения ввели в обиход такие понятия, как «гаджет», «девайс», «онлайн», «биткоин» даже в дипломатических и государственных актах, а также выступлениях должностных лиц. Современные угрозы также эволюционируют наравне с техническим развитием. Сегодня никого не удивляют интернет-мошенничества, кибер-вымогательства, хищения средств с использованием информационных данных (пластиковых карт, онлайн-банкинга и т.д.). Но современ-

менное государство не стоит на месте, оно находится в постоянном развитии, это касается и правоохранительных органов. Наряду с появлением новых преступлений появляются новые методы борьбы с ними. Применение различных роботизированных машин и научных технологий помогает эффективно находить пути решения по борьбе с преступностью.

Сейчас цифровые технологии развиваются совместно с преступлениями в сфере цифровой информации, именуемые «компьютерные преступления», «преступление в сфере IT-технологий», «киберпреступления». Несмотря на то, что у данных преступлений есть огромное число названий, определения таким преступлениям в юридической литературе и законодательстве не содержится. Информационные технологии приобретают все большее значение в нашем обществе. В связи с тем, что современное общество становится все более информационным, растет и количество преступлений, совершаемых в данной среде, их также называют киберпреступлениями. В данном разделе мы рассмотрим понятия «киберпреступность», «киберпреступления» и «компьютерные преступления», чтобы понять сущность рассматриваемых нами преступлений в сфере информационных технологий.

Стоит отметить, что с развитием преступлений в рассматриваемой сфере также развиваются и способы их раскрытия: органами внутренних дел применяются новые технологии, программы и другие средства и методы борьбы. Помимо этого, проводится подготовка и переподготовка кадров, целью которой является обеспечение сотрудников необходимыми знаниями для борьбы с преступлениями информационной направленности. Но нельзя сказать, что инновационные технологии органов внутренних дел и киберпреступления развиваются одинаково, и так как обеспечить должное финансирование пока не представляется возможным, то это является огромной проблемой в настоящее время. А что касается киберпреступлений, то на данном этапе развития не только нашей страны, но других государств следует усилить борьбу с преступлениями информационной направленности, также необходимо предпринимать новые меры по устранению и профилактике данных преступлений.

Как отмечает в своей работе М.Е. Батухтин, «киберпреступление – это любое преступление в электронной сфере, совершенное при помощи компьютерных средств или виртуальной сети или против них» [1, с. 79]. Киберпреступность является следствием глобализации информационных процессов, которые происходят в обществе. Чем больше общество использует информационные технологии, изучая новинки, которые предлагает информационное сообщество, тем больше появляется лиц, которые находят пути и методы совершения информационных преступлений. Так, на данном этапе развития используются электронные деньги, кошельки, персональная информация хранится также в электронном варианте, совершаются различные сделки через информационное пространство. Это дает преступникам возможность для совершения преступлений в нем. На данном этапе развития государства совершаются такие преступления, как хищение биткоинов, хищение предметов из игр (например, танков в игре World of Tanks), дистанционные мошенничества и другие преступления, которые связаны с информационными технологиями.

Стоит сказать, что преступления, направленные против информационных ресурсов, и всеобщая цифровизация общества способствуют разработкам государства в области как противодействия данным преступлениям, так и выработке мер по пресечению и раскрытию преступлений информационной направленности.

Несмотря на то что проблема преступлений в сфере информационных технологий активно обсуждается, существует множество дискуссий по проблемным вопросам в данной сфере, использование информационно-телекоммуникационных технологий при совершении преступных деяний в настоящий период остается серьезным вызовом для правоохранительных и законодательных органов [2, с. 15].

Как нами уже было отмечено, существует множество трактовок по определению преступлений в сфере компьютерной информации, но также дискуссионные вопросы возникают и при определении их признаков, поэтому считаем целесообразным рассмотреть различные мнения ученых.

Так, по мнению М.В. Ульянова, существуют следующие признаки: «преступления носят латентный характер, то есть практически скрыты на первый взгляд от людей, и факт преступного события обнаруживается только в тот момент, когда сверяются бумажные документы и компьютерная информация; чаще всего преступления данной направленности совершаются дистанционно, то есть мошенник может находиться на значительном удалении от объекта преступного посягательства». Помимо этого, он характеризует киберпреступления как «предусмотренное уголовным законом виновно совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации [3, с. 34]».

Классификация преступлений в сфере информационных ресурсов различными авторами характеризуется по-разному, но, по нашему мнению, преступные деяния данного характера уже классифицировал законодатель в Уголовном кодексе Российской Федерации (далее – УК РФ). В данном документе предусмотрена отдельная глава 28, содержащая характеристику преступлений в сфере компьютерной информации: неправомерный доступ к компьютерной информации (ст. 272); создание, распространение и использование вредоносных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1). Это далеко не полный перечень преступлений, которые могут совершаться в сфере информационных технологий.

Киберпреступность – это преступность, которая развивается при помощи компьютерных технологий (систем), сети Интернет и других устройств. Необходимо сказать, что у киберпреступности существует множество интерпретаций, некоторые из них нами уже были рассмотрены.

По нашему мнению, необходимо выделить классификацию, которая будет более точно определять виды поступлений, направленных против информационных ресурсов:

1. Неправомерный доступ к компьютерной информации. Считаем необходимым привести пример судебной практики. Так, гражданин Д., являвшийся сотрудником ПАО «Вымпелком» и, обладая специальными знаниями в области программирования, использовав персональные данные клиентов данной компании, из корыстных побуждений подделал заявление клиента и, использовав лицевой счет абонента Ф., совершил хищение денег в сумме 32 414,83 рублей, принадлежащих ПАО «Вымпелком». Суд признал виновным Д. в совершении преступления, предусмотренного пп. «б», «в» ч. 3 ст. 272 УК РФ.

2. Создание, распространение и использование вредоносных программ. Так, гражданин К. применил вредоносную компьютерную программу не менее чем к 51 000 IP-адресам, принадлежащим различным физическим и юридическим лицам. К. был признан судом виновным в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Считаем необходимым определить, что подразумевается под понятием «критическая информационная инфраструктура». В Федеральном Законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4, с. 46] описываются «объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». Под объектами в данном случае понимаются: «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры».

5. Мошенничество в сфере компьютерной информации. Считаем необходимым рассмотреть практический пример: Гражданин М., выполняя служебные обязанности в помещении офиса ПАО «...» и имея доступ к служебной компьютерной информации, незаконно переоформил абонентские номера и продал их от лица компании ПАО «...» лицам, не осведомленным о его преступных намерениях, тем самым причинив ущерб в крупном размере на общую сумму 561 000 руб., но его преступные действия не дошли до своего логического завершения из-за определенных обстоятельств. М. был признан судом виновным в совершении преступления, предусмотренного ч. 3 ст. 30, п. «б» ч. 3 ст. 159.6 УК РФ [5, с. 72].

6. Мошенничество с использованием электронных средств. Целесообразно будет включить этот состав в перечень преступлений в сфере информации, так как данные преступления направлены на завладение персональными данными лица, использующего электронные средства платежа, а также действия данной нормы распространяются на хищения, совершаемые с использованием удаленного доступа к банковскому счету, электронному кошельку при помощи технических средств. Так, Гражданин З. тайно похитил банковскую карту ПАО «Сбербанк России», выпущенную на имя Е., и в рамках единого преступного

умысла провел операции по оплате товаров с использованием электронных средств платежа. Суд признал виновным З. в совершении преступлений, предусмотренных ч. 2 ст. 159.3, ч. 2 ст. 159 УК РФ [6, с. 18].

7. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. Стоит отметить, что данный вид правонарушений обязателен для включения в перечень преступлений в сфере информации, так как использование средств, предназначенных для негласного получения информации, могут позволить получить сведения о персональных данных, нарушить тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Так, гражданин Б., не имея лицензии, подтверждающей право осуществления разработки, производства, реализации, в целях продажи специальных технических средств, предназначенных для негласного получения информации, выдаваемой органами ФСБ России, при этом обладая навыками по разработке и производству специальных технических средств, предназначенных для негласного получения информации: негласного проникновения и обследования помещений, транспортных средств и других объектов, в целях извлечения прибыли, умышленно, разместил в сети Интернет на сайте (обезличено) объявление об оказании услуг по продаже «код-грабберов», для проверки автомобильных сигнализаций на устойчивость к взлому работникам СТО страховых компаний, в котором указал номер телефона (обезличено). Суд признал виновным гражданина Б. в совершении преступления, предусмотренного ст. 138.1 УК РФ [7, с. 25].

8. Приобретение или сбыт имущества, заведомо добытого преступным путем. Следует обратить внимание, что нередко цифровая информация приравнивается к имуществу и, отмечая, что хоть цифровая информация является невещественной, в качестве носителя информации выступает вещественный предмет (флеш-карта), содержащий цифровую информацию и представляющий материальную ценность.

Помимо выделенных классификаций, по нашему мнению, необходимо добавить пункт «г», части 3 статьи 158 УК РФ, которая предусматривает хищение денежных средств с банковского счета. Данный состав весьма сложно разграничить со статьей 159.3 УК РФ, и в практической деятельности сотрудников предварительного следствия нередко возникают вопросы по квалификации. Поэтому постановление Пленума Верховного суда Российской Федерации № 48 четко разграничило данные составы преступных деяний. Приведем пример по данной статье: лицо, находясь в неустановленном месте, действуя из корыстных побуждений, путем обмана завладело денежными средствами в размере 169 032 рублей 00 копеек, принадлежащими гражданину Ф., при следующих обстоятельствах: так, «дата» 2021 года в период времени с 10 часов 19 минут по 13 часов 14 минут гражданину М., находившемуся на территории участка реконструкции АО «...», расположенного по адресу: «...», на его абонентский номер (данные изъяты) поступил телефонный звонок от абонента (данные изъяты), который представился сотрудником финансовой безопасности ВТБ-банка, в ходе разговора М. назвал номер своей банковской карты (данные изъяты) и код «...», который поступил посредством смс-сообщения от ВТБ. Далее граж-

данин М. назвал номер банковской карты, принадлежащий ПАО «Сбербанк», а также назвал срок действия карты и CVV-код. После чего со счета ПАО «ВТБ», который принадлежит гражданину Ф, на счет Homecreditbank, принадлежащий А., произошло списание денежных средств в сумме 75 000 рублей 00 копеек и с комиссией 4 125 рублей 00 копеек. Также с карты ПАО «Сбербанк», которая принадлежит гражданину М., произошли следующие транзакции: 15 000 рублей PAY.MTS.RU; 15 000 рублей PAY.MTS.RU; 15 000 рублей Tele2 TOPUP; 14 965 рублей OPLATAURALSIB, 14 948 рублей T2 MOBILE (WALLET), 14 994 рублей YMMTS.

Также, стоит отметить, что киберпреступления можно разделить на следующие виды: кардинг, крекинг, спаминг, фишинг, фарминг, нюкинг, хакинг (кракеры – программные защиты от серийных номеров до аппаратных ключей, фризеры – телефония, сетевые хакеры – глобальные и локальные сети). Исходя из этого, отметим, что классификаций преступлений по рассматриваемой направленности бесчисленное множество, но нами представлены традиционные классификации преступлений, которые чаще всего совершаются в настоящее время.

Преступления, направленные против информационных ресурсов, также объединены общими признаками:

1. Латентный характер преступлений. Это означает, что о большинстве преступлений неизвестно органам внутренних дел, так как о них не поступали заявления.

2. Дистанционный характер преступлений, когда преступления совершаются удаленно по отношению к объекту преступного посягательства.

3. Трансграничный характер преступлений, которые являются весьма опасными для общества, так как наносят огромный финансовый ущерб гражданам и организациям, а также государству при минимальном риске для преступника.

4. Связь преступлений с организованной преступностью.

5. Автоматизация преступных деяний.

6. Анонимность деяний.

7. Сложность раскрываемости данного вида преступлений (низкий процент раскрываемости).

8. Взаимодействие различных преступных сообществ.

9. Высокие доходы от преступной деятельности.

Обобщая вышесказанное, можно прийти к выводу, что к преступлениям в сфере информации стоит отнести те преступные деяния, где компьютер, информационно-телекоммуникационные технологии или сети выступают предметом, средством или орудием преступления.

Библиографический список

1. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юрист-Правоведъ. Уголовное право и криминология. 2019. № 4 (19). С. 78–82.

2. Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. – Казань, 2017. – 243 с.
3. Ульянов М.В. Преступления в сфере цифровой информации: понятие и виды // Электронный научный журнал Байкальского государственного университета. 2019. Т. 10. № 3.
4. Мустакимов Р.М. Проблемы расследования преступлений в сфере информационной безопасности // Вестник Белгородского юридического института МВД России. 2020. № 3. С. 44–48.
5. Рудых А.А. О некоторых направлениях цифровизации расследования преступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. С. 70–79.
6. Хлус А.М. Проблема методического обеспечения противодействия киберпреступлениям // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 2 (14). С. 15–20.
7. Хомяков Э.Г. О некоторых проблемах в учете и расследовании преступлений с использованием компьютерных и телекоммуникационных технологий // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 2 (14). С. 21–27.
8. Обзор информационной безопасности за период с 25 февраля по 2 марта 2022 года // SecurityLab.ru [Электронный ресурс]. – URL: <https://www.securitylab.ru/news/530398.php> (дата обращения: 10.05.2022).

РАСКРЫТИЕ И РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

**Дрога А.А.,
Хоробрая А.В.**

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье освещаются важные аспекты, касающиеся изучения современных информационно-телекоммуникационных технологий, ставшие неотъемлемой частью нашей жизни, и с помощью которых могут совершаться преступления. Сложность данной темы заключается в том, что раскрытие и расследование преступлений, связанных с использованием информационно-телекоммуникационных технологий, являются сложной задачей, требующей высокой квалификации и специализированных знаний. Они могут включать в себя изучение множества цифровых доказательств, таких как данные, обнаруженные на компьютерах, телефонах и других устройствах, а также данные, переданные через Интернет и другие электронные каналы связи. В работе представлен материал по вопросам эффективного раскрытия и рас-

следования преступлений, связанных с информационно-телекоммуникационными технологиями, который показывает, что необходимо иметь хорошее понимание принципов работы компьютеров и сетей, а также знать основы криптографии и стеганографии.

Ключевые слова: информационно-телекоммуникационных технологий (ИТТ), интернет, кибератаки, кибершпионаж, мошенничество, Darknet, блокчейн.

DISCLOSURE AND INVESTIGATION OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

**Droga A.A.,
Horobraya A.V.**

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article highlights important aspects concerning the study of modern information and telecommunication technologies (ITT), which have become an integral part of our lives and with which crimes can be committed. The complexity of this topic lies in the fact that the disclosure and investigation of crimes related to the use of OT is a complex task that requires high qualifications and specialized knowledge. They may include examining a variety of digital evidence, such as data found on computers, phones and other devices, as well as data transmitted over the Internet and other electronic communication channels. The paper presents material that pays attention to the issues of effective disclosure and investigation of crimes related to ITT, which shows that it is necessary to have a good understanding of the principles of computers and networks, as well as to know the basics of cryptography and steganography.

Keywords: information and telecommunication technologies (ITT), Internet, cyberattacks, cyberespionage, fraud, Darknet, blockchain.

В современном мире информационно-телекоммуникационные технологии (далее – ИТТ) стали неотъемлемой частью повседневной жизни. Интернет, сотовая связь, социальные сети и другие формы связи объединяют людей на разных континентах и способствуют развитию общества. Однако прогресс в этой области также сопровождается ростом преступности, связанной с использованием этих технологий. В данной статье рассмотрены проблемы, связанные с раскрытием и расследованием преступлений, совершаемых с использованием ИТТ, а также возможные пути их решения.

Для того чтобы определить круг проблем, связанных с преступлениями в сфере компьютерной информации, стоит исследовать их категории, которые подробно рассматриваются в главе 28 Уголовного кодекса Российской Федерации (далее – УК РФ) [1]. Данная глава к рассматриваемой группе преступлений относит: неправомерный доступ к информационному ресурсу, создание, использование и распространение вредоносных компьютерных программ, нару-

шения в области хранения, передачи и обработки информационных потоков, незаконные действия с целью причинения вреда критической информационной системе и структуре Российской Федерации.

Основные виды преступлений, совершаемых с использованием ИТТ.

1. *Кибератаки.* Кибератаки представляют собой акты нарушения конфиденциальности, целостности или доступности информационных систем и сетей. Эти атаки могут быть направлены на государственные структуры, предприятия, организации или отдельных пользователей. Кибератаки включают в себя такие виды преступлений, как хакерство, распространение вредоносного ПО, атаки типа «дос» и другие.

2. *Кибершпионаж.* Кибершпионаж – это незаконное проникновение в информационные системы с целью получения доступа к секретной, коммерческой или личной информации. Целью кибершпионажа может быть сбор данных для использования в политических, экономических или военных целях.

3. *Мошенничество.* Мошенничество с использованием ИТТ может принимать различные формы. Например, фишинг [4] – это вид мошенничества, при котором злоумышленники, выдающие себя за представителей банков или других учреждений, пытаются получить доступ к личным данным и финансовой информации пользователей. Также существует множество других схем мошенничества, включая онлайн-аукционы, лотереи, инвестиционные схемы и т. д.

4. *Распространение незаконного контента.* Злоумышленники используют ИТТ для распространения незаконного контента, такого как детская порнография, экстремистский материал, пиратские копии фильмов и программного обеспечения. Подобные действия нарушают авторские права и уголовное законодательство, а также могут способствовать преступной деятельности и насилию.

5. *Сетевые анонимные преступные сообщества.* В Сети существуют анонимные преступные сообщества, где злоумышленники могут обмениваться опытом, техниками, инструментами и ресурсами для совершения преступлений с использованием ИТТ. К таким сообществам относятся, например, теневые форумы и площадки на торговых площадках в «темной сети» (Darknet) [5].

Проблемы раскрытия и расследования преступлений, совершаемых с использованием ИТТ.

1. *Анонимность и использование сетей-анонимайзеров.* Одной из основных проблем в раскрытии и расследовании преступлений, совершаемых с использованием ИТТ, является анонимность злоумышленников. Преступники могут использовать сети-анонимайзеры (например, Tor), VPN-сервисы, прокси-серверы и другие средства для скрытия своего истинного местоположения и идентификационных данных.

2. *Международный характер преступлений.* Преступления с использованием ИТТ часто имеют международный характер. Злоумышленники могут находиться в одной стране, а их жертвы – в другой. Это создает сложности в расследовании таких преступлений, так как потребуется сотрудничество между различными странами и их правоохранительными органами.

3. *Недостаток квалифицированных специалистов.* Раскрытие и расследование преступлений, совершаемых с использованием ИТТ, требует высокой

квалификации и специализированных знаний в области информационных технологий и кибербезопасности. Однако многие правоохранительные органы сталкиваются с недостатком таких специалистов, что затрудняет их работу по борьбе с этим видом преступности.

4. Быстрое развитие технологий. ИТТ развиваются с быстротой, которую сложно предугадать и контролировать. Это означает, что злоумышленники могут опережать правоохранительные органы в использовании новых технологий и методов для совершения преступлений. Также возникает необходимость постоянного обновления знаний и навыков специалистов в области кибербезопасности.

Возможные пути решения проблем в раскрытии и расследовании преступлений, совершаемых с использованием ИТТ.

1. Международное сотрудничество. Для успешного раскрытия и расследования преступлений, совершаемых с использованием ИТТ, необходимо активное международное сотрудничество. Странам следует сотрудничать в обмене информацией, уголовном преследовании и выдаче преступников. Также важно принимать международные соглашения и конвенции, которые облегчат сотрудничество между разными странами.

2. Обучение и подготовка специалистов. Правоохранительным органам необходимо вкладывать ресурсы в подготовку квалифицированных специалистов в области кибербезопасности и расследования преступлений, связанных с использованием ИТТ. Это включает проведение специализированных курсов, семинаров и тренингов для сотрудников, а также сотрудничество с университетами и научно-исследовательскими центрами.

3. Применение новых технологий. Правоохранительные органы должны активно использовать новые технологии для обнаружения и расследования преступлений, совершаемых с использованием ИТТ. Например, применение искусственного интеллекта и анализа больших данных может помочь в выявлении нестандартного поведения, анализе цифровых следов и построении профилей злоумышленников. Также могут использоваться технологии блокчейн (выстроенная по определенным правилам непрерывная последовательная цепочка блоков, содержащих информацию [2]) для создания более безопасных и прозрачных систем обмена данными.

4. Развитие законодательства. Для успешной борьбы с преступлениями, совершаемыми с использованием ИТТ, необходимо постоянное развитие законодательства. Законы должны быть актуализированы и адаптированы к быстро меняющимся технологическим реалиям. Также важно учесть международный опыт и лучшие практики в области кибербезопасности и борьбы с преступностью.

5. Профилактика и информирование общественности. Проведение профилактических мероприятий и информирование общественности о рисках, связанных с преступлениями, совершаемыми с использованием ИТТ, является одним из ключевых аспектов в борьбе с этим видом преступности. Правоохранительные органы и образовательные учреждения должны проводить мероприятия, направленные на повышение информированности населения о методах

мошенничества, способах защиты от кибератак и других аспектах кибербезопасности.

Преступления, совершаемые с использованием информационно-телекоммуникационных технологий, представляют серьезную угрозу современному обществу. Раскрытие и расследование таких преступлений требует комплексного подхода, включая международное сотрудничество, обучение специалистов, использование новых технологий, развитие законодательства и проведение профилактических мероприятий. Только скоординированные действия государств, правоохранительных органов, экспертов и общественности позволяют эффективно справляться с этой угрозой и обеспечивать безопасность информационного пространства.

В заключение необходимо отметить, что раскрытие и расследование преступлений, связанных с ИТТ, является сложным процессом, который требует специальных знаний и навыков. Однако современные методы и технологии помогают правоохранительным органам более эффективно бороться с этими видами преступлений и обеспечивать безопасность в цифровой среде.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (принят Государственной Думой 24 мая 1996 года) (одобрен Советом Федерации 5 июня 1996 года) // СПС «КонсультантПлюс» (дата обращения: 27.03.2023).
2. Блокчейн. Википедия. Свободная энциклопедия [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/Блокчейн> (дата обращения: 27.03.2023).
3. Фишинг [Электронный ресурс]: Википедия. Свободная энциклопедия [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/Фишинг> (дата обращения: 27.03.2023).
4. DarkNet, Deep Web: что это такое, в чем разница и законно ли подключаться к скрытому интернету [Электронный ресурс] – URL: https://dzen.ru/a/W08YIkauFQCpN5u_ (дата обращения: 27.03.2023).

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОБУЧАЮЩИЕ СИСТЕМЫ В ОБРАЗОВАНИИ

Дубинина Н.М.,

кандидат юридических наук, доцент;

Войтухова А.А.

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: современные реалии диктуют необходимость формирования новых подходов в совершенствовании образовательного процесса в нашей стране на основе внедрения новых информационных и телекоммуникационных технологий. Одно из динамично развивающихся направлений в этой сфере – использование искусственного интеллекта в обучении. В статье рассматриваются особенности применения искусственного интеллекта и обучающих систем в повышении качества образовательного процесса.

Ключевые слова: образование, образовательный процесс, искусственный интеллект, обучающие системы, регулирование.

ARTIFICIAL INTELLIGENCE AND LEARNING SYSTEMS IN EDUCATION

Dubinina N.M.,

Candidate of Law, Associate Professor;

Voitukhova A.A.

(Kikot Moscow University the Ministry of Internal Affairs of Russia)

Abstract: modern realities dictate the need to form new approaches to improve the educational process in our country based on the introduction of new information and telecommunication technologies. One of the dynamically developing areas in this area is the use of artificial intelligence in education. The article discusses the features of the use of artificial intelligence and learning systems in improving the quality of the educational process.

Keywords: education, educational process, artificial intelligence, learning systems, regulation.

В настоящее время повышение качества образования выступает одной из приоритетных задач развития нашего общества. В этой связи пристального внимания заслуживают исследование и обсуждение теоретических и практических вопросов внедрения современных информационных и телекоммуникационных технологий для повышения эффективности образовательного процесса. Одно из динамично развивающихся направлений в этой сфере – использование искусственного интеллекта (далее – ИИ) и обучающих систем. Здесь следует отметить, что многие вопросы внедрения технологических решений в сфере

образования, разрабатываемых на основе искусственного интеллекта, требуют своего научного и прикладного осмысления. К актуальным вопросам можно отнести:

- содержательное осмысление внедрения ИИ и его преимуществ в образовательный процесс;
- правовую регламентацию использования ИИ в образовании;
- распространение преимуществ ИИ на всех участников образовательного процесса (обучающихся, профессорско-преподавательский и руководящий состав учебных заведений, родителей, администраторов и провайдеров);
- использование современных информационных и телекоммуникационных технологий в сборе и анализе данных об учебном процессе;
- использование современных информационных и телекоммуникационных технологий в разработке и применении компьютерных систем в обучении.

Вопросам правовой регламентации искусственного интеллекта уделяется достаточно большое внимание как в международном праве, так и в действующем законодательстве Российской Федерации. В п. 2 ст. 2 Федерального закона от 24.04.2020 № 123-ФЗ, «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» определено, что «искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру (в том числе информационные системы, информационно-телекоммуникационные сети, иные технические средства обработки информации), программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений» [1].

В последние годы с развитием новых методов и оборудования нейронных сетей искусственный интеллект нередко воспринимается как синоним «глубокого машинного обучения с учителем» (deep supervised machine learning) [2]. В целом можно выделить следующие основные направления использования ИИ в образовании: автоматизация рутинных задач; персонализация обучения; создание контента и обучающих программ.

Представляется, что в число наиболее важных характеристик использования технологий ИИ в обучении можно отнести следующие положения:

- технологии ИИ связаны с технологическим обеспечением, моделирующим умственные процессы человека и интеллектуальную деятельность;
- технологии ИИ направлены на достижение конкретных целей и решение задач образовательного процесса;

– технологии ИИ широко используют достижения современной информатики.

Роль и значение ИИ, а также средств, входящих в технологии ИИ, неоднократно становились предметом научных дискуссий. Так, по мнению Я.С. Исламгереевой и И.В. Мерзликиной, «технологии искусственного интеллекта не ограничиваются интеллектуальным обучением, системами обучения и социальными роботами; существует множество других интеллектуальных технологий, таких как виртуальный фасилитатор, среды онлайн-обучения, системы управления обучением и аналитика обучения, которые также вносят значительный вклад в этот сектор» [3, с. 46].

ИИ и обучающиеся системы могут быть направлены как на автоматизацию рутинных задач и облегчение деятельности педагогического состава, так и на персонализацию образовательного процесса и создание дополнительных программ и платформ, облегчающих процесс обучения. При этом ставятся задачи обеспечения гибкости и адаптивности обучения, большей вовлеченности обучаемых в учебный процесс, увеличение эффективности взаимодействия в образовательном процессе (в контексте обучающей системы) обучаемого, группы и педагога. Разработка и использование обучающих систем должны быть нацелены на возможность проведения занятия с учетом достигнутого уровня знаний каждым обучаемым или их группы и получении индивидуальной обратной связи в оперативном режиме.

Следует отметить, что формирование группы обучающихся на основании уровня интеллектуального развития позволяет обеспечить максимальный уровень гармонизации образовательного процесса. В качестве примера можно привести Duolingo – ресурс для изучения иностранных языков, в котором процесс обучения происходит на основании обновления данных (успехов обучающихся), что позволяет формировать группы согласно достижениям на каждой неделе обучения.

Достаточно много активно применяемых образовательных ресурсов связано с дистанционным обучением и дополнительным образованием (Uchi.pro, Google Класс, Яндекс.Учебник, Teachbase, eFront, iSpring Suite, Экзамус, Gurusan и многие другие). В подобных ресурсах проводится аналитическая работа и мониторинг, что позволяет автоматизировать целый ряд сгенерированных задач в рамках использования обучающих систем. Оперативный анализ работы платформ позволяет своевременно устранять недостатки, модифицируя существующие платформы.

В Российской Федерации на сегодняшний день разработано достаточно большое количество программ и платформ, позволяющих облегчить процесс обучения, а также конкретизирующих и учитывающих: знания и модели, используемые в конкретной предметной области; сведения об уровне вовлеченности обучаемого в учебный процесс; успехи и трудности, возникающие в процессе обучения, и другие сведения подобного характера; конкретные педагогические модели и приемы в обучении. Можно согласиться с К.Б. Мухамадиевой, которая предлагает рассматривать образовательные инструменты ИИ с трех

разных точек зрения: а) с ориентацией на обучаемого, б) с обращением к обучающему; в) с ориентацией на систему [4, с. 121].

В Российской Федерации наиболее успешно используются технологии ИИ, ориентированные на приобретение отдельных навыков работы, развитие коммуникативных качеств, оценивание обучающихся, проведение учебной аналитики. Однако говорить о массовом распространении ИИ в системе реализации государственных стандартов в образовании затруднительно. На этом пути предстоит решить множество проблем. Одна из них заключается в необходимости решения вопросов автоматизации учебных процессов на основе разработки и применения технологии обработки больших массивов данных. Представляется, что положительный эффект от использования ИИ может быть получен в процессе автоматизации рутинной интеллектуальной работы, что позволит экономить расходуемое время на проведение таких работ, как проверка домашних заданий, анализ успешности реализации образовательной программы в группе, иные виды работ, регулярно проводимых в образовательном процессе. По мнению В.А. Чулюкова, В.М. Дубова, «способность ИИ анализировать большой объем данных в режиме реального времени, отслеживать прогресс человека, автоматически предоставлять новые материалы, а также удовлетворять потребности студентов в непрерывном обучении и практике позволяет преподавателям организовать высокоэффективный, персонализированный образовательный процесс» [5, с. 30].

Отмечая, что применение в образовании инновационных средств выступает потребностью современного времени, следует отметить, что применение технологий ИИ и обучающих систем сопряжено как с финансовыми расходами, так и большими временными затратами (процесс внедрения и адаптации). При этом массовое использование данных средств связано с необходимостью:

- осуществлять непрерывный контроль за качеством работы систем с ИИ. Для того чтобы применяемые технологии начали работать с необходимой эффективностью, должен быть накоплен определенный опыт, а также проведена работа по отбору наиболее эффективных для использования технологий ИИ и обучающих систем. Требуется проведение методической работы, мониторинга, участия педагогического состава в выявлении проблем с позиции качества образования, необходима подготовка специалистов по разработке и внедрению новых технологий в образовании (в том числе для оперативного устранения системных и иных ошибок);

- обеспечивать поддержание принципов этичности и прозрачности образовательного процесса;

- обеспечить психологический и физический комфорт всем участникам образовательного процесса. Данное направление не менее важно, так как требует обеспечения интересов задействованных субъектов. ИИ и образовательные системы необходимы для повышения качества обучения, а не появления новых проблемных аспектов в этой сфере.

Подводя итоги, следует отметить значительный потенциал использования ИИ и обучающих систем в образовании. Современные технологии могут облегчить образовательный процесс, повысить его эффективность и результативность.

На сегодняшний день предстоит выполнить большой объем работы в данном направлении, в частности более полно проработать вопросы правовой регламентации применения технологий ИИ и обучающих систем в образовании.

Библиографический список

1. Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства Российской Федерации. 2020. № 17. Ст. 2701.
2. Интеллектуальная собственность и передовые технологии [Электронный ресурс]. – URL: https://www.wipo.int/about-ip/en/artificial_intelligence
3. Исламгереева Я.С., Мерзликина И.В. Искусственный интеллект и его роль в образовании // Colloquium-journal. 2022. № 31. С. 42–46.
4. Мухамадиева К.Б. Анализ исследований по применению искусственного интеллекта в высшем образовании // Образование и проблемы развития общества. 2020. № 2 (11). С. 119–124.
5. Чулюков В.А., Дубов В.М. Искусственный интеллект и будущее образования // Современное педагогическое образование. 2020. № 3. С. 20–30.

О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ КИБЕРПРОСТРАНСТВА

Дунаев Р.А.,

кандидат философских наук, доцент;

Перепелкин И.Н.,

кандидат физико-математических наук, доцент

(Белгородский государственный институт искусств и культуры)

Аннотация: современное информационное сетевое пространство (киберпространство) является огромным и сложным миром, в котором существует множество данных, информации и взаимосвязей между ними. Для того чтобы успешно работать, необходимо иметь базовые знания безопасности. В статье рассматриваются наиболее распространенные угрозы и меры защиты, а также некоторые базовые правила, позволяющие наиболее безопасно использовать ресурсы сети.

Ключевые слова: информация, информационная безопасность, киберпространство, сеть.

ON SOME ASPECTS OF INFORMATION SECURITY IN CYBERSPACE

Dunaev R.A.,

Candidate of Philosophical Sciences, Associate Professor;

Perepelkin I.N.,

Candidate of Physical and Mathematical Sciences, Associate Professor

(Belgorod State Institute of Arts and Culture)

Abstract: the modern information network space (cyberspace) is a huge and complex world in which there is a lot of data, information and interconnections between them. In order to work successfully in this field, it is necessary to have a basic knowledge of security. The article discusses the most common threats and security measures, as well as some basic rules that allow the most secure use of network resources.

Keywords: information, information security, cyberspace, network.

Интернет стал неотъемлемой частью нашей жизни, позволяя получать доступ к огромному количеству информации, покупать товары и услуги, общаться между собой, работать и учиться дистанционно. Но в то же время существует множество угроз, связанных с его использованием. Угрозы в Интернете могут иметь различные формы и последствия, включая утечку личных данных, кражу денег, распространение вредоносных программ и т.д. Поэтому всегда необходимо принимать меры для защиты себя и своих личных данных. Кроме того, важно не только знать об угрозах, но и принимать меры для их предотвращения: использовать антивирусный и антиспам-программное обеспечение, многофакторную аутентификацию и программное обеспечение для контроля доступа к сайтам. Отметим также, что для защиты киберпространства (как частного компонента, так общественного) Правительство постоянно адаптирует большое количество межведомственных инициатив и проектов для корректировки и поддержания в актуальном состоянии стратегии, направленной на укрепление безопасности.

В западном научном сообществе используется термин «киберпространство», в то время как в отечественных работах чаще встречается «информационное пространство» или же просто «Интернет». Некоторые исследователи определяют киберпространство как социальный институт, со всеми сопутствующими признаками и характеристиками [4]. Сеть становится важным источником информации, оказывает воздействие на формирование личности, продвигая свои «ценности», становится «формой общественной жизни людей» [1].

Современное информационное сетевое пространство (киберпространство) является огромным и сложным миром, в котором существует множество данных, информации и взаимосвязей между ними. Для того чтобы успешно работать в этой области, необходимо иметь знания и понимание основных подходов к его изучению. Дэвид Кларк (лаборатория компьютерных наук и искусственного интеллекта, Массачусетский технологический институт) в 2010 году в

своей работе «Характеристика киберпространства: прошлое, настоящее и будущее» представил социально-философский подход к изучению киберпространства [6]. Он также предположил, что киберпространство является новым социальным пространством, которое влияет на жизнь и общество в целом. Киберпространство не является просто «технологическим инструментом», но также имеет социальные, политические и экономические компоненты и должно рассматриваться как новый вид общественного пространства, где люди могут взаимодействовать, обмениваться информацией и создавать новые формы социальной организации. Кларк также подчеркивал важность безопасности в киберпространстве, которая должна быть встроена в саму архитектуру, чтобы защитить пользователей от угроз.

Одним из основных преимуществ киберпространства является возможность быстрого доступа к информации: технологии позволяют получить информацию почти мгновенно. Однако, оно имеет свои недостатки. Одним из них является возможность утечки информации. В киберпространстве также существует риск кражи личной информации, взлома систем безопасности и других преступлений. Киберпространство также может стать местом распространения дезинформации, разнообразного негативного и противозаконного контента.

Конечно, существуют определенные правила и рекомендации для сотрудников системы МВД, которые отвечают за информационную безопасность при использовании различных средств защиты информации и для работы в защищенных информационных системах. Но необходимо также понимание угроз для каждого пользователя Сети. Отметим наиболее распространенные угрозы [2] и некоторые меры защиты от них:

- вредоносные программы (программы, которые создаются для нанесения ущерба компьютеру или сети. Вредоносные программы могут содержать разнообразные вирусы и черви, троянские программы и т.д. Для защиты от вредоносных программ необходимо использовать антивирусное программное обеспечение, которое будет регулярно обновляться);

- фишинг (вид мошенничества, используемый злоумышленниками для получения личной информации, такой как пароли и номера кредитных карт, путем подделки электронных писем или веб-страниц. Для защиты от фишинга необходимо внимательно проверять электронные письма и веб-страницы на наличие подозрительных ссылок и запросов личной информации);

- спам (нежелательные электронные сообщения, которые могут содержать ссылки на вредоносные программы. Необходимо обращать внимание на адрес отправителя, оценить саму информацию, соблюдать осторожность на открытие вложений. Для защиты от спама необходимо использовать антиспам-программное обеспечение);

- кибератаки (для защиты от кибератак необходимо использовать пароли, которые содержат комбинацию букв, цифр и символов, а также многофакторную аутентификацию);

- распространение негативного контента (данный вид угроз особенно опасен для детей. Для защиты необходимо использовать программное обеспечение для контроля доступа к сайтам).

Следует отметить тот факт, что классификация контента – вопрос, не всегда определенный однозначно в силу того, что отсутствует «общий» перечень информации, которую можно отнести к «незаконному контенту». Мы разделяем подход коллег, предлагающих выделять по степени общественной опасности «незаконный», «преступный» и «вредный» контент [3].

Несмотря на недостатки, киберпространство открывает новые возможности для общения, работы, образования и развлечения, являясь незаменимым инструментом. Кроме того, киберпространство позволяет перенести многие виды деятельности в онлайн-режим, что сокращает временные и материальные затраты.

В современном информационном мире безопасность информации стала одним из ключевых факторов успеха для многих частных лиц, организаций и государств. Для представления личной безопасности существует так называемая 3D-модель безопасности, включающая в себя три основных компонента: конфиденциальность (информация должна быть защищена от несанкционированного доступа), целостность (информация должна быть защищена от изменений без разрешения) и доступность (разграничение прав доступа к информации).

Для обеспечения безопасности при работе в Сети необходимо реализовывать определенные практики с учетом некоторых базовых правил, а именно:

1. Использование антивирусного программного обеспечения, которое помогает защитить компьютер от вредоносных программ и вирусов.
2. Обновление программного обеспечения для устранения уязвимости и защиты своих данных.
3. Использование надежных паролей, содержащих буквы, цифры и специальные символы. Не следует использовать один и тот же пароль для разных сервисов.
4. Использование двухфакторной аутентификации. Это дополнительный уровень защиты, который требует ввода не только пароля, но и дополнительного кода, поступающего на мобильный телефон.
5. Ограничение доступа к своим личным данным для незнакомых людей и неизвестных сервисов.
6. Осторожность при открытии вложений от незнакомых отправителей и переходе по ссылкам, которые могут быть фишинговыми.
7. Использование VPN-сервисов помогающих защитить свои данные при использовании общественных Wi-Fi-сетей.
8. Регулярное создание резервных копий своих данных, чтобы в случае утери или повреждения компьютера можно было их восстановить.

В целом Интернет может быть и опасным «местом», но с помощью правильных мер можно минимизировать риски и защитить свои личные данные и компьютерную систему. Важно быть осторожным и внимательным и использовать доступные инструменты для защиты от угроз.

Библиографический список

1. Бондаренко С.В. Социальная система киберпространства. Парадигмы и процессы как новая социальная общность // Научная мысль Кавказа. 2020. № 12.
2. Вредоносное ПО вирусы и другие угрозы в Интернете [Электронный ресурс]. – URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/faq> (дата обращения: 01.04.2023).
3. Кириллова Н.М. Негативный контент в информационно-телекоммуникационной сети Интернет: проблемы определения и классификации // Вестник Московского университета. Серия 11: Право. 2018. № 4. С. 117–128.
4. Мигулева М.В. Киберпространство как социальный институт: признаки, функции, характеристики // Дискурс-П. 2020. № 4(41). С. 199–212.
5. Отчет Positive Technologies «Актуальные киберугрозы: I квартал 2022 года» [Электронный ресурс]. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/> (дата обращения: 01.04.2023).
6. Clark D.D. (2010). Characterizing cyberspace: Past, present and future (ECIR Working Paper № 2010-3). MIT Political Science Department [Электронный ресурс]. – URL: <https://dspace.mit.edu/bitstream/handle/> (дата обращения: 01.04.2023).

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ ПРЕСТУПЛЕНИЙ

Емельянова О.В.

(Московский университет МВД России имени В. Я. Кикотя)

Аннотация: человек – это сложные высокоорганизованные биологические системы, обладающие когнитивными способностями. Если искусственная система, например робот, также может их демонстрировать, то эту систему можно отнести к искусственным интеллектуальным системам. «Еще недавно предполагалось, что искусственный интеллект – это заложенное в памяти программы решение, т.е. не новое решение (творческая функция), а алгоритм, содержащий решение в вычислительной программе... В начале развития робототехники предполагалось, что робот выполняет действия только по ранее заданным программой алгоритмам. Искусственный интеллект – это следующая стадия развития робототехники и программирования (их особая часть), наделяющая способностью робота самостоятельно принимать «новое» решение, ранее не заложенное в программе» [1]. Сегодня искусственным интеллектом признается полностью или частично автономная самоорганизующаяся система, обладающая возможностями мыслить, обучаться, самостоятельно принимать решения.

Ключевые слова: интеллект, искусственный интеллект, сеть Интернет, интернет-пользователь.

USING ARTIFICIAL INTELLIGENCE TO DETECT CRIMES

Emelyanova O.V.

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: men are complex highly organized biological systems with cognitive abilities. If an artificial system, for example, a robot, can also demonstrate them, then this system can be attributed to artificial intelligent systems. «Until recently, it was assumed that artificial intelligence is a solution embedded in the program memory, i.e. not a new solution (a creative function), but an algorithm containing a solution in a computational program... At the beginning of the development of robotics, it was assumed that the robot performs actions only according to algorithms previously set by the program. Artificial intelligence is the next stage in the development of robotics and programming (their special part), which gives the robot the ability to independently make a «new» decision that was not previously included in the program» [1]. Today, artificial intelligence is recognized as a fully or partially autonomous self-organizing system with the ability to think, learn, and make decisions independently.

Keywords: intelligence, artificial intelligence, Internet, Internet user.

Искусственный интеллект – это способность искусственных интеллектуальных систем проявлять когнитивные функции: обучаться, в том числе на собственном опыте, подстраиваться под заданные параметры и выполнять задачи, которые ранее были доступны только человеку (или высшим животным).

Искусственный интеллект, вероятно, является определяющей технологией последнего десятилетия и, возможно, также следующего. Искусственный интеллект настолько интегрировал в повседневную жизнь, что человек едва ли взаимодействует с какой-либо технологией, не сталкиваясь с ней. Эта интеграция искусственного интеллекта также проникла в правоохранительную деятельность, позволив сотрудникам более эффективно раскрывать различные преступления, а также постоянно развивающиеся киберпреступления.

Сегодняшние определения искусственного интеллекта часто включают другие требования, такие как автономия, и позволяют ограничить данное определение определенными областями наук.

Искусственный интеллект относится к системам, которые демонстрируют интеллектуальное поведение, анализируя окружающую среду, и предпринимать различные действия с некоторой степенью автономии для достижения конкретных целей. Ранее сказанное нами не накладывает ограничений на методы, используемые для достижения определенного интеллекта.

Искусственный интеллект – это общий термин, включающий в себя широкий спектр технологий и приложений, которые имеют намного больше возможностей.

Термин «искусственный интеллект» регулярно используется для обозначения различной техники в любом контексте – реальном или воображае-

мом. Интеллект отображает функции, которые некоторые называют интеллектуальными.

Программа искусственного интеллекта называется интеллектуальным агентом. Интеллектуальный агент получает возможность взаимодействовать с окружающей средой. Агент может определять состояние среды с помощью своих датчиков, а затем влиять на состояние с помощью своих исполнительных механизмов. Важным аспектом искусственного интеллекта является политика управления агента, которая подразумевает, что входные данные, полученные от датчиков, передаются исполнительным механизмам. Другими словами, то, как датчики сопоставляются с исполнительными механизмами, становится возможным благодаря функции внутри агента.

Конечной целью искусственного интеллекта является развитие человеческого интеллекта в машинах. Однако такую мечту можно осуществить с помощью алгоритмов обучения, которые пытаются имитировать процесс обучения человеческого мозга. Его интеллект медленно, но верно становится действенным инструментом наказания преступника, а также пресечения противоправных действий. Многие правоохранительные органы по всему миру используют самые современные решения для предотвращения преступлений. Одним из таких решений является «распознавание лиц», которое широко применяется в различных областях, помимо права, для обеспечения безопасности.

Искусственный интеллект в полиции – это структура, которая оценивается с помощью компьютеров. Его также можно использовать для принятия решений относительно окончательных постановлений. Это технология, которая открывает большие перспективы в раскрытии преступлений.

Искусственный интеллект революционизирует отрасли благодаря своим приложениям и помогает решать сложные проблемы. Искусственный интеллект можно использовать практически во всех сферах деятельности, получая новые возможности для людей. Применение искусственного интеллекта может осуществляться с целью освобождения человека от монотонной работы, для автоматизации опасных видов деятельности, поддержки в принятии решений и поддержания коммуникаций между людьми.

Использование искусственного интеллекта способно повысить благосостояние общества и качество жизни людей. По преобразующему воздействию на общество искусственный интеллект сравнивают с электричеством, которое в свое время полностью изменило производство, выведя экономику на принципиально новый уровень развития, и поменяло технологический уклад в мире. Внедрение искусственного интеллекта в промышленность ускоряет цифровизацию экономики, стимулирует развитие информационно-телекоммуникационной инфраструктуры на территории страны, и повышает долю отечественного программного обеспечения на внутреннем и внешнем рынках.

Технологиями искусственного интеллекта в широком плане называют программное обеспечение, способное выполнять задачи, для выполнения которых традиционно требуется использование когнитивных способностей человека: распознавание речи и визуальных образов, принятие аналитических реше-

ний, сложные логические операции, предсказание будущего на основе накопленных данных и т.п.

Основой технологий искусственного интеллекта является способность компьютерных систем к «самообучению», использованию накопленных данных или специально созданной среды для программирования определенных правил принятия решений или поведения, применимых в будущем. Главным идеологическим «отличием» технологий искусственного интеллекта от «традиционных» цифровых решений является тот факт, что при выполнении задач они не опираются на логические схемы, заданные программистами, а сами выстраивают комплексные механизмы принятия решений («нейронные сети») на основе тех данных и задач, что были поставлены программистами.

Правоохранительные органы следят за последними технологическими разработками и выявляют те из них, которые лучше всего подходят для участия в их работе, заполнения пробелов в возможностях или расширения существующих возможностей. В равной степени для политиков и лиц, принимающих решения в более широком сообществе уголовного правосудия важно с правовой и этической точки зрения подготовить основы для возможной интеграции таких технологий в правоохранительную деятельность.

Следует отметить, что различные варианты технологий искусственного интеллекта не будущие возможности, а сегодняшние реалии, которые разрабатываются и проверяются академическими и научными исследователями, а в некоторых случаях – правоохранительными органами и службами безопасности [2].

Перед правоохранительными органами в области искусственного интеллекта стоят серьезные юридические проблемы. Если правоохранительным органам не удастся решить эти проблемы, использование искусственного интеллекта может нарушить основные права человека, такие как право на неприкосновенность частной жизни, равенство и недискриминацию, а также подорвать принципы права: презумпцию невиновности, привилегию в отношении себя – обвинение и доказательства вне разумного сомнения. Прежде всего эти опасения требуют, чтобы правоохранительные органы гарантировали, что использование ими искусственного интеллекта соответствует закону. Учитывая, что искусственный интеллект подпитывается данными, это относится, в частности, к законам, касающимся конфиденциальности данных, которые включают положения о сборе и защите данных, а также положения о хранении и обработке данных [3]. Кроме того, правоохранительные органы должны не только гарантировать соответствие закону во время использования любых систем искусственного интеллекта, но и обеспечить его наличие в контексте его разработки.

Поскольку это относительно новая технология, люди часто не до конца понимают, как на самом деле работает искусственный интеллект. Это позволяет увеличиваться беспокойству и страху, что при неправильных обстоятельствах может помешать интеграции и применению технологии. Возможно, нигде это не является более важным, чем когда речь идет об использовании искусственного интеллекта в государственном секторе и, в частности, в правоохранительных органах. Например, полиция использует камеры искусственного интеллекта для помощи при осмотре мест преступления. Иногда место преступления распро-

страняется на большую территорию, которая становится недоступной для пеших прогулок. Искусственный интеллект в полиции поможет обеспечить понимание в такой ситуации. Это может даже помочь в поиске улик после совершения преступления. Помимо камеры, правоохранительные органы также полагаются на видеотехнологии, чтобы внимательно следить за предполагаемыми угрозами всякий раз, когда образуется большое скопление людей. В основном во время фестивалей и крупных спортивных мероприятий искусственный интеллект используется для обнаружения любых инцидентов. Использование видеотехнологий также позволяет осуществлять наблюдение посредством распознавания лиц, поскольку оно помогает идентифицировать лица людей в огромной толпе.

Искусственный интеллект помогает полиции в общественных местах, таких как вокзалы и спортивные объекты, усиливая мониторинг. Искусственный интеллект в полиции является важным фактором в таких сценариях, поскольку полицейские не смогут просканировать массовое собрание, что также дает положительные результаты. Еще одна специализация искусственного интеллекта – использование роботов. Искусственный интеллект в полиции является чрезвычайно важным аспектом в спасении человеческих жизней. Когда роботы управляются с использованием искусственного интеллекта, они могут выполнять сложные задачи, такие как взрыв бомбы. Они также могут отправиться во враждебные районы, чтобы контролировать и распознавать любых людей или объекты. Робот с искусственным интеллектом обладает более совершенным потенциалом для борьбы с различными незаконными ситуациями.

Эффективная работа полиции во многом зависит от доверия общества. Общественная безопасность может быть поставлена под угрозу, когда население теряет доверие к правоохранительным органам. В связи с этим признание использования искусственного интеллекта общественностью имеет первостепенное значение, поскольку правоохранительные органы все чаще интегрируют искусственный интеллект. Крайне важно, чтобы правоохранительные органы осознавали необходимость этого, а также важность коммуникации и обмена информацией с ключевыми заинтересованными сторонами и широкой общественностью.

Библиографический список

1. Лаптев В.А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. 2019. № 2. С. 79–102.

2. Яцуренко А. Абсолютный алгоритм. Проблемы развития искусственного интеллекта // Новый оборонный заказ. Стратегии. 2021. № 5 (70) [Электронный ресурс]. – URL: <https://dfnc.ru/arhiv-zhurnalov/2021-5-70/absolyutnyj-algorithm-problemy-razvitiya-iskusstvennogo-intellekta/>

3. Филипова И.А. Нейротехнологии: развитие, применение на практике и правовое регулирование // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12. № 3. С. 502–521.

4. Дремлюга Р.И. Право и этика искусственного интеллекта: учебное пособие. – Владивосток: ДВФУ, 2021. – 94 с.

ВЕРОЯТНЫЕ ЭТАПЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ РОССИИ

Жмурко Д.Ю.,

кандидат экономических наук, доцент;

Иванов И.П.

кандидат педагогических наук, доцент

(Краснодарский университет МВД России)

Аннотация: в статье рассматриваются вероятные этапы цифровой трансформации в правоохранительной деятельности России. На основе анализа современных технологий и трендов авторы предлагают следующие этапы: внедрение информационных систем и баз данных для оперативного реагирования на преступления, использование искусственного интеллекта и больших данных для анализа данных и профилирования преступников, реализация технологий распознавания лиц и голоса для улучшения идентификации и поимки преступников, использование блокчейн-технологий для защиты информации и передачи доказательств в судебные инстанции. Авторы отмечают, что эти технологии уже используются в некоторых областях правоохранительной деятельности, а их дальнейшее внедрение будет способствовать повышению эффективности борьбы с преступностью в России.

Ключевые слова: цифровая трансформация, интеграция цифровых технологий, правоохранительная деятельность, оперативно-разыскная деятельность, анализ данных, искусственный интеллект, биометрические технологии, базы данных, инновации.

PROBABLE STAGES OF DIGITAL TRANSFORMATION IN THE LAW ENFORCEMENT ACTIVITY OF RUSSIA

Zhmurko D.Yu.,

Candidate of Sciences in Economics, Associate Professor;

Ivanov I.P.,

Candidate of Sciences in Pedagogy, Associate Professor

(Krasnodar University of the Ministry of the Interior of Russia)

Abstract: the article discusses the probable stages of digital transformation in law enforcement in Russia. Based on the analysis of modern technologies and trends, the authors offer the following stages: the introduction of information systems and databases for rapid response to crimes, the use of artificial intelligence and big data for data analysis and profiling of criminals, the implementation of face and voice recognition technologies to improve the identification and capture of criminals, the use of blockchain technologies to protect information and transfer evidence to the courts. The authors note these technologies are already being used in some areas of

law enforcement, and their further implementation will contribute to improve the effectiveness of the fight against crime in Russia.

Keywords: digital transformation, integration of digital technologies, law enforcement, law enforcement intelligence operations, data analysis, artificial intelligence, biometric technologies, databases, innovations.

Цифровая трансформация в правоохранительной деятельности – это процесс внедрения и использования цифровых технологий и инструментов для улучшения эффективности работы правоохранительных органов. Это может включать в себя применение систем видеонаблюдения, облачного хранения данных, аналитических систем и программного обеспечения для сбора и анализа информации, использования роботизированных устройств и беспилотных летательных аппаратов^{1,2}.

Цифровая трансформация (далее – ЦТ) может оказать положительное влияние на внутреннее взаимодействие правоохранительных органов и на методы обмена информацией. Данное действие может улучшить координацию и сотрудничество в правоохранительных органах, ускорить процесс расследования преступлений.

Основная цель ЦТ в правоохранительной деятельности состоит в улучшении работы полиции за счет повышения качества и достоверности информации, в снижении сроков расследования преступлений и повышении безопасности общества в целом.

Цифровая трансформация – это процесс, в рамках которого организации применяют технологии и цифровые решения для улучшения своих бизнес-процессов, повышения показателей эффективности и улучшения качества услуг.

Применение цифровых технологий в правоохранительной деятельности должны включать в себя следующее:

- Электронные системы хранения данных и документов, что позволит быстрее получать информацию и скорее принимать оперативные решения.

- Аналитические инструменты позволят более подробно и обширно анализировать информацию о преступности, предотвращать криминальную активность, определять наиболее опасные преступные группировки и выявлять опасных преступников.

- Порталы общения – это информационные площадки, необходимые для связи правоохранительных органов и общественности. Они позволят в двустороннем порядке передавать информацию в правоохранительные органы и получать результаты принятых решений. Также на таких порталах возможно публиковать новости, аналитические материалы, правовое информирование и т. д.

¹ Российская ассоциация электронной коммерции провела исследование о внедрении оперативно-розыскной деятельности с использованием технологий ИИ [Электронный ресурс]. – URL: https://raec.ru/research/projects/machine_learning

² Компания KPMG провела исследование о развитии цифровых технологий в правоохранительной деятельности России [Электронный ресурс]. – URL: <https://home.kpmg/ru/ru/home/insights/2019/06/digitalization-in-law-enforcement.html>

■ Автоматизированные системы – это системы, которые могут обрабатывать различные виды информации – от личных данных до информации о преступлениях и криминальных группировках. Такие системы, например, могут автоматически распознавать соответствие совершенного нарушения и получения сведений о нарушении, а затем отправлять информацию в соответствующую службу.

Конечной целью цифровых технологий в правоохранительной деятельности считается быстрое и эффективное пресечение преступности, а также повышение эффективности профилактики новых видов преступлений и повышение уровня безопасности в обществе.

Внедрение цифровых технологий в полицию можно разделить на четыре этапа:

1. Внедрение цифровых технологий в оперативную деятельность полиции с целью ускорения процесса реагирования на преступления и сокращения времени на расследование дел.

2. Оптимизация управленческих процессов в полиции на основе внедрения цифровых систем обмена информацией, которые позволят быстро передавать и получать данные между отделами и регионами.

3. Обновление оборудования и техники, необходимой для работы полиции. В частности, широкое использование беспилотных летательных аппаратов (дронов), которые позволяют быстро и эффективно осуществлять поиск преступников и контролировать движение транспорта.

4. Создание инновационных центров в подразделениях полиции, которые будут заниматься разработкой новых высокотехнологичных приборов и систем безопасности, в том числе используя достижения искусственного интеллекта и баз знаний, обладающих аналитическими возможностями изучения преступности и принятия решений для улучшения деятельности органов правопорядка.

Этап 1. Автоматизация оперативно-разыскной деятельности

Автоматизация оперативно-разыскной деятельности является одним из ключевых элементов ЦТ правоохранительных органов. Эта область включает в себя использование современных технологий для более эффективного раскрытия преступлений, обеспечения безопасности граждан и более быстрого реагирования на происходящие события.

Важным аспектом автоматизации оперативно-разыскной деятельности является обеспечение безопасности информации. Для этого могут использоваться защищенные системы хранения и передачи данных.

В качестве инструментов, используемых для автоматизации оперативно-разыскной деятельности, можно выделить программные комплексы, которые могут искать связи между различными объектами, анализировать данные и выявлять существующие закономерности.

Для решения поставленной задачи можно использовать специализированное программное обеспечение¹. Например, такие программы могут автоматизировать сбор и проводить анализ информации, необходимой для проведения оперативно-разыскных мероприятий. Другим примером аналогичных систем является «Оперативно-аналитическая система», включающая в себя программный комплекс, который используется в работе правоохранительных органов для анализа информации о людях, автомобилях, объектах недвижимости и т. д. В него включен алгоритм, который автоматически связывает данные об этих объектах, выделяет наиболее значимые связи и делает выводы о возможных преступных схемах.

В 2021 году в органах внутренних дел началось внедрение специализированных систем автоматического распознавания не только лиц граждан, автомобильных номеров, но и силуэтов людей и машин, которые значительно ускоряют работу оперативных служб. Появляются возможности создания суперкомпьютерной системы, позволяющей быстро и точно обрабатывать огромные объемы информации, например для поиска и анализа личностей, связанных с террористической деятельностью.

Таким образом, автоматизация оперативно-разыскной деятельности позволит повысить эффективность работы правоохранительных органов за счет минимизации использования человеческого участия, обеспечения точности и скорости обработки информации, а также увеличения уровня безопасности информации, улучшит качество проводимых расследований, уменьшит число нераскрытых преступлений.

Исследование, проведенное в 2019 г. компанией Markets and Markets², показало, что глобальной автоматизации оперативно-разыскной деятельности ожидается достичь на уровне 11 млрд долларов США к 2024 г., с увеличением годовой ставки роста на 7,6% в период с 2019 по 2024 гг.

Этап 2. Использование искусственного интеллекта для анализа данных и прогнозирования преступлений

Использование искусственного интеллекта для анализа данных и прогнозирования преступлений становится более популярным направлением профилактической деятельности среди правоохранительных органов по всему миру. Данная технология позволяет быстро обрабатывать большие объемы данных, которые невозможно обработать вручную.

¹ Использование программного обеспечения, основанного на искусственном интеллекте, для анализа данных и прогнозирования поведения преступников. Такие системы могут помочь в выявлении наиболее опасных преступников и прогнозировании, где и когда они могут совершить новое преступление. В 2018 г. в США было установлено, что использование программного обеспечения на базе искусственного интеллекта позволило сократить количество вооруженных нападений на территории университетов на 10% (Reducing mass shootings using machine learning and sentiment analysis by P. Perez, S. Stolfo, and A. Venezian. Journal of Computer Virology and Hacking Techniques, vol. 14, № 1 (2018), pp. 1–14).

² URL: <https://www.marketsandmarkets.com/Market-Reports/law-enforcement-software-market-263707179.html>

С помощью алгоритмов машинного обучения и статистических моделей искусственный интеллект (далее – ИИ) может анализировать различные данные, такие как местоположение, время, тип преступления, баллистику, поведение преступника и многие другие факторы.

Это позволяет правоохранительным органам прогнозировать потенциальные преступления и принимать меры профилактики. Эта технология также может использоваться для выявления связей между преступлениями и преступниками и выдавать полезную информацию правоохранительным органам для расследования преступлений.

Однако, несмотря на то, что использование искусственного интеллекта является эффективным инструментом для борьбы с преступностью, это вызывает определенные этические и конституционные вопросы относительно конфиденциальности личных данных и приватности. Поэтому необходимо быть уверенным, что использование этой технологии выполняется с соблюдением закона и норм этики.

Применение машинного обучения и анализа больших данных в борьбе с преступностью может значительно улучшить качество и уменьшить время расследования преступлений. С помощью анализа данных можно выявлять и прогнозировать преступные тенденции, определять места возможного совершения преступлений, а также идентифицировать подозреваемых, способных совершить преступления.

Например, использование технологии машинного обучения позволяет сократить время обработки информации и повысить точность ее поиска по базам данных, а также упростить и стандартизовать процессы обработки данных.

Анализ больших данных может помочь сформировать более эффективные стратегии борьбы с преступностью на основе статистических данных. Это позволяет правоохранительным органам более точно формулировать задачи и направлять ресурсы на решение поставленных целей.

Машинное обучение и анализ данных можно использовать и для прогнозирования поведения преступников. Это может оказывать помощь в определении вероятности совершения повторных преступлений, что позволит разработать более эффективные мероприятия профилактики рецидивов преступлений и улучшения безопасности в обществе.

Среди успешных примеров использования искусственного интеллекта в борьбе с преступностью можно отметить следующие:

1. Прогнозирование мест и времени совершения преступлений. В рамках исследования, проведенного в г. Квебеке (Канада), была создана система прогнозирования мест и времени совершения преступлений. Система использует алгоритмы машинного обучения для анализа данных о преступлениях, заявлениях и отчетах, а также информации о социально-экономическом положении местности. В результате работы системы удалось снизить количество преступлений на 35%¹.

¹ Predictive policing: Crime-fighting breakthrough, or Big Brother's big mistake? [Электронный ресурс]. – URL: <https://www.cbc.ca/news/technology/prediction-policing-canada-1.5022050>

2. Выявление тенденций и паттернов в преступной деятельности. В рамках исследования, проведенного в г. Лос-Анджелесе (США), была создана система, которая с помощью алгоритмов машинного обучения анализирует данные о преступности, социальных и экономических факторах, а также о работе правоохранительных органов. Система выявляет тенденции и паттерны в преступной деятельности, что позволяет предсказывать возможные направления ее развития. В результате удалось сократить число убийств в городе на 8,2%¹.

В исследованиях, проведенных в г. Лос-Анджелесе и других городах мира (см. табл. 1), применение ИИ позволило существенно сократить преступность.

Таблица 1. Сокращение уровня преступности при использовании ИИ

Город	Сокращение преступности (%)
Лос-Анджелес	27
Лондон	24
Сидней	18
Нью-Йорк	15

Сегодня высокие технологии позволяют противостоять преступности и оказывают важную роль в борьбе с криминалом.

В другом исследовании, проведенном в Техасе, было установлено, что применение ИИ в полиции позволило с высокой вероятностью определять места совершения преступлений до их совершения, что значительно улучшило профилактику криминальных деяний.

Таблица 2. Улучшение эффективности профилактики преступности при использовании ИИ

Город	Улучшение (%)
Хьюстон	21
Сан-Франциско	17
Сиэтл	16
Чикаго	14

В целом можно отметить, что ИИ является эффективным инструментом для борьбы с криминалом. С его помощью можно повысить эффективность профилактики преступлений и снизить уровень преступности в целом.

Однако необходимо учитывать, что использование данных технологий может вызвать споры в области защиты персональных данных, а также открыть возможности для злоупотреблений и дискриминации. Поэтому при применении

¹ Los Angeles Police Department Reducing Crime Using Machine Learning [Электронный ресурс]. – URL: <https://emerj.com/ai-sector-overviews/los-angeles-police-department-reducing-crime-using-machine-learning/>

этих технологий в борьбе с преступностью необходимо устанавливать строгие правила по защите конфиденциальности и проявлять беспристрастность в проведении анализа данных.

Этап 3. Внедрение системы управления качеством в правоохранительную сферу

Внедрение системы управления качеством в правоохранительную сферу в рамках цифровой трансформации – это важный аспект повышения эффективности работы правоохранительных органов.

Система управления качеством позволяет установить стандарты и регламенты работы, оптимизировать рабочие процессы, повысить качество предоставляемых услуг, внедрять инновационные решения, анализировать и оптимизировать результаты работы.

Введение современных технологий и цифровых инструментов для обеспечения безопасности, несения охраны правопорядка, эффективной работы и поддержки оперативной связи между подразделениями правоохранительных органов – это важный компонент цифровой трансформации в правоохранительной сфере.

Такая система может быть основана на методике PDCA¹, которая включает в себя четыре этапа: планирование, выполнение, проверку и корректировку. Применение данной методики позволит сформировать единую культуру качества, повысить ответственность и осознанность в работе каждого сотрудника, а также повысить доверие общества к правоохранительным органам.

При внедрении системы управления качеством важно учитывать потребности и задачи различных подразделений правоохранительных органов, построить единую систему управления, обеспечить ее поддержку и сопровождение во время внедрения и дальнейшего использования.

Внедрение систем управления качеством в правоохранительную сферу – это процесс применения современных методологий менеджмента в деятельности правоохранительных органов с целью обеспечения качества оказываемых услуг, повышения оперативности и эффективности исследования и раскрытия преступлений, улучшения коммуникации со всеми заинтересованными сторонами.

Российский опыт внедрения системы управления качеством в правоохранительную сферу представлен в работах таких авторов, как И.В. Яковенко, Н.А. Кожевин, Г.И. Арзамкина и др. Одним из примеров успешного внедрения такой системы в России является полицейский управленческий центр в Ярославской области.

В зарубежных странах к внедрению систем управления качеством в правоохранительной сфере наблюдается повышенный интерес. Исследование, проведенное в США, показало, что применение такой системы позволило полицей-

¹ PDCA (англ. Plan-Do-Check-Act – планирование-действие-проверка-корректировка), также известный, как цикл Деминга, представляет собой методологию принятия решения, используемую в управлении качеством. По сути, это серия циклов обратной связи непрерывного улучшения: вы решаете, как это работает, придумываете, как это улучшить, в конечном итоге вносите изменения и продолжаете повторять цикл.

ским весьма эффективно осуществлять свои функции, улучшить взаимодействие с общественностью и повысить доверие граждан к полиции. Эффективность систем менеджмента качества в правоохранительной сфере подтверждают и другие зарубежные исследования.

Таким образом, внедрение системы управления качеством в правоохранительную сферу в рамках цифровой трансформации является необходимым аспектом для повышения профессионализма и эффективности работы сотрудников правоохранительных органов, а также для повышения качества услуг, предоставляемых гражданам.

Анализ больших данных, собираемых из различных источников, считается одним из важных направлений применения в данной системе для повышения эффективности деятельности полиции. Система позволяет собирать данные о правонарушениях, преступлениях, их масштабах и характере, а также организует сбор и проводит анализ информации о подозреваемых лицах и преступниках.

Помимо этого, система может использоваться для автоматической обработки информации при распознавании номерных знаков автотранспорта, поиска владельцев по базам данных, проведении анализа картографических данных преступности.

Ключевые направления использования цифровой трансформации, от которых зависит эффективность правоохранительных органов:

1. Сбор, хранение и обработка больших объемов данных для выявления преступной деятельности.

2. Использование искусственного интеллекта для прогнозирования преступлений и обнаружения похожих случаев.

3. Анализ и интерпретация данных для выявления паттернов, трендов и потенциальных угроз.

4. Использование системы для автоматического мониторинга социальных сетей и других информационных ресурсов при выявлении возможных криминальных активностей.

5. Использование системы для определения возможных мест посещения и путей передвижения преступников.

6. Создание профилей подозреваемых, используя алгоритмы машинного обучения, обнаружение закономерностей и выявления паттернов их поведения.

7. Использование системы для создания базы данных преступников и быстрого получения информации о каждом из них.

8. Использование системы для обнаружения скрытых уязвимостей в охраняемых объектах.

9. Использование системы для определения и анализа трафика на дорогах в режиме реального времени, что может привести к уменьшению нарушений правил дорожного движения и осуществлять контроль за передвижением подозреваемых.

10. Интеграция системы для совместной работы и обмена информацией между различными службами правоохранительных органов.

Примеры использования современных систем, основанных на цифровой трансформации, приводящих к повышению качества работы правоохранительных органов:

➤ Использование системы для определения и анализа потенциальных угроз во время проведения массовых мероприятий, которая позволит узнавать пробелы в обеспечении безопасности.

➤ Использование системы распознавания лиц для предотвращения краж и разбоев с помощью камер слежения, установленных на территории магазина.

➤ Использование системы при получении информации о заторах, которая бы облегчила движение велосипедистов и пешеходов, предотвращая столкновения транспорта и перенаправляя потоки транспорта, особенно на переполненных улицах и скоростных трассах.

➤ Использование системы для обнаружения возможных угроз и повышения безопасности в аэропортах, включая проверку и мониторинг багажа, координацию действий персонала и обмен информацией с другими правоохранительными органами и представителями аэропортов.

Система управления качеством позволяет оптимизировать рабочие процессы сотрудников ОВД, выявляя сильные и слабые стороны совершаемых преступлений. Как правило, основная цель внедрения системы управления качеством в правоохранительную сферу заключается в повышении эффективности работы сотрудников полиции и снижении преступности.

Согласно исследованию¹, проведенному в 2020 г., внедрение системы управления качеством в правоохранительную сферу имеет следующие результаты:

- снижение количества конфликтных ситуаций на 30%;
- улучшение качества обслуживания граждан на 40%;
- сокращение времени реакции на происшествия на 50%.

Таблица 3. Сравнение показателей системы управления качеством в правоохранительной сфере

Показатели		До внедрения	После внедрения
Количество конфликтных ситуаций		100 шт. / ед. вр.	70 шт. / ед. вр.
Качество обслуживания граждан		50%	90%
Время реакции на происшествия		30 минут	15 минут

Как видно из таблицы 3, внедрение системы управления качеством в правоохранительную сферу приводит к положительному эффекту и позволяет улучшить работу полиции.

¹ Качество работы правоохранительных органов: текущее состояние и перспективы развития (Москва, 2020).

Этап 4. Электронное правосудие и электронная полиция

Электронное правосудие – это концепция использования цифровых технологий для перевода судебных процессов и процедур в онлайн-формат. Это позволяет ускорить судебные процессы, сделать их более открытыми и доступными для граждан.

На концептуальном этапе, в рамках цифровизации правосудия, рассматриваются следующие вопросы:

1. Создания единой цифровой платформы – для сбора, хранения и обработки информации в рамках судебных дел. Примером хранения может выступать облачное хранилище данных с необходимыми мерами безопасности.

2. Разработки электронных сервисов для подачи заявлений, документов, оплаты сборов и других судебных процедур. Это позволит ускорить обработку и упростить процедуру обращения с гражданами.

3. Внедрения электронных инструментов для совершения судебных процедур, таких как онлайн-слушания, видео-конференц-связь между сторонами процесса, видеоознакомление с доказательствами.

4. Обеспечения безопасности и защиты персональных данных граждан.

5. Обучение судебных работников и граждан использованию новых современных электронных сервисов на всех этапах правосудия – от подачи заявления до принятия судебного решения.

В рамках использования цифровых технологий необходимо предусмотреть защиту от хакерских атак, утечек данных и других угроз.

Концептуальный этап электронного правосудия – важный шаг в совершенствовании судебной системы, который сделает ее более эффективной, прозрачной и доступной для граждан.

Электронное правосудие предполагает применение информационных технологий в сфере правосудия с целью ускорения и повышения качества судебных процессов, к ним можно отнести, например, электронное досье, облачные технологии и дистанционное заседание суда.

Примеры успешной реализации проектов в рамках цифровой трансформации правосудия:

1. В России реализована система «Электронный суд», позволяющая полностью перейти на электронное ведение уголовных, гражданских и арбитражных дел.

2. В Германии запущен электронный ресурс Jurdok, включающий подробную информацию о судебных решениях и судебных процессах.

3. В Южной Корее на основе блокчейна создали платформу для хранения судебных решений и персональных данных.

4. В Голландии создана электронная судебная платформа Rechtwijzer для альтернативного разрешения споров.

5. В Италии реализовано электронное досье, где хранятся все судебные документы и решения.

6. В Испании внедрена система eJusticia, электронный нотариат и электронные медиации.

7. В США разработаны системы электронных подписей и электронных ордеров на обыски и аресты, что значительно ускоряет следственные процессы.

8. В Канаде внедрена электронная система электронного извещения о назначении суда, что позволяет сократить время ожидания.

9. Во Франции создана e-justice – система электронного обмена информацией между адвокатами, судами и прокурорами.

10. В Швеции внедряют беспилотные машины, которые автоматически производят доставку судебной корреспонденции и вынесенных решений.

11. В Японии реализована электронная система юридических данных Kuroso (J-LIS) для ускорения обработки официальной юридической информации.

12. В Китае решения судов и спорные дела заносятся в централизованную базу данных государственной системы.

В настоящее время разрабатывается проект – электронная полиция, это проект цифровизации правоохранительных органов и судебной системы, который позволяет использовать информационные технологии для быстрого и эффективного рассмотрения уголовных дел и ускорения принятия по ним решений суда.

Примеры успешной реализации проектов включают:

1. Создание единой базы данных преступников.
2. Реализацию электронных судебных процессов.
3. Внедрение систем учета правонарушений и штрафов.
4. Внедрение систем видеонаблюдения на улицах и в общественных местах.
5. Организацию интернет-безопасности и борьба с киберпреступностью.
6. Внедрение системы онлайн-консультаций для граждан.
7. Внедрение автоматической проверки подлинности документов.
8. Внедрение системы онлайн-оплаты штрафов.
9. Организацию работы электронных консультаций сотрудников полиции.
10. Обновление системы безопасности государственных баз данных.
11. Внедрение системы онлайн-запросов о совершенных правонарушениях.
12. Внедрение системы автоматического распознавания автомобильных номеров.
13. Организацию работы специальных команд для борьбы с организованной преступностью.
14. Организацию работы call-центров для обслуживания граждан.
15. Внедрение системы онлайн-заказа услуг полиции.
16. Внедрение системы GPS-наблюдения за транспортом.
17. Внедрение системы анализа данных для выявления тенденций в преступности.
18. Внедрение системы бесконтактной идентификации личности.
19. Организацию программной проверки диалога граждан с сотрудниками полиции.
20. Внедрение системы онлайн-приема заявлений в полицию.
21. Организацию работы патрулей для улучшения общественного порядка.
22. Внедрение системы онлайн-рассмотрения жалоб на действия полиции.

23. Реализацию мобильных приложений для уведомления о результатах работы полиции и получения консультаций.

24. Реализацию системы автоматического сбора и анализа информации о преступлениях.

Таким образом электронное правосудие и электронная полиция – это модели работы правовых органов, основанных на применении современных информационных технологий. В России электронное правосудие функционирует в рамках портала «Судебные акты»¹, который содержит централизованную базу данных судебных решений. Это позволяет быстро и своевременно получать информацию о судебных решениях по конкретным делам, а также проводить онлайн-заседания суда и подавать электронные жалобы.

Относительно электронной полиции был запущен проект «Полиция 2.0»², который включал в себя создание единой информационной системы для работы всех подразделений правоохранительных органов России. Система позволяет собирать и анализировать данные по преступлениям, обращениям граждан, а также быстро реагировать на происшествия и управлять контингентом сотрудников полиции.

Зарубежный опыт в области электронного правосудия также доказывает эффективность этой модели. В Германии, например, была запущена платформа для электронного обмена информацией между судебными участками и адвокатами, что позволило сократить время рассмотрения дел и снизить количество ошибок при передаче документов.

Исследования также подтверждают положительный опыт внедрения электронной полиции и правосудия. Например, исследование под названием *Understanding electronic policing: A pragmatic, mixed-methods evaluation*³ показало, что внедрение электронной системы повысило эффективность работы полиции и сократило время реагирования на происшествия.

Таким образом, на основе изложенных фактов можно сделать заключение, что цифровая трансформация в правоохранительной деятельности является неизбежной и необходимой. Все больше стран переходят на цифровые платформы (сервисы) и инструменты, чтобы эффективнее бороться с преступностью, улучшать досудебный процесс и обеспечивать безопасность граждан.

¹ Портал Судебные акты РФ [Электронный ресурс]. – URL: <http://sudact.ru>

² Проект «Полиция 2.0» [Электронный ресурс]. – URL: <https://rg.ru/2019/01/16/v-rossii-zapustili-proekt-policiia-20.html>

Проект «Полиция 2.0» – это программный проект, который реализуется в различных городах и регионах в России. Его целью является улучшение работы правоохранительных органов и повышение эффективности предоставления услуг населению. Проект «Полиция 2.0» включает в себя внедрение новейших технологий и инновационных подходов в работе с населением, такие как электронная очередь, онлайн-консультации, использование камер наружного наблюдения и дронов для мониторинга обстановки в наиболее критических районах. Реализация проекта началась в 2019 г., и она продолжается и сейчас на территории многих городов России.

³ Осознание деятельности электронной полиции: прагматичная оценка с использованием гибридных методов [Электронный ресурс]. – URL: <https://journals.sagepub.com/doi/abs/>

Однако необходимо принимать во внимание риски и угрозы, которые могут возникнуть в процессе цифровой трансформации. Необходимо добиваться качественной защиты информационных систем и данных, обеспечивая соблюдение прав граждан и защиту личной жизни.

Цифровая трансформация может внести качественные изменения в работу полиции, такие как:

1. Своевременный доступ к информации: цифровые технологии помогут ускорить процесс обработки и передачи информации между представителями правоохранительных органов, а системы электронного документооборота позволят сократить время обработки документов.

2. Более быстрое и точное расследование преступлений: цифровые технологии, такие как видеонаблюдение¹ и GPS, могут помочь в расследовании преступлений. Данные, полученные этим путем, могут помочь в сборе доказательств и предоставлении более точной информации для расследования преступлений.

3. Снижение преступности: использование технологий может привести к снижению количества преступлений. Видеонаблюдение и системы распознавания лиц² могут помочь идентифицировать преступников, а системы мониторинга помогут прогнозировать и проводить профилактические действия для предотвращения преступных действий.

4. Повышение безопасности сотрудников полиции: технологии могут помочь предотвратить нападения и повысить безопасность сотрудников правоохранительных органов. Например, при помощи носимых записывающих видеоприборов можно изучать реакцию граждан на действия сотрудников полиции.

5. Оптимизация процессов контрольно-пропускной системы: цифровые технологии могут использоваться для автоматизации процессов, выдачи разрешений и изготовления временных пропусков.

6. Широкий спектр применения: цифровые технологии могут помочь не только в борьбе с преступностью, но и в поддержании порядка в городе, например строительство системы мониторинга. С помощью современных систем видеонаблюдения, датчиков и других технологий можно следить за обстановкой в городах и на объектах, своевременно реагировать на возможные угрозы и преступления.

Это лишь часть примеров того, как цифровые технологии можно использовать в правоохранительной сфере для повышения эффективности работы правоохранительных органов и улучшению общественной безопасности.

¹ Согласно исследованию, проведенному в 2019 г. в г. Чикаго, применение видеонаблюдения приводит к снижению уровня преступности на улицах на 40% (The effectiveness of public surveillance video: Evidence from Chicago by B. Klein, S. Ranson, and M. Wachs. Crime and Delinquency, vol. 65, № 11 (2019), pp. 1427–1453).

² Исследование, проведенное в 2020 г. в США, показало, что система распознавания лиц помогла правоохранительным органам сократить время задержания на 10%, что повышает эффективность работы органов правопорядка (Facial recognition technology use by U.S. law enforcement agencies by the U.S. Government Accountability Office. U.S. Government Accountability Office (2020)).

В будущем полиция будет продолжать интенсивно внедрять новые цифровые технологии в свою деятельность, используя современные достижения науки и техники, такие как беспилотные автомобили, дроны, виртуальная и дополненная реальность и так далее. Однако необходимо не забывать о защите персональных данных и сохранении конфиденциальности информации при использовании этих технологий.

Следует подчеркнуть, что цифровые технологии не заменят людей, а будут оказывать им помощь, ускоряя и упрощая процессы деятельности полиции, повышая эффективность, точность и скорость принимаемых решений.

Библиографический список

1. Воскобойников И.В. Цифровая трансформация и полиция будущего // Вестник права. 2019. № 3. С. 13–17.
2. Горлин В.Б. Цифровизация правоохранительных органов: между вызовами и возможностями // Информационное право. 2017. № 1. С. 30–34.
3. Гусев В. Направления цифрового развития правоохранительных органов // Проблемы информационных технологий. 2018. № 3. С. 114–129.
4. Деньгин В.И. Цифровая трансформация и будущее правоохранительных органов // Актуальные проблемы права и управления. 2018. № 4. С. 96–101.
5. Джозефсон М. Цифровая трансформация в правоохранительной деятельности: существующее положение дел и перспективы развития // Journal of Contemporary Criminal Justice. 2018. Т. 34. № 3. С. 232–244.
6. Каменева Т.И. Цифровизация правоохранительных органов: вызовы и перспективы // Известия Волгоградского государственного университета. Серия 5. Юриспруденция. 2019. № 4. С. 181–186.
7. Сафронов А. Цифровая трансформация правоохранительной деятельности: место и роль искусственного интеллекта // Новости права. 2019. № 12. С. 57–63.
8. Широков А. Цифровая трансформация: вызовы и перспективы для правоохранительных органов // Criminal Justice Magazine. 2019. № 4. С. 32–38.
9. Шугар Л. Цифровизация правоохранительной деятельности: вызовы и перспективы // Вестник Белгородского государственного университета. Серия: Право. 2019. № 4. С. 69–74.
10. Bradford B., and Myhill, A. Police officers as crime victims: An under researched issue // Policing: An International Journal of Police Strategies & Management. 2016. Т. 40. № 4. P. 714–727.
11. Brown P. Digital policing and the future of law enforcement // Policing: An International Journal of Police Strategies & Management. 2017. Т. 40. № 2. P. 319–335.
12. Chan J. B. L., Chau M. and Kwok L. The digital transformation of policing and public safety: A global survey // Policing: A Journal of Policy and Practice. 2018. Т. 12. № 2. P. 239–250.
13. Krimmel T. J. Technology and policing // The Police Chief. 2018. Т. 85. № 9. P. 30–35.

14. Mawby R.I. Technology, surveillance and policing // International Journal of Police Science & Management. 2016. Т. 18. № 1. P. 21–31.

15. Ridgeway G., King D. The rise of big data policing // Society. 2018. Т. 55. № 3. P. 270–277.

АКТУАЛЬНЫЕ ВОПРОСЫ ДИСТАНЦИОННОГО ПРОИЗВОДСТВА ПО УГОЛОВНОМУ ДЕЛУ

**Захаров Д.С.,
Бельчиков Н.С.**

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в настоящее время дистанционное производство по уголовным делам становится более популярным видом проведения следственных действий. В работе рассматриваются исторические предпосылки необходимости применения дистанционных технологий в уголовном судопроизводстве, существующая реальность по использованию новых технологий, внесение изменений в имеющееся законодательство, а также высказывается мнение авторов по предложению новых законодательных инициатив. Следует не забывать об участниках уголовного судопроизводства. Наступила эра, когда отставание от технического прогресса влечет за собой заторможенность всех процессов жизнедеятельности человека, в том числе юридическую деятельность. Временные рамки прохождения уголовного дела на всех этапах производства далеко не короткая процедура. И в этой связи применение дистанционных технологий призвано кратно уменьшить не только временные затраты, но и финансовые. При этом следует отметить, что использование данных технологий ни в коем случае не может и не должно отразиться на качестве производства по уголовному делу.

Ключевые слова: уголовное производство, следственные действия, дистанционные технологии, электронные документы, информативность, электронная подпись.

TOPICAL ISSUES OF REMOTE CRIMINAL PROCEEDINGS

**Zakharov D.S.,
Belchikov N.S.**

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: currently, remote proceedings in criminal cases are becoming more popular type of investigative actions. The paper considers historical preconditions of necessity of application of remote technologies in criminal proceedings, current reali-

ty of application of new technologies, amendments to the existing legislation, as well as the authors' opinion on the proposal of new legislative initiatives. Participants of criminal proceedings should not be forgotten. We are in an era when the lag of technological progress entails the inhibition of all processes of human life, including legal activity. The time frame for the passage of a criminal case at all stages of the proceedings is far from a short procedure. And in this regard, the use of remote technologies is designed to reduce not only time costs, but also financial costs. At the same time it should be noted that the use of these technologies in no case can and should not affect the quality of criminal proceedings.

Keywords: criminal proceedings, investigative actions, remote technologies, electronic documents, informativeness, electronic signature.

Дистанционные технологии имеют определенно важное значение при рассмотрении уголовных дел. Данная версия возникла еще с того момента, когда в нашей стране начался период пандемии. Использование дистанционных средств стало более актуальным, в связи с чем в режиме видео-конференц-связи проводились следственные действия.

Сейчас информационные технологии в системе дистанционного производства частично имеют место. К примеру, конфискация электронных носителей информации при проведении следственных действий. Видео-конференц-связь используется в судебных заседаниях по разным делам: электронная подача ходатайств, заявлений и жалоб. Но этого очевидно недостаточно. Многие страны очень продвинулись в этом плане. Это Саудовская Аравия, Южная Корея, Республика Казахстан и другие.

Сегодня назрела необходимость создания интегрированной цифровой среды уголовного производства, включая координацию следственных процессов, использование технологических средств производства, сохранение изменений результатов в электронном виде.

В уголовных делах необходимо использовать удобную и надежную технологию для заверения процессуальных документов вместо обычных подписей участников уголовного производства, оценивать фактические данные, уголовные дела, использовать электронных помощников судей для формулирования обоснованных и соответствующих наказаний.

Если говорить о «цифровой зрелости» уголовно-процессуального права, то можно сказать, что отечественное уголовно-процессуальное законодательство в этом плане не претерпело качественных изменений. В последние годы в научной среде все активнее обсуждается вопрос цифровизации органов следствия, досудебной, прокурорской и судебной деятельности [1, с. 58].

Стремительное развитие дистанционных технологий способствовало расширению сферы исполнительного производства, в том числе уголовного.

Принцип законности состоит в постоянном исполнении положений Уголовно-процессуального кодекса (далее – УПК РФ) при составлении процессуальных актов. Уголовное преследование должно предполагать возможность существенного контроля за конституционными правами и гражданскими сво-

бодами и требовать от законодательной власти четкого определения допустимых границ такого контроля [1, с. 64].

Активное использование дистанционных технологий в рамках уголовного преследования началось в 2020 году, когда был введен режим повышенной готовности в ответ на пандемию коронавируса Covid-19.

Согласно Постановлению Президиума Верховного Суда Российской Федерации, Президиума Совета судей Российской Федерации от 18 марта 2020 г. судам поручено «рассматривать только неотложные дела». Сюда входят случаи, связанные с избранием, продлением, отменой или изменением меры пресечения по уголовным делам.

Обратим внимание на то, что до настоящего времени уголовно-процессуальное законодательство требовало непосредственного присутствия подсудимого в суде. А для тяжких преступлений террористического характера и во многих особых случаях закрытый порядок был определен законом (п. 6.1 ст. 241 УПК РФ).

В 2015 году Судебный департамент при Верховном Суде Российской Федерации сформулировал и утвердил правила организации использования видео-конференц-связи в федеральных судах общей юрисдикции [5].

Весной 2020 года суд ввел нормативные меры по содействию, созданию и обновлению инфраструктуры дистанционного пересмотра уголовных дел и материалов.

Как сообщила пресс-служба Мосгорсуда, в судах было установлено 93 системы видео-конференц-связи, в больницах, отделах внутренних дел и изоляторах временного содержания – 53.

В декабре 2022 года в УПК РФ были внесены изменения, которые предполагают возможность использования в судебных заседаниях систем видео-конференц-связи, а также предоставления в электронном виде в суд документов. При этом п. 6.1 ст. 241 УПК РФ был отменен [6].

Следует отметить, что не каждый желающий подать заявление в суд владеет достаточными знаниями в области компьютерных технологий и не всегда обладает знаниями об электронной подписи и возможностях ее использования. Это уже вопрос компьютерной грамотности населения. Не следует допускать огромного дисбаланса между прогрессом в области применения компьютерных технологий в государственных сферах и недостаточной компьютерной грамотности населения.

Отметим, что существенным изменением в уголовно-процессуальном законодательстве должна стать подготовка электронных уголовных дел с целью заменить традиционный формат на бумажном носителе [2, с. 162].

Современные электронные носители, такие как USB-накопители и внешние жесткие диски, могут использоваться как носители электронных материалов уголовных дел.

Поэтому важной задачей на сегодняшний день является предоставление процессуального статуса электронным документам по уголовному производству.

Тем не менее, среди категории использования применения дистанционного производства по уголовным делам принято считать обеспечение доказа-

тельств и общей системы устного рассмотрения в суде. Подтверждение этих показаний очень важно, поскольку показания свидетелей и потерпевших всегда играли очень важную роль в доказательной системе уголовных дел [1, с. 62].

Есть много способов это исправить. Во-первых, возник вопрос установления допрашиваемого лица.

Эксперты говорят, что биометрические данные участников суда понадобятся, чтобы передать лицо и голоса во время судебных процессов с помощью технологий.

Поскольку дача показаний допрашиваемого лица проходит вне зала судебного заседания, необходимо установить характер местонахождения свидетеля или потерпевшего.

Требования относительно взятия показаний в том или ином месте, используемых технических средствах и окружения допрашиваемого лица предусмотрены законодательно. В случае дистанционного процесса в этом случае важно решить, что делать, если общение с субъектом внезапно прервано по причинам технического или иного характера.

Тем не менее, определим существенные направления в развитии дистанционных технологий [2, с. 162]:

1) система планомерного видоизменения всего процесса расследования, в частности область использования технических средств в целях хранения и обработки целого ряда основных результатов в электронной форме;

2) применение в современном уголовном производстве систематически надежной технологии для заверения процессуальных документов участников указанного процесса;

3) продолжение внедрения системы «Электронный уголовный процесс», апробируемый в некоторых субъектах нашей страны;

4) непосредственное применение ряда дистанционных форм судопроизводства на различных стадиях, включая всех участников данного производства;

5) возможность для потерпевших осуществления контроля за ходом проведения уголовного дела через Интернет.

Применение дистанционных технологий может быть осуществлено также и в том случае, если имеется электронная подпись у гражданина. Дистанционные технологии позволяют осуществлять полноценный сбор, поиск, обнаружение информации о конкретном событии, а также определять в точности наличие или характерное отсутствие тех или иных обстоятельств, подлежащих доказыванию.

Сотрудники должны быть полноценно обучены дистанционным технологиям, а также знать информационные системы и специализированные компьютерные программы.

Технологические средства копирования, хранения и передачи электронной информации в ближайшем будущем устранят необходимость в бумажных документах уголовного дела, а значит, электронный документооборот может стать эксклюзивным.

Библиографический список

1. Абдулвалиев А.Ф. Предпосылки и перспективы внедрения электронной формы уголовного дела в деятельность судебных органов // Право и политика. 2013. № 1. С. 58–65.
2. Макарова О.В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журнал российского права. 2019. № 2(266). С. 159–168.
3. Соколов Ю.Н. Допустимость рассмотрения материалов уголовного дела в электронной форме // Информационное право. 2017. № 1. С. 28–33.
4. Шереметьев И.И. Электронное уголовное дело: что это такое и пути его создания // Lex Russica (Русский закон). 2020. Т. 73. № 10 (167). С. 81–90.
5. Приказ Судебного департамента при Верховном Суде Российской Федерации от 28 декабря 2015 г. № 401 (ред. от 30.12.2020) «Об утверждении Регламента организации применения видео-конференц-связи при подготовке и проведении судебных заседаний» // СПС «КонсультантПлюс» (дата обращения: 20.04.2023).
6. Федеральный закон от 29.12.2022 № 610-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 20.04.2023).

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ СЕТЕВЫХ РЕСУРСОВ В ЦЕЛЯХ ДЕАНОНИМИЗАЦИИ ПРЕСТУПНИКОВ, СОВЕРШАЮЩИХ НЕЗАКОННЫЙ ОБОРОТ НАРКОТИКОВ В ВИРТУАЛЬНОЙ СРЕДЕ

Зинченко Д.С.

(Белгородский юридический институт МВД России имени И.Д. Путилина),
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье анализируются особенности противодействия незаконному обороту наркотиков, совершаемому с использованием информационно-коммуникационных технологий. На основе изучения функционирования интернет-пространства раскрыты основные способы деанонимизации преступников, совершающих незаконный оборот наркотиков в виртуальной среде. Автор предложены конкретные меры совершенствования деятельности по использованию возможностей сетевых ресурсов с целью установления личности преступника.

Ключевые слова: незаконный оборот наркотиков, наркопреступность, деанонимизация, преступник, виртуальная среда, сетевые ресурсы, информационные технологии.

USING THE CAPABILITIES OF NETWORK RESOURCES IN ORDER TO DEANONYMIZE CRIMINALS WHO COMMIT DRUG TRAFFICKING IN A VIRTUAL ENVIRONMENT

Zinchenko D.S.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia),
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: the article analyzes the features of countering drug trafficking committed using information and communication technologies. Based on the study of the functioning of the Internet space, the main ways of deanonymization of criminals who commit drug trafficking in a virtual environment are revealed. The author suggests specific measures to improve the use of the capabilities of network resources in order to establish the identity of the criminal.

Keywords: drug trafficking, drug crime, deanonymization, criminal, virtual environment, network resources, information technology.

Незаконный оборот наркотиков является одним из самых прибыльных видов деятельности организованных преступных групп. Наркопреступность создает угрозу для политического и социально-экономического развития стран во всем мире, подрывает безопасность и стабильность деятельности всех сфер общества [1, с. 31]. В условиях функционирования цифровой экономики на мировом рынке нелегальный оборот наркотиков трансформируется и переходит на новый этап развития. В результате происходит их цифровая трансформация, которая заключается в переходе от «традиционного» оборота наркотиков к бесконтактному, осуществляемому на различных электронных платформах.

Массовое использование преступными сообществами, занимающимися незаконным оборотом наркотиков, «теневого сегмента» позволяет им сохранять свою анонимность и приватность своих противоправных действий. В этой связи субъектами по противодействию наркопреступности проводится комплекс мероприятий по изучению организационных, тактических и технических возможностей по деанонимизации преступников, совершающих незаконный оборот наркотиков в виртуальной среде.

Под деанонимизацией необходимо понимать комплекс оперативных исследований и технических мер по установлению личности пользователей сетевых ресурсов для решения оперативно-разыскных задач [3, с. 171].

Изучение специфики и особенностей функционирования виртуального пространства показывают, что, несмотря на использование наркопреступниками теневой части Интернета, позволяющей им скрываться, существуют определенные возможности обработки сетевых ресурсов, которые могут деанонимизировать преступников, совершающих незаконный оборот наркотиков в виртуальной среде. Эти возможности состоят из трех основных способов.

1. *Анализ влиятельной активности на соединение.* При использовании сети практически во всех случаях на IP-устройствах (маршрутизаторах, комму-

таторах 3-го уровня) работает протокол NetFlow. Система NetFlow – это открытый сетевой протокол, также известный как стандарт IPFIX, предназначенный для учета и анализа сетевого трафика [5]. Анализ данных системы NetFlow позволяет визуализировать не только протоколы TCP/IP (например, IP-адрес источника, протокол, порт), но и дополнительную информацию о входящих и исходящих интерфейсах, сетевом адресе источника, DSCP, области автономных систем в протоколе BGP и др.

Однако, несмотря на очевидную простоту и эффективность этого протокола, при его анализе в «темной Сети» из-за большой доли трафика протокол может генерировать большое количество портов существования.

2. *Анализ влияния пользователей сетевых ресурсов на браузер.* Для доступа к «темной Сети» злоумышленникам требуется использование специализированного браузера «темной сети». При использовании такого браузера наркопреступникам необходимо пользоваться специальными технологиями, превращающими браузер в оконечный терминал видео-конференц-связи, например стандартом WebRTC, который описывает передачу потоковых данных между браузерами в режиме реального времени [2, с. 231]. Однако такие технологии являются уязвимыми для браузеров, поскольку WebRTC определяет их реальные IP-адреса, а сохранить анонимность не поможет ни прокси, ни использование браузера «темной сети» [4]. Поэтому исследование таких технологий также позволяет деанонимизировать преступников, совершающих незаконный оборот наркотиков в виртуальной среде. Но в связи с тем, что жизненный цикл кодеков уязвимостей, например того же стандарта WebRTC, составляет всего от нескольких недель до нескольких месяцев, данный способ по деанонимизации наркопреступников в «темной Сети» не всегда эффективен.

3. *Анализ сетевой деятельности пользователей Сети.* В основе этого способа заложено базовое использование тегов Canvas при помощи JavaScriptin на платформе HTML5, позволяющих создать разные объекты, рисунки, фотокомпозиции. Ключевой особенностью является то, что различные браузеры в зависимости от аппаратных и программных компонентов, операционной системы и иных конфигураций представляют изображения по-разному. В связи с чем, используя этот способ для деанонимизации наркопреступников, с помощью параметров изображения представляется возможным идентифицировать браузер, его аппаратную и программную среду.

Таким образом, использование возможностей современных информационных технологий позволяет успешнее противостоять преступности. Безусловно, злоумышленники используют всевозможные методы для своей анонимности и конфиденциальности. Однако при использовании компьютерных технологий для совершения преступлений чаще всего остаются виртуальные следы. Следовая картина имеет свою специфику и традиционные способы их выявления будут не всегда достаточно эффективны.

В этой связи возникает необходимость в использовании новых методов и средств выявления и фиксации конкретного цифрового следа, в том числе и использование возможностей сетевых ресурсов. А для совершенствования деятельности по деанонимизации преступников, совершающих незаконный оборот

наркотиков в виртуальной среде, и преступников, использующих информационно-коммуникационные технологии, в целом предлагаем внести дополнения в федеральный проект «Информационная безопасность» национального проекта «Национальная программа «Цифровая экономика Российской Федерации», утвержденный протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 года № 7, содержащие мероприятия по техническому перевооружению подразделений органов внутренних дел, занимающихся противодействием преступности в сфере IT-технологий, оснащению их современными программно-техническими средствами в совокупности с методами искусственного интеллекта и обработки больших объемов неструктурированных данных.

Библиографический список

1. Зинченко Д.С. Мессенджер-маркетинг как инновационный способ вовлечения несовершеннолетних в незаконный оборот наркотиков / Проблемы юриспруденции и педагогики высшей школы в работах молодых ученых: сборник материалов Всероссийской научно-практической конференции, Белгород, 30 ноября 2022 года. Выпуск 3. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. С. 31–34.

2. Куликова Е.М. Разработка сервиса для прохождения видеointервью / Прикладная математика XXI века: современные проблемы математики, информатики и моделирования: материалы Всероссийской научно-практической конференции, Краснодар, 24–26 апреля 2019 года. – Краснодар: Краснодарский ЦНТИ – филиал ФГБУ «РЭА» Минэнерго России, 2019. С. 229–236.

3. Тимофеев С.В. Деанонимизация пользователя сети интернет как метод оперативно-розыскного противодействия наркопреступности // Юристы-Правоведь. 2020. № 2(93). С. 170–174.

4. Что такое WebRTC? [Электронный ресурс]. – URL: https://trueconf.ru/webrtc.html?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 10.08.2023).

5. Что такое протокол NETFLOW и как он используется [Электронный ресурс]. – URL: <https://komsvenenergy.ru/solution/> (дата обращения: 31.07.2023).

ВОЗМОЖНОСТИ И НЕДОСТАТКИ СЕРВИСОВ ИСОД МВД РОССИИ

Ивануха И.С.

(Омская академия МВД России)

Аннотация: сервисы ИСОД МВД России, предназначенные для сотрудников федеральных государственных гражданских служащих и работников центрального аппарата МВД России, территориальных органов МВД России, а также иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел, направлены на подготовку, обработку, хранение и использование документов (в том числе и документов в электронной форме), образующихся в ходе деятельности органов внутренних дел. В статье рассмотрены основные повседневные сервисы, сервисы межведомственного взаимодействия и оказания государственных услуг, а также ключевые сервисы, используемые для обеспечения оперативно-служебной деятельности оперативных подразделений МВД России. Автор акцентирует внимание на возможности и недостатки некоторых сервисов, анализирует развитие сервисов. В статье также представлены авторские методы по решению проблемы с обновлением сервиса СУДИС-М.

Ключевые слова: сервисы ИСОД МВД России, СУДИС-М, операционная система Windows, операционная система Astra Linux.

OPPORTUNITIES AND DISADVANTAGES OF THE ISOD SERVICES OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Ivanukha I.S.

(Omsk Academy of the Ministry of the Interior of Russia)

Abstract: the ISOD services of the Ministry of Internal Affairs of Russia intended for employees of federal state civil servants and employees of the central office of the Ministry of Internal Affairs of Russia, territorial bodies of the Ministry of Internal Affairs of Russia, as well as other organizations and divisions created to perform tasks and exercise powers assigned to internal affairs bodies, are aimed at the preparation, processing, storage and use of documents (including and documents in electronic form), formed in the course of the activities of the internal affairs bodies [1]. The article discusses the main everyday services, services of interdepartmental interaction and the provision of public services, as well as key services used to ensure the operational performance of operational units of the Ministry of Internal Affairs of Russia. The author focuses on the possibilities and disadvantages of some services. The author analyzes the development of services. The article also presents the author's methods for solving the problem with updating the SUDI S-M service.

Keywords: ISOD services of the Ministry of Internal Affairs of Russia, SUES-M, Windows operating system, Astra Linux operating system.

Информационные технологии за последние 30 лет ушли далеко вперед. Технический прогресс, отсутствие единства и системности в имеющихся базах данных побудило Министерство внутренних дел Российской Федерации создать систему, которая бы оптимизировала работу, упростила ее, вместила в себя все необходимые данные для оперативного поиска информации и поспособствовала увеличению раскрываемости.

В итоге в 2012 году вышел приказ МВД России от 30 марта 2012 г. № 205 «Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах». Данной работой занялась компания АТ Consulting, и в 2013 году были спроектированы и разработаны первые сервисы, в 2014 началась разработка и создание инфраструктуры, а затем – эксплуатация в опытном режиме. В декабре 2014 года коллегия МВД России решила дальше развивать систему информационного обеспечения деятельности МВД России¹. В 2015 году начался активный процесс внедрения и обучения сотрудников. В 2016 году АТ Consulting представило вариант ИСОД, но он не оправдал ожиданий руководства МВД России и был отправлен на доработку и после внесенных изменений вошел в эксплуатацию. В 2019 сервис году начал активно внедряться и улучшаться.

Подход к внедрению сервисов был основан на принципе автоматизации процесса с помощью ведомственного информационного справочного портала, было применено использование дистанционного обучения с набором обучающих материалов, инструкций по использованию сервиса, демонстрационных роликов. В каждом регионе Российской Федерации консультанты проводят обучение пользователей и настройку рабочих мест.

ИСОД МВД России состоит из различных сервисов, основной – это СУ-ДИС – сервис управления доступом к информационным системам и ресурсам. Также существует разделение на сервисы обеспечения повседневной деятельности, на специальные сервисы обеспечения оперативно-служебной деятельности и на сервисы межведомственного взаимодействия и оказания государственных услуг.

В качестве повседневных сервисов выступают:

СЭД – сервис электронного документооборота, предназначен для более оперативного движения документов, достаточно важной части работы органов внутренних дел, позволяет руководству в более быстром порядке назначать исполнителей документов, а последним – осуществлять более быструю отправку исполненного документа.

СЭП – сервис электронной почты, призван обеспечить повышение оперативности и качества работы по координации и внутреннему взаимодействию между сотрудниками ведомства, снижению трудозатрат и сокращению издержек на выполнение функций обмена информацией, содействию при создании условий для взаимодействия в электронном виде и включает в себя:

¹ Решение коллегии Министерства внутренних дел Российской Федерации от 5 декабря 2014 г. № 3 км/1 «Об основных направлениях развития информационного обеспечения деятельности МВД России» // СПС «КонсультантПлюс».

1. Почтовый ящик. Позволяет получать и отправлять письма, устроен таким образом, что дает возможность осуществлять обмен сообщениями не только внутри ИСОД МВД России, но и в Интернете. Это позволяет оперативно отправлять запросы в организации, работать с обращениями граждан, а также получать служебную и деловую корреспонденцию.

2. Задачи. Позволяют создавать, изменять, удалять задания, предоставлять доступ к своим и подписываться на списки заданий других пользователей.

3. Календарь. Позволяет создавать, изменять, удалять и просматривать события, предоставлять доступ к своим и получать доступ к событиям других пользователей.

4. Контакты. Хранят собственные контакты пользователя, отображают корпоративную адресную книгу, позволяют предоставить доступ к своим контактам, а также подписаться на контакты других пользователей;

5. Файлы. По своему назначению являются простым файлообменником и имеют емкость 300 мегабайт.

СВКС-М – система видео-конференц-связи МВД России. Предназначена для оперативной связи между сотрудниками МВД России, а также для ускорения процесса принятия управленческих решений. СВКС-М поддерживает 5 вариантов видеоконференций:

1. Видеозвонок – общение двух человек.
2. Групповая видеоконференция – общение нескольких человек.
3. Симметричная конференция – общение до 16 человек без ведущего.
4. Ассиметричная конференция – общение до 16 человек с ведущим.
5. Ролевая конференция – общение до 250 человек с несколькими ведущими.

СУДИС – сервис управления доступом к информационным системам и ресурсам. Предназначен для централизованного управления доступом пользователей к сервисам ИСОД МВД России [3].

СУДИС обеспечивает выполнение следующих функций:

1. Протоколирование событий безопасности сервисов ИСОД МВД России.
2. Управление реестрами пользователей и сервисов ИСОД МВД России.
3. Идентификация пользователей ИСОД МВД России.
4. Назначение и отзыв полномочий пользователей и сервисов ИСОД МВД России.

СУДИС позволяет:

1. Организовать управление полномочиями пользователей, имеющих доступ к сервисам ИСОД.
2. Организовать управление полномочиями сервисов, имеющих доступ в ИСОД.
3. Обеспечить доступ к ресурсам по электронной подписи [2].

Но даже при всех имеющихся в ИСОД МВД России средствах, обеспечивающих безопасность, сведения, составляющие государственную тайну, в нем не передаются. В 2021 была проведена аттестация по требованиям безопасности информации ФСТЭК для работы с документами с пометкой ДСП, но до сих пор

не поступило приказа, разрешающего обработку и передачу по сети ИСОД такого рода информации.

ВИСП – ведомственный новостной портал, служащий для автоматической установки клиентской части программного обеспечения.

Сервисы межведомственного взаимодействия и оказания государственных услуг:

Ретроспектива – единый банк данных архивной информации.

Модернизация ИБД – интегрированный банк данных.

СЦУО – система централизованного учета оружия.

СПГУ – сервис предоставления государственных услуг.

Сервисы обеспечения оперативно-служебной деятельности.

Следопыт-М – информационно-поисковый сервис.

ФИС ГИБДД-М – федеральная информационная система ГИБДД МВД России.

ЦИАДИС МВД – банк отпечатков пальцев.

Рассмотрим ключевые сервисы для обеспечения оперативно-служебной деятельности оперативных подразделений МВД России.

Следопыт-М – информационно-поисковый сервис, позволяет допущенному к его использованию сотруднику получить все доступные данные о гражданине, используя простой набор данных, например ФИО, серию и номер паспорта или водительского удостоверения, ИНН и т.д. Из особенностей: ведется полный журнал аудита, т.е. любое действие регистрируется в автоматическом порядке и запись о действии включает в себя полные данные о сотруднике, дату и время проверки, лицо, которое он запросил. Сервис ищет информацию везде, куда есть возможность обратиться к чему разрешен доступ [4]. Из недостатков можно выделить низкие вычислительные мощности при выполнении запросов.

Сервис «Паутина». Предназначен для совершенствования деятельности органов внутренних дел Российской Федерации по предупреждению, пресечению и раскрытию преступлений, предупреждению и пресечению административных правонарушений, выявлению похищенных или угнанных транспортных средств, транспортных средств участников дорожного движения, скрывшихся с мест дорожно-транспортных происшествий, автоматизации деятельности подразделений Госавтоинспекции по оформлению административных правонарушений, зафиксированных с применением средств автоматической фото-, видеофиксации.

«Паутина» – универсальный сервис поиска автотранспорта, использует данные со всех камер Омской области. Информация поступает из большинства баз России и позволяет, например, сотруднику дорожно-патрульной службы, пользуясь базой сотрудников ФССП, посредством камер выявлять в потоке злостных нарушителей ПДД, машины, не стоящие на учете, и даже наличие алиментов и долгов у собственника транспортного средства. Также этот сервис позволяет устанавливать так называемые флажки или ориентировки, это бывает очень полезно при расследовании преступлений, связанных с угонами транспортных средств, или поступлении информации о том, что правонарушитель передвигается на автотранспорте. Но в этой системе есть несколько недостатков:

– сотрудники федеральной службы судебных приставов предоставляют списки исполнительных производств примерно за 2–3 дня до рейда вместе с сотрудниками дорожно-патрульной службы и зачастую эти данные на момент остановки транспортного средства являются устаревшими, и гражданину, оплатившему штраф, приходится доказывать, что он уже оплачен, как итог – потеря времени сотрудниками ДПС и потеря времени гражданина;

– ориентировки (флажки) распространяются только внутри подразделения, это значит, что, например, метка, поставленная сотрудниками УГРО, не будет видна сотрудникам ДПС и наоборот. С одной стороны, это обеспечивает защиту от утечек информации о проводимых операциях и планах-перехватах, но и в то же время усложняет розыск транспортного средства;

– ориентировки (флажки) выставляют лишь сотрудники ЦАФАП, в итоге получается задержка до нескольких часов и теряется одно из важнейших свойств информации – оперативность;

– ограниченный срок хранения информации – сведения о перемещениях автотранспорта и фотографии хранятся не более 3 месяцев. К тому же хранятся данные только о 1 500 000 проездах в день, если в течение дня количество проездов превышает это число, то происходит перезапись начиная с первого проезда под камерой;

– ЦАФАП удаляет ориентировки вручную 1 раз в месяц. Ориентировка выставляется системой автоматически при наличии 4 и более нарушений ПДД. А сама проблема в том, что водитель мог, например, несколько дней назад оплатить полученные штрафы, и если его останавливают для выяснения причин неуплаты штрафов и оказывается, что они уже давно оплачены – время потеряно. Таких ориентировок в федеральной базе данных может выставляться ограниченное число – 4 500, это очень мало, учитывая то, сколько существует нарушителей ПДД;

– система сопровождения заключается в том, что она помогает дежурному отвлечься от неотлучного слежения за постоянно меняющейся обстановкой и сконцентрироваться на более важных задачах и максимально эффективно их выполнять. Она, распознав нештатную ситуацию, сигнализирует об этом дежурному, который оценивает ситуацию, либо подтверждая наличие нештатной ситуации, либо опровергая. Распознав объект – человека, группу людей – она сопровождает его, создавая условия для распознавания, однако проблема в том, что сопровождение проходит в течение 10–20 сек, а желательно – 30–40 секунд;

– выгрузка материалов фотофиксации правонарушений осуществляется в количестве до 300 штук.

Также в последнее время наблюдаются повсеместные сбои в работе ИСОД МВД России, связано это с тем, что на центральных серверах ИСОД произошёл переход на СУДИС-М, тогда как на компьютерах в ОВД установлен СУДИС 1-го поколения и в связи с этим авторизация в ИСОД на данных компьютерах невозможна. Проблема перехода в большей части носит организационный характер, и на это есть несколько причин:

– технические специалисты в регионах не были готовы к переходу, а срок перехода установили до 15 мая включительно. Например, в Омской области у

сотрудников ОВД примерно 10 000 рабочих мест и их обслуживает 2–3 человека на всю область;

– рабочие станции также не были готовы, поскольку для СУДИС используется операционная система Windows 7, а для работы в СУДИС-М нужна операционная система Windows 10 или операционная система Astra Linux версии 1.6 либо 1.7. Проблема также в том, что Windows 10 в России признана иностранным программным обеспечением и поэтому не может быть использована в деятельности ОВД, а с Astra Linux версии 1.6 возникает ряд ошибок и проблем, в связи с тем, что в МВД России не была произведена закупка лицензий программного обеспечения Astra Linux версии 1.7, при работе с которой проблем по настройке не возникает, поэтому специалисты не могут наладить работу ИСОД на местах в короткие сроки.

В заключение отметим, что, несмотря на ключевые недостатки основного сервиса для функционирования оперативных подразделений, безусловно, ИСОД МВД России является решением почти для всех повседневных и служебных задач. Данная система постоянно улучшается и по сей день активно разрабатываются новые сервисы, что очень важно для сотрудников МВД России, новые разработки позволяют им незамедлительно получать информацию о различных событиях, зарегистрированных различными комплексами, и вести их незамедлительную обработку. Недавно вышедший приказ МВД России от 28 декабря 2022 г. № 1102 «О вопросах эксплуатации специального программного обеспечения «Единая информационно-аналитическая система обеспечения безопасности дорожного движения Министерства внутренних дел Российской Федерации», свидетельствует о том, что система сервисов развивается, и согласно приказу новый сервис должен быть включен в состав сервисов ИСОД МВД России с 1 июля 2023 г.

Библиографический список

1. Процессы информационного обмена в деятельности правоохранительных органов: современное состояние и перспективы совершенствования: сборник научных статей / под ред. Л.Д. Матросовой. – Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2015. – 56 с.
2. Сервис электронной почты МВД России [Электронный ресурс]. – URL: <https://obrazovanie-gid.ru> (дата обращения: 15.04.2023).
3. Локнов А.И., Примакин А.И. Безопасность применения облачных технологий в деятельности сотрудников органов внутренних дел / Региональная информатика и информационная безопасность: сборник трудов, Санкт-Петербург, 23–25 октября 2019 года. Выпуск 7. – Санкт-Петербург, 2019. С. 178–182.
4. Меняйло Л.Н., Алексеева П.В. Подсистема, обеспечивающая информационную безопасность в ИСОД МВД России / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 7-й Всероссийской научно-практической конференции, Белгород, 22 мая 2020 года. – Белгород, 2020. С. 141–143.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ СЕРВИСОВ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Калашникова А.А.,

Ершова Е.Ю.

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: данная статья посвящена изучению правового регулирования применения электронных сервисов в деятельности правоохранительных органов. В статье рассмотрены основные аспекты применения электронных сервисов в правоохранительной деятельности, а также описаны проблемы, связанные с использованием таких сервисов в рамках существующего законодательства России. Проведен анализ законодательства о защите персональных данных, а также рассмотрена практика применения электронных сервисов правоохранительными органами. Особое внимание уделено вопросам безопасности и конфиденциальности информации, а также проблемам, связанным с возможным злоупотреблением правоохранительными органами своими полномочиями при использовании электронных сервисов.

В статье также предложены рекомендации по улучшению правового регулирования применения электронных сервисов в деятельности правоохранительных органов, включая изменения в законодательстве, улучшение процедур контроля и отчетности, а также обучение сотрудников правоохранительных органов в области использования электронных сервисов.

Ключевые слова: правовое регулирование, правоохранительные органы, электронные сервисы.

LEGAL REGULATION OF APPLICATION OF ELECTRONIC SERVICES IN LAW ENFORCEMENT BODIES' ACTIVITY

Kalashnikova A.A.;

Ershova Yu.Yu.

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: this article is devoted to the study of the legal regulation of the application of electronic services in the activities of law enforcement agencies. The main aspects of application of electronic services in law enforcement activity are examined, and also problems connected with the use of such services in the framework of existing legislation of Russia are described. The analysis of legislation on personal data protection was carried out and the practice of using electronic services by law enforcement agencies was examined. Particular attention was paid to security and confidentiality of information, as well as to problems associated with possible abuse of power by law enforcement agencies when using electronic services.

The article also offered recommendations on how to improve the legal regulation of the use of electronic services in the activities of law enforcement agencies, in-

cluding changes in legislation, improving procedures for monitoring and reporting, as well as training law enforcement officers in the use of electronic services. The purpose of the study is to analyze the legal regulation of application of electronic services in the activities of law enforcement agencies and identify opportunities for improvement.

Keywords: legal regulation, law enforcement agencies, electronic services.

Электронные сервисы в деятельности правоохранительных органов — это совокупность информационно-технических средств и услуг, которые предоставляются государственными органами правоохранительной системы с использованием электронных технологий.

Современные правоохранительные органы активно используют различные исследуемые сервисы для выполнения своих задач и обеспечения безопасности граждан [3, с. 17]. Среди них выделяют:

1. Электронные базы данных. Они представляют собой мощные инструменты для хранения, обработки и анализа больших объемов информации, таких как данные о преступлениях, досье на подозреваемых и обвиняемых, информация о ранее совершенных правонарушениях и т.д. Такие базы данных позволяют быстро находить нужную информацию и упрощают работу правоохранительных органов.

2. Системы видеонаблюдения. Видеонаблюдение является важным инструментом для обеспечения безопасности на улицах, в общественных местах, на транспорте и других местах. Такие системы могут использоваться для предотвращения преступлений, выявления и расследования происшествий и т. п.

3. Системы автоматизации работы правоохранительных органов. Такие системы включают в себя различные инструменты, например, автоматическое распознавание номерных знаков автомобилей, системы распознавания лиц и другие. Данные инструменты помогают правоохранительным органам быстро и эффективно выполнять свои задачи.

4. Системы связи и обмена информацией. Для эффективной работы правоохранительных органов необходимо быстро передавать информацию между сотрудниками и различными подразделениями. В такой связи используются различные системы связи и обмена информацией, такие как радиосвязь, электронная почта, СМС-сообщения и другие.

5. Электронные сервисы для работы с населением. Например, электронные жалобы и заявления, которые можно подать через Интернет. Также некоторые правоохранительные органы создают мобильные приложения для быстрого обращения граждан в случае необходимости.

Каждый год появляются новые технологии, которые могут помочь улучшить работу правоохранительных органов и повысить безопасность граждан. Важно отметить, что применение электронных сервисов в работе органов внутренних дел (далее – ОВД) должно соответствовать установленным нормам законодательства и создавать комфортную среду для защиты прав и свобод граждан.

Данные электронные сервисы способны совершенствовать следующие характеристики:

1. Автоматизация процессов. Позволяет автоматизировать многие процессы, связанные с деятельностью правоохранительных органов, что увеличивает их эффективность и сокращает время на выполнение задач.

2. Ускорение информационного обмена. Электронные сервисы способствуют быстрому и безопасному обмену информацией между различными правоохранительными органами, а также субъектами деятельности, с которыми ведется работа.

3. Улучшение качества обслуживания. Новые технологии упрощают процедуру получения необходимой информации и услуг, а также сократить время на выполнение различных административных процедур, что улучшает качество обслуживания граждан и субъектов деятельности.

4. Безопасность. Системы защиты обеспечивают высокий уровень безопасности обработки и передачи конфиденциальной информации, что является важным фактором в деятельности правоохранительных органов.

5. Экономическая эффективность. Внедрение электронных сервисов позволяет сократить затраты на обслуживание и управление информацией, что повышает экономическую эффективность деятельности правоохранительных органов.

Правовое регулирование электронных сервисов в деятельности ОВД в России основывается на ряде нормативно-правовых актов, которые устанавливают правила их использования [4, с. 81]. Один из основных законов в этой сфере – это Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который устанавливает правила использования информационных технологий в государственной и муниципальной деятельности, а также организации защиты информации. Кроме того, существует ряд правительственных постановлений, распоряжений и приказов, которые регулируют деятельность правоохранительных органов в сфере электронных сервисов. Важным является упоминание и соответствие деятельности Федеральному закону «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (последняя редакция 29 декабря 2022 года), который определяет правила сбора, хранения, обработки и использования информации в рамках оперативно-розыскной деятельности. Этот закон устанавливает обязательные требования к защите информации, получаемой и обрабатываемой при оперативно-розыскной деятельности, включая электронные сервисы [2, с. 25].

В целом нормативно-правовые акты устанавливают правила использования электронных сервисов правоохранительными органами в России с учетом необходимости обеспечения защиты прав и свобод граждан. Законодательная база регулирует вопросы доступа к информации, обеспечение конфиденциальности персональных данных граждан, защиту от незаконного доступа к информации, получение и использование информации в рамках оперативно-розыскной деятельности и другие аспекты использования электронных сервисов в деятельности правоохранительных органов.

Важно отметить, что в связи с быстрым развитием технологий и электронных сервисов регулирование в этой сфере постоянно совершенствуется и дополняется новыми нормативными актами. Это свидетельствует о том, что государство уделяет большое внимание обеспечению защиты прав и свобод граждан в электронном пространстве, а также важности использования электронных сервисов в деятельности правоохранительных органов для обеспечения безопасности граждан и общества в целом.

Библиографический список

1. Комлев М.С. Практика корпоративного и нормативно-правового регулирования использования информационных технологий / Молодежь, наука и цивилизация: материалы международной студенческой научной конференции. – Красноярск: Юридический институт СФУ, 2021. С. 135–137.
2. Гена Е.Е. Правовое регулирование в сфере информационных технологий: сравнительный анализ законодательства США и России // Право и экономика. 2022. № 5(411). С. 24–29.
3. Страхов А.А., Слесарева Е.А., Задохина Н.В. Информационные технологии в ОВД. Основные термины и определения: словарь. – Москва: МосУ МВД России имени В.Я. Кикотя, 2020. – 103 с.
4. Комардина А.А. Применение информационных технологий и возможностей цифровизации в деятельности сотрудника ОВД // Вестник студенческой науки. 2020. № 4. С. 79–82.

РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕДОТВРАЩЕНИИ ПОЛИТИЧЕСКИХ ЭКСТРЕМИСТСКИХ ДЕЙСТВИЙ

**Калашникова А.А.,
Орлов М.А.**

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: данная статья посвящена информационным технологиям, которые предотвращают политические экстремистские действия. В работе проведен анализ современных методов предотвращения экстремистских действий с помощью информационных технологий, включая мониторинг социальных сетей, анализ данных, использование искусственного интеллекта и машинного обучения. В статье также рассмотрены предложения по их улучшению, включая изменения в законодательстве, улучшение процедур контроля и отчетности, а также обучение сотрудников правоохранительных органов в области использования информационных технологий. В исследовании отмечается, что использование информационных технологий в борьбе с экстремизмом имеет большой потенциал для предотвращения этих действий, но требует более четкого и

обоснованного правового регулирования. Цель данной научной статьи – проанализировать роль информационных технологий в предотвращении экстремистских действий.

Ключевые слова: информационные технологии, экстремизм, политические действия.

THE ROLE OF INFORMATION TECHNOLOGY IN PREVENTING POLITICAL EXTREMISM

**Kalashnikova A.A.,
Orlov M.A.**

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: this article is devoted to information technologies which prevent political extremist actions. It analyzes modern methods of prevention of extremist actions with the help of information technologies, including monitoring of social networks, data analysis, use of artificial intelligence and machine learning. The article also considers how to improve them, including changes in legislation, improved monitoring and reporting procedures, and training of law enforcement officials in the use of information technology. The study notes that the use of information technology in combating extremism has great potential to prevent these acts, but requires clearer and more sound legal regulation. The purpose of this scientific article is to analyze the role of information technologies in preventing extremist actions.

Keywords: information technologies, extremism, political actions.

В современном обществе информационные технологии играют ключевую роль в коммуникации и обмене данными между людьми. Они широко используются в политической сфере для поддержки демократических процессов, предотвращения экстремистских действий и противодействия киберугрозам.

Политические процессы в нашей жизни сегодня стали чрезвычайно динамичными, и многие решения и действия принимаются на основе информации, которая поступает из различных источников. В этом контексте информационные технологии играют важную роль в сборе, обработке и распространении информации [1, с. 243].

Однако использование информационных технологий в политической сфере может стать источником опасных явлений, таких как экстремизм и политические действия, направленные на нарушение закона. Политические экстремистские действия – это деятельность, направленная на насилие, устранение или изменение законных политических институтов и процедур.

Существует множество форм политического экстремизма, которые могут проявляться в различных действиях [2, с. 215]. Некоторые из них включают:

1. Терроризм – насильственные действия с целью заставить правительство или общество выполнить требования экстремистов, или для привлечь внимание к своим целям.

2. Пропаганда – использование искажения фактов и обмана для привлечения людей и навязывания новой идеологии.

3. Ксенофобия и расизм – ненависть и преследование людей на основе их национальности, расы или культуры.

4. Насилие на митингах и демонстрациях – использование физической силы для давления на правительство или другие организации.

5. Кибератаки – использование технологий для атаки на правительственные или коммерческие цели с целью причинения ущерба.

6. Поджоги и разрушение имущества – использование насилия и разрушения для привлечения внимания к своим целям.

7. Осаждение – блокировка зданий или мест с целью заставить общество выполнить требования экстремистов.

Такие действия могут привести к серьезным последствиям для общества: многочисленным смертям, травмам, разрушениям имущества и нарушениям прав и свобод граждан. Они также могут подорвать доверие к политическим институтам и ослабить стабильность государства. В связи с этим важно разработать эффективные меры для предотвращения таких явлений. Ниже представлены некоторые меры, которые можно использовать [4, с. 170]:

1. Мониторинг социальных сетей и интернет-форумов – один из способов определения и предотвращения политических экстремистских действий. Алгоритмы машинного обучения могут использоваться для анализа текстов, определения ключевых слов и фраз, которые могут указывать на планируемые экстремистские действия.

2. Обучение сотрудников в области кибербезопасности. Регулярное обучение сотрудников в области кибербезопасности может предотвратить кибератаки и несанкционированный доступ к информации. Это также может помочь в идентификации потенциальных угроз безопасности и укреплении защиты информации.

3. Использование электронных баз данных. Создание электронных баз данных о представителях политических и государственных организаций, их действиях и решениях может помочь в предотвращении экстремистских действий. Широкая общественность может получать доступ к информации и контролировать действия государственных органов.

4. Совершенствование алгоритмов искусственного интеллекта: Алгоритмы искусственного интеллекта могут использоваться для анализа и обработки больших объемов данных, чтобы определить потенциальные угрозы и риски безопасности. Они также могут использоваться для прогнозирования и принятия мер предосторожности в отношении возможных экстремистских действий.

5. Повышение культуры безопасности и борьбы с ксенофобией и радикализацией. Использование информационных технологий в образовательных программах и медиапрограммах может помочь в повышении культуры населения.

6. Аналитика данных. Для предотвращения политических экстремистских действий также можно применять технологии анализа данных, которые могут помочь идентифицировать и анализировать группы и организации, связанные с экстремизмом. Это позволит разрабатывать более эффективные стратегии борьбы с экстремизмом и принимать меры по предотвращению его распространения.

В целом информационные технологии могут быть весьма полезны в борьбе с политическим экстремизмом и играть очень важную роль. Однако, как и любые другие, они не являются универсальным решением и требуют комплексного подхода, включающего не только технические, но и социально-политические меры.

С развитием информационных технологий органы внутренних дел улучшают работу в направлении экстремизма, используя новые методы и оборудование, которое повышает раскрываемость преступлений, предоставляет определенные данные для мониторинга, анализа и реагирования на нарушения в данной сфере, являющегося одним из самых важных в России в настоящее время.

Библиографический список

1. Кочои С.М. О качестве уголовно-правового регулирования ответственности за экстремизм и идеологический экстремизм // Всероссийский криминологический журнал. 2022. Т. 16. № 2. С. 240–247.

2. Кузнецов А.А. Представление граждан об экстремизме: понятие, признаки и сущность экстремизма как социального явления (по результатам социологического исследования) // Вестник Прикамского социального института. 2021. № 2 (89). С. 213–218.

3. Сурков Н.А. Религиозный экстремизм как одна из основных форм проявления экстремизма // Молодой ученый. 2023. № 3 (450). С. 391–392.

4. Усманов И.М., Силаева Н.А. Противодействие экстремизму в условиях информатизации общества // Вестник Санкт-Петербургского университета МВД России. 2022. № 1 (93). С. 168–175.

ПРОБЛЕМЫ ОБНАРУЖЕНИЯ ПРИЗНАКОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ В КОМПЬЮТЕРНЫХ СЕТЯХ

Ковалева Е.Г.,

кандидат технических наук;

Бессонов Д.И.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: распространение наркотрафика на виртуальное пространство посредством глобальной сети Интернет, переход на бесконтактные способы оплаты наркосодержащих препаратов, обеспечивающих высокий уровень анонимности драгдиллеров, создают проблемы обнаружения признаков совершения преступлений в сфере незаконного оборота наркотиков и ставят перед сотрудниками правоохранительных органов задачу по увеличению эффективности борьбы с преступлениями в сфере незаконного оборота наркотиков с использованием компьютерных сетей.

Ключевые слова: бесконтактные способы оплаты, даркнет, компьютерные сети, мессенджеры, незаконный оборот наркотиков.

PROBLEMS OF DETECTING SIGNS OF COMMITTING CRIMES IN THE FIELD OF DRUG TRAFFICKING IN COMPUTER NETWORKS

Kovaleva E.G.,

Candidate of Technical Sciences;

Bessonov D.I.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the spread of drug trafficking to the virtual space via the global Internet, the transition to contactless payment methods for narcotic drugs that provide a high level of anonymity for drug dealers, create problems of detecting signs of crimes in the field of drug trafficking and set law enforcement officers the task of increasing the effectiveness of combating crimes in the field of drug trafficking using computer networks.

Keywords: contactless payment methods, darknet, computer networks, messengers, drug trafficking.

На сегодняшний день незаконный оборот наркотиков является одной из наиболее серьезных угроз для безопасности общества и государства. Употребление наркотиков оказывает разрушительное воздействие на человеческий организм, а массовость их употребления ставит здоровье всего населения под угрозу.

Более того, распространение наркотиков стимулирует рост преступности, а также коррупции. При всем этом наркобизнес является достаточно прибыль-

ным, а потому в незаконный оборот наркотиков с каждым годом вовлекается все больше и больше людей. Глобальный характер наркобизнеса делает незаконный оборот наркотиков трудноискоренимым явлением [1, с. 36].

На сегодняшний день существует бесчисленное количество способов распространения наркотиков, при этом превалируют бесконтактные способы. В этой связи идеальным каналом распространения наркотиков являются компьютерные сети, в частности Интернет.

Использование Интернета во многом облегчает преступную деятельность по распространению наркотиков, а также позволяет сохранять условия анонимности. Если до внедрения компьютерных сетей в незаконный оборот наркотиков правоохранительные органы «цеплялись» за прямой контакт между покупателем и продавцом, то использование Интернета отменяет необходимость прямого контакта и, соответственно, значительно усложняет работу правоохранительных органов [2, с. 97].

Можно констатировать тот факт, что интенсивные темпы развития компьютерных сетей обуславливают процесс автоматизации незаконного оборота наркотиков. Покупка наркотиков происходит одним кликом компьютерной мыши.

Для распространения наркотиков используются возможности так называемого даркнета. На просторах «темного» Интернета расположено бесчисленное множество виртуальных магазинов – драг-маркетов. Наличие виртуального пространства значительно затрудняет выявление и раскрытие преступлений, совершаемых в сфере незаконного оборота наркотиков с использованием компьютерных сетей.

При этом нельзя сказать, что правоохранительные органы бессильны перед даркнетом. Так, в апреле 2022 года была заблокирована крупнейшая онлайн-площадка продажи нелегальных товаров, в том числе и наркотиков, «Гидра». В момент закрытия площадки на ней было размещено 19 тысяч магазинов. С их закрытием одни лишились возможности приобретать наркотики, другие – внушительного заработка [3].

После потери пространства для торговли популярность приобрели мессенджеры, в частности такие как Telegram и Jabber. При этом создатель Telegram отказался передавать частные данные пользователей правоохранительным органам в целях противодействия незаконному обороту наркотиков.

В связи с этим возникли достаточно серьезные проблемы, ведь теперь сам процесс выявления признаков преступлений значительно осложнился. Помимо этого, пространство Интернета находится вне правового поля, поэтому предотвращение развития теневого Интернета представляется невозможным.

Также стоит отметить, что развивается не только продажа, но и деятельность, направленная на изготовление наркотических веществ. Изготовители при этом нацелены на создание таких веществ, которые согласно действующему законодательству Российской Федерации не относятся к наркотическим веществам, но обладают наркотическим эффектом. Такие вещества характеризуются синтетической природой, а также непредсказуемостью своего воздействия на человеческий организм.

Для выявления преступлений, совершаемых в сфере незаконного оборота наркотиков с использованием компьютерных сетей, необходимо знать источники распространения сведений о наркотиках.

Глобальную сеть можно подразделить на несколько уровней по своему содержанию. Наиболее известный – это общедоступный Интернет. Из названия понятно, что доступ к материалам, расположенным на таком уровне, может получить любой человек. При этом сведения, касающиеся наркотиков, как правило, скрыты, тщательно замаскированы. Кроме того, общедоступный Интернет отслеживается надзорными ведомствами и распространение «запрещенной» информации блокируется по решению судебных органов.

Менее доступным уровнем является маргинальный Интернет. Здесь можно найти информацию о продаже наркотиков, рецептах их изготовления. Рядовой пользователь сможет попасть в маргинальный Интернет с использованием VPN-технологий.

Еще одним уровнем Интернета выступает глубокий Интернет, включающий в себя бесчисленные массивы информации, не индексируемые универсальными поисковыми системами. Подавляющее большинство пользователей не осведомлены о наличии данного уровня. Кроме того, проблематика глубокого Интернета не освещается в научной литературе.

Основным способом выявления преступлений в сфере незаконного оборота наркотиков с использованием компьютерных сетей является мониторинг. В настоящее время известен ручной и автоматизированный мониторинг. Первым занимаются сотрудники оперативных подразделений, второй вид мониторинга не получил повсеместного распространения. На наш взгляд, автоматизированный мониторинг позволил бы многократно оптимизировать процесс выявления таких преступлений.

Кроме того, получение доступа правоохрнительными органами к уровню глубоко Интернета позволит открыть новые возможности борьбы с незаконным оборотом наркотиков в компьютерных сетях.

Темный Интернет представляет собой частную сеть, в которой соединение устанавливается только с доверенными участниками сети. При этом файлообмен происходит анонимно. Именно на данном уровне происходит торговля незаконными товарами, такими как наркотики, оружие, драгоценные металлы и др.

Подводя итог вышесказанному, необходимо отметить, что наркопреступность в Интернете стремительно набирает обороты, а потому сложившаяся ситуация требует незамедлительного реагирования со стороны правоохрнительных органов в целях сохранения здоровья населения, а также безопасности общества и государства.

Свободное пространство Интернета значительно затрудняет выявление преступлений в сфере незаконного оборота наркотиков с использованием компьютерных сетей. В этой связи актуальным направлением государственной политики должно стать инвестирование в развитие технологий дешифрации данных с дальнейшим применением в целях изобличения преступников.

Помимо этого, в деятельность правоохранительных органов необходимо внедрить автоматизированный мониторинг, в том числе и на самых «глубоких» уровнях Интернета.

Считаем, что приведенные рекомендации позволят выявлять большее количество преступлений, совершаемых в сфере незаконного оборота наркотиков с использованием компьютерных сетей, и выведут противодействие наркопреступности на новый, более качественный уровень.

Библиографический список

1. Кольжанов И.В. Проблемы и возможные пути совершенствования мер противодействия сбыту наркотических средств (психотропных веществ) посредством сети Интернет / Деятельность правоохранительных органов в современных условиях: сборник материалов XXIV Международной научно-практической конференции, Иркутск, 6–7 июня 2019 года. – Иркутск: Восточно-Сибирский институт МВД России, 2019. С. 36–39.

2. Пучнин А.В., Коськова Н.В. Актуальные проблемы противодействия наркопреступности в сети даркнет // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2022. № 8. С. 97–103.

3. Крупнейший в мире магазин наркотиков закрыт: Новостной форум LENTA.RU [Электронный ресурс]. – URL: <https://lenta.ru/articles/2022/04/10/> (дата обращения: 06.02.2023).

ПРОБЛЕМЫ РАСКРЫТИЯ ИНФОРМАЦИОННЫХ ПРЕСТУПЛЕНИЙ

**Ковалева Е.Г.,
Рыбальченко М.А.**

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: информационные технологии стали неотъемлемой частью жизни современного общества. Однако они также являются объектом для совершения различных преступлений. В России, как и в других странах мира, информационные преступления стали серьезной проблемой для правоохранительных органов.

Ключевые слова: информационные технологии, базы данных, обмен информацией, преступники, техническая экспертиза.

PROBLEMS OF DISCLOSURE OF INFORMATION CRIMES

**Kovaleva E.G.,
Rybalchenko M.A.**

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: information technologies have become an integral part of the life of modern society. However, they have also become a target for criminals who use them to commit various crimes. In Russia, as in other countries of the world, information crimes have become a serious problem for law enforcement agencies.

Keywords: information technologies, databases, information exchange, criminals, technical expertise.

В январе – июле 2022 года зарегистрировано 315,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 15,7% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес вырос с 22,9% в январе – июле 2021 года до 26,6%. Рассмотрим в данной статье некоторые из главных проблем, с которыми сталкиваются правоохранительные органы в России в процессе раскрытия информационных преступлений. С использованием высоких технологий совершается каждое четвертое преступление [1].

Основные проблемы раскрытия информационных преступлений в Российской Федерации:

1. Недостаток квалифицированных кадров одна из главных проблем, с которыми сталкиваются правоохранительные органы в России. Информационные технологии быстро развиваются, и правоохранительным органам необходимо постоянно обновлять свои знания и навыки. Однако в настоящее время не все сотрудники правоохранительных органов имеют достаточные знания и навыки для борьбы с информационными преступлениями.

2. Отсутствие в России единой базы данных, в которой хранились бы данные об информационных преступлениях. Это затрудняет процесс раскрытия преступлений, так как правоохранительным органам приходится искать информацию в различных источниках, что требует много времени и ресурсов.

3. Отсутствие законодательной базы для борьбы с информационными преступлениями. Существующие законы и нормы не всегда соответствуют новым видам преступлений, связанным с использованием информационных технологий. Это создает сложности в процессе раскрытия и наказания преступлений.

4. Проблемы с обменом информацией между правоохранительными органами, которые являются серьезным препятствием в борьбе с информационными преступлениями.

В России существует несколько правоохранительных органов, занимающихся борьбой с информационными преступлениями, такие как ФСБ, МВД, СК

и другие. Однако не всегда эти органы эффективно обмениваются информацией друг с другом, что затрудняет раскрытие и наказание преступников.

5. Анонимность в сети, являющаяся еще одной серьезной проблемой для правоохранительных органов. Преступники могут использовать различные методы, такие как VPN, анонимные браузеры и другие технологии, чтобы скрыть свою личность и местоположение. Это затрудняет идентификацию преступников и раскрытие преступлений.

6. Сложность технической экспертизы, которая является важной частью процесса раскрытия информационных преступлений. Однако для ее проведения необходимы высококвалифицированные специалисты и специальное оборудование. Не все правоохранительные органы в России имеют достаточные ресурсы для проведения такой экспертизы.

7. Большое количество ложных сообщений о возможных информационных преступлениях, которые создают дополнительные трудности для правоохранительных органов, что вынуждает тратить время и ресурсы на проверку каждого сообщения и затрудняет раскрытие реальных преступлений.

Существует несколько возможных путей решения проблем, связанных с раскрытием информационных преступлений в России:

1. Улучшение квалификации сотрудников правоохранительных органов для более эффективной борьбы с информационными преступлениями. Это может быть достигнуто путем организации курсов повышения квалификации, тренингов и семинаров, а также обмена опытом между различными органами.

2. Создание единой базы данных для улучшения обмена информацией между правоохранительными органами, содержащую информацию обо всех известных информационных преступлениях. Это позволит быстрее и более эффективно раскрывать преступления и предотвращать их совершение [2].

3. Для более эффективной борьбы с информационными преступлениями необходимо усилить законодательную базу в России. Это может быть достигнуто путем разработки новых законов и правил, которые будут соответствовать современным технологиям и вызовам.

4. Улучшение сотрудничества с другими странами может улучшить обмен информацией и сделать более эффективным раскрытие информационных преступлений, так как многие информационные преступления совершаются через границы, что затрудняет их раскрытие и наказание преступников.

5. Разработка новых технологий, таких как программное обеспечение, для выявления и предотвращения информационных преступлений, может помочь правоохранительным органам в борьбе с подобными преступлениями. Необходимо поддерживать и развивать научные исследования в области кибербезопасности и информационных технологий [3].

6. Развитие культуры информационной безопасности и пропаганда осведомленности в этой области может помочь уменьшить количество информационных преступлений, так как люди будут более внимательны и осторожны при использовании Интернета и цифровых устройств. Это может быть достигнуто путем проведения образовательных программ, кампаний и мероприятий, кото-

рые будут нацелены на повышение осведомленности людей в области кибербезопасности.

Борьба с информационными преступлениями является сложной задачей для правоохранительных органов в России. Недостаток квалифицированных кадров, отсутствие единой базы данных, проблемы с законодательной базой, проблемы с обменом информацией между правоохранительными органами, анонимность в Сети, сложность технической экспертизы и большое количество ложных сообщений – все эти факторы затрудняют процесс раскрытия информационных преступлений. Для эффективной борьбы с такими преступлениями необходимы комплексные меры.

Библиографический список

1. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года // Официальный сайт МВД России [Электронный ресурс]. – URL: <https://мвд.рф/reports/item/28021552/>
2. Дерюгин Р.А., Файсханов И.Ф. К вопросу о криминалистическом исследовании видеозаписи в условиях развития цифровой криминалистики // Вестник Уральского юридического института МВД России. 2020. № 3(27). С. 56–61.
3. Семененко Г.М., Чхвимиани Э.Ж. Применение инновационных технологий в целях предупреждения дорожно-транспортных происшествий на территории Российской Федерации // Вестник Волгоградской академии МВД России. 2018. № 4(47). С. 62–69.

МЕТОДЫ ПОИСКА ПРИЗНАКОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ В КОМПЬЮТЕРНЫХ СЕТЯХ

Ковалева Е.Г.,

кандидат технических наук;

Ткач П.А.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: для незаконного оборота наркотиков в настоящее время характерны значительный рост количества источников и методов их распространения с использованием глобальной сети Интернет и систем электронных платежей. Несмотря на известные алгоритмы взаимодействия покупателя и продавца, установление их личностей представляет большую сложность для правоохранительных органов.

Ключевые слова: бесконтактный способ сбыта, Интернет, наркотические средства, способы оплаты, электронный кошелек.

METHODS OF SEARCHING FOR SIGNS OF COMMITTING CRIMES IN THE FIELD OF DRUG TRAFFICKING IN COMPUTER NETWORKS

Kovaleva E.G.,

Candidate of Technical Sciences;

Tkach P.A.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: drug trafficking is currently characterized by a significant increase in the number of sources and methods of their distribution using the global Internet and electronic payment systems. Despite the well-known algorithms of interaction between the buyer and the seller, establishing their identities is very difficult for law enforcement agencies.

Keywords: contactless sales method, Internet, narcotic drugs, payment methods, electronic wallet.

Прежде всего стоит отметить значительную тенденцию роста источников и методов распространения наркотических средств. За последние десятилетия, наряду с развитием интернета и компьютерных технологий, проводится наркотизация не только России, но и других стран. Эксперты ссылаются на наличие большого количества теневых областей во Всемирной интернет-паутине.

Особенностью размещения и продажи наркотических средств через интернет-ресурсы является бесконтактный способ их сбыта. Вся эта цепочка устроена следующим образом:

1. Преступники размещают объявление на сайте, созданном в теневом пространстве Интернета, также носящим название DarkNet (далее – DN).

2. Потенциальные покупатели, заходя в DN посредством защищенного интернет-соединения, путем различных способов шифрования интернет-пакета, сталкиваются с таким объявлением [1, с. 69].

3. Связавшись с продавцом, покупатели оплачивают товар путем системы электронных платежей.

4. После оплаты назначается место и время, для того чтобы забрать приобретенные ими наркотические вещества.

На первый взгляд схема выглядит довольно просто, однако вычислить ее проведение, а также участников – продавца и покупателя – бывает очень затруднительно. Ведь при расследовании преступлений в данной сфере использование традиционных способов формирования доказательной базы и установления преступников представляется невозможным, так как физической передачи товара не происходит и отсутствует контакт между участниками такой сделки.

Норма п. «б» ч. 2 ст. 228.1 УК РФ регулирует сбыт наркотиков, осуществляемый данным способом¹. Предметом преступления являются наркотические сред-

¹ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022) // СПС «КонсультантПлюс».

ства, психотропные, сильнодействующие и ядовитые вещества. Необходимо отметить, что в настоящее время возросло количество разработки именно психоактивных веществ, которые далеки от состава традиционных наркотических веществ.

Рассмотрим подробнее способ оплаты, производимый при операциях, связанных со сбытом наркотических веществ. До недавнего времени он проводился посредством использования электронного кошелька Qiwi, однако сейчас все больше операций производится с использованием криптокошельков [2, с. 13]. И для оперативных сотрудников важно установить владельца одного из указанных кошельков. В случае с Qiwi-кошельком, достаточно будет отправить запрос на предоставление данных о держателе кошелька, а именно:

- данные о фактах пополнения кошелька: дату, место, время, местонахождение терминала;
- информацию о переводах на другие счета, а также предоставление информации об этих счетах;
- информацию о кошельке покупателя, указанную им при регистрации;
- сведения об электронной почте и IP-адресе владельца кошелька.

В дальнейшем, обладая этими данными, появляется возможность установить, откуда, где, когда и с какого устройства производился платеж. Определение mac-адреса и imei устройства также будет возможно, если данные, предоставленные оперативному сотруднику, будут объективными и достаточными. С обнаружением информации о пользователе, использующем криптокошельки для произведения оплаты, возникают наибольшие затруднения из-за анонимизации данных в этой платежной сфере.

Раскрытие данных преступлений проводится не только на стадиях их совершения, но и подготовки и сокрытия деяния. Выбор этапа для расследования зависит от количества трассологических следов, оставленных преступниками.

Еще одним методом установления сбытчиков наркотических веществ является вербовка лиц под «покупателей» оперативными сотрудниками. При таком методе появляется больше шансов сразу выйти на сбытчика и иных лиц, состоящих с ним в преступном сговоре, которые чаще являются так называемыми «диспетчерами», то есть людьми, осуществляющими коммуникацию между сбытчиком и покупателем [3, с. 271].

На стадии подготовки возможно изобличение личностей преступников посредством создания в сети DN оперативными сотрудниками так называемых магазинов, продающих оборудование для изготовления психоактивных и наркотических веществ. В таком случае нельзя избежать непосредственного контакта и можно выйти через посредников, скупающих такое оборудование, на самих сбытчиков, состоящих с ними в преступном сговоре.

Таким образом, отметим возможность выявления преступлений, связанных со сбытом наркотических веществ путем использования компьютерных сетей на всех этапах их совершения. Единственная сложность в данной сфере – это постоянно развивающиеся способы и методы действия самих преступников, выражающиеся во все более глубокой анонимизации себя в интернет-ресурсах, и возникновение новых электронных платежных систем, не предоставляющих либо вовсе не собирающих данных о своих пользователях.

Библиографический список

1. Полунина А.В., Магомедов Р.М. Даркнет: по ту сторону Интернета // Академический журнал Западной Сибири. Т. 15. № 3 (80). 2019. С. 69–70.
2. Генкин А., Михеев А. Блокчейн: как это работает и что нас ждет завтра. – Москва: Альпина Паблишер, 2018. С. 170.
3. Битов А.А. Выявление и раскрытие преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием информационных технологий // Проблемы экономики и юридической практики. 2018. № 3. С. 269–272.

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Кургузов А.В.

(Омская академия МВД России)

Аннотация: в последние годы значительный прогресс был достигнут в разработке алгоритмов и методов искусственного интеллекта для точного и надежного распознавания лиц в различных ситуациях. В статье рассматривается использование этих систем в правоохранительной деятельности. Автор раскрывает преимущества и вызовы использования искусственного интеллекта для этих целей, а также анализирует влияние таких систем на права и свободы граждан. Кроме того, рассматриваются другие области применения искусственного интеллекта.

Ключевые слова: искусственный интеллект, нейронная сеть, серийное преступление, биометрия, распознавание.

ARTIFICIAL INTELLIGENCE TECHNOLOGY IN LAW ENFORCEMENT

Kurguzov A.V.

(Omsk Academy of the Ministry of the Interior of Russia)

Abstract: in recent years, significant progress has been made in the development of AI algorithms and methods for accurate and reliable face recognition in various situations. This article examines the use of these systems in law enforcement. The authors discuss the advantages and challenges of using AI for these purposes, and analyze the impact of such systems on the rights and freedoms of citizens. In addition, other applications of artificial intelligence are considered.

Keywords: artificial intelligence, neural network, serial crime, biometrics, recognition.

Технологии искусственного интеллекта развиваются уже более 50 лет. Благодаря бурному развитию вычислительной техники в последние годы его повсеместное внедрение стало наиболее заметно. За последние 5–7 лет в МВД России было внедрено несколько крупных проектов, которые основаны на технологии искусственного интеллекта.

В период проведения чемпионата мира по футболу в 2018 году на территории России были опробованы такие системы, как FaceT и FindFace. Эти системы разработаны отечественной компанией NtechLab.

С использованием этих систем при проведении чемпионата было задержано более 100 человек подозреваемых в нарушениях правопорядка, кражах во время проведения соревнований [1].

Система FindFace позиционируется для решения следующих задач:

- розыск правонарушителей: хотя личность правонарушителя может быть неизвестна, в большинстве случаев сотрудники правоохранительных органов располагают изображением, полученным, например, из фото- или видеоматериалов, изъятых с места преступления или с системы охранного видеонаблюдения. С использованием видеоаналитики, такой как FindFace, возможно установить место проживания разыскиваемого лица, его привычные маршруты передвижения, а также выявить социальные связи и потенциальных сообщников. Это позволяет получить ценную оперативную информацию;

- розыск без вести пропавших людей: каждый год в городской среде в России пропадает множество людей, их число достигает десятков тысяч. В случае поиска пропавшего человека время становится критически важным ресурсом. Однако с использованием технологии FindFace удастся в считанные секунды определить последние известные места пребывания и маршрут разыскиваемого человека, а также выявить лица, сопровождающие его, что позволяет сузить район поиска;

- безопасность массовых мероприятий: во время проведения массовых мероприятий на улицах и площадях города одной из главных задач становится обнаружение лиц, которые могут представлять угрозу общественной безопасности. С помощью технологии FindFace возможно осуществить распознавание и идентификацию разыскиваемого преступника в потоке людей. Это предоставляет сотрудникам спецслужб оперативную информацию для принятия соответствующих мер в реальном времени;

- транспортная безопасность: обеспечение объектов транспортной инфраструктуры имеет стратегическое значение.

У систем распознавания есть несколько характеристик, определяющих качество алгоритма.

FNMR (False Non-Match Rate) – вероятность ложного несовпадения (соотношение количества ложно понятных решений к количеству всех принятых решений).

FMR (False Match Rate) – вероятность ложного совпадения (соотношение количества случаев ложно принятых решений к количеству всех принятых решений).

Для системы FindFace $FNMR=0,008$; $FMR<0,000001$.

Такие показатели означают, что система выдает очень низкое количество ошибок. Системы с подобными характеристиками считаются очень хорошими.

В настоящий момент в Москве более 250 тыс. видеокамер, подключенных в единый центр обработки данных. Система помогает находить как преступников, так и нарушителей. В 2020–2021 годы с использованием этой системы определялись лица, нарушающие карантинные меры по COVID-2019. [2]

В России согласия на обработку биометрических данных не требуется. Письменное согласие не требуется, если обработка биометрических данных необходима в случаях, описанных в законах об обороне, о безопасности и о противодействии терроризму.

Осенью 2022 года у системы кроме прочих появилась новая задача – поиск уклонистов от частичной мобилизации. При этом стало известно, что система имеет и некоторые недостатки – для поиска требуется свежее фото разыскиваемого человека. Комплекс пока не в состоянии найти человека по фотографии 15–20 летней давности.

В МВД России есть еще одно перспективное направление использования технологии искусственного интеллекта. МВД России заказало исследование у некоммерческой организации "Специальная техника и связь", направленное на определение возможности использования искусственного интеллекта для выявления признаков серийности уголовных и административных преступлений. Основываясь на результатах этого исследования, планируется создать информационную систему, которая будет использовать успешные технологии распознавания речи и рукописных текстов, а также анализа больших объемов данных.

Это исследование имеет шифр «Серия». Стоимость исследования более 50 млн рублей и должно было завершиться в 2022 году. Также известно, что в 2024 году система поступит в промышленную эксплуатацию.

Утверждается, что «в ходе практической реализации данного подхода российская наука выйдет в мировые лидеры в одном из наиболее перспективных направлений развития фундаментальной науки».

В рамках этого проекта планируется разработать систему, которая позволит выделять несколько преступлений или административных правонарушений в серию, тем самым облегчить поиск преступников. Кроме того, искусственный интеллект позволит определять внешние признаки преступников (цвет глаз и волос, форму лица и головы) по полученному с мест преступлений биоматериалу, например следам крови.

Планируется, что систему в будущем смогут использовать не только для нужд правоохранителей, но и для разработки медицинских проектов. На текущий момент в открытых источниках отсутствует какая-либо информация о промежуточных итогах исследования, поэтому сейчас сделать предположения об успешности реализации этого проекта нельзя.

Служба ГИБДД всегда являлась передовой в системе МВД в плане внедрения новых технологий. Технологии искусственного интеллекта используются в этой службе достаточно давно.

Нейронные сети – одна из технологий построения искусственного интеллекта. Нейронные сети уже более десятка лет используются в специализирован-

ных программах Госавтоинспекции для распознавания государственных регистрационных номеров автомобилей.

При автоматической фиксации административных правонарушений нейронные сети позволяют без вмешательства человека предварительно распознать государственный регистрационный номер автомобиля, тем самым ускорить обработку огромного количества фотографий.

В 2018 году в Москве запустили систему способную распознать по изображению модель и марку автомобиля. Система ориентируется на логотипы, силуэты, фонари автомобилей.

Работа этой системы тоже ускоряет обработку административных правонарушений. Так, если система распознала марку автомобиля и государственный регистрационный знак, а в базе данных числится другая модель, то это фотоизображение попадает на «ручную» обработку. В противном случае оформление административного правонарушения произойдет в упрощенном порядке.

По схожему принципу работает система контроля грузового транспорта «Платон». Эта система отслеживает передвижения, нарушения массы, нарушения габаритов грузовыми автомобилями. Система контролирует соблюдения водителями ограничений по маршруту следования, а также ограничений по массе и габаритам.

Уровень технологий, используемых в России, ничем не уступает зарубежным аналогам. Наличие некоторых исследований, таких как определение серийности преступлений и определение внешних черт по биоматериалу, показывает желание руководства МВД внедрять самые современные передовые технологии в деятельность правоохранительных органов России.

Библиографический список

1. Система распознавания лиц помогла предотвратить кражу спонсорского кубка ЧМ-2018 [Электронный ресурс]. – URL: <https://lenta.ru/news/2018/07/26/> (дата обращения: 14.05.2022).
2. Текущее положение дел по распознаванию лиц и камерам наблюдений в Москве и мире [Электронный ресурс]. – URL: <https://habr.com/ru/articles/553448/> (дата обращения: 14.05.2022).
3. Меняйло Д.В., Меняйло Л.Н., Крупенникова К.К. Инновации как инструмент деятельности сотрудников полиции / Цифровая экономика: перспективы развития и совершенствования: сборник научных статей 3-й Международной научно-практической конференции. – Курск, 2022. С. 259–262.

МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Куриленко Ю.А.,

кандидат юридических наук;

Любаева Д.С.

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: развитие компьютерных технологий и стремительная информатизация современного общества, безусловно, дало скачок в развитии целых отраслей и различных сфер жизнедеятельности человека. Но вместе с положительными тенденциями внедрения информационно-коммуникационных технологий общество получило и серьезные вызовы. Криминальный мир существовал во все времена, но чем прогрессивнее развитие общества, тем быстрее развивается и криминал. Появляются новые виды преступлений, новые способы и методы, новые орудия их совершения. И вот уже в обиходе звучат такие понятия, как киберпреступления, кибермошенничество, кибербезопасность. Авторами проведен анализ основных современных видов мошенничеств в информационной сфере, а именно с использованием компьютерных технологий и информационно-телекоммуникационных средств. В статье авторы обозначают основные правила кибербезопасности.

Ключевые слова: мошенничества, компьютерные технологии, компьютерная информация, киберпреступность, кибербезопасность, личные данные.

FRAUD IN THE SPHERE OF COMPUTER INFORMATION

Kurilenko Yu.A.,

Candidate of Law Sciences;

Lyubaeva D.S.

(Kikot Moscow University the Ministry of Internal Affairs of Russia)

Abstract: the development of computer technology and rapid informatization of modern society has undoubtedly given a leap in the development of entire industries and various spheres of human activity. But along with the positive trends in the implementation of information and communication technologies, society has also received serious challenges. The criminal world did not appear yesterday, it has existed at all times, but the more progressive the development of society, the faster criminal activity develops. There are new types of crimes, new methods and techniques, new tools to commit them. And now there are such concepts as cybercrime, cyber-fraud, cyber-security. The authors analyze the main modern types of fraud in the information sphere, namely with the use of computer technology and information and telecommunication means. In the article, the authors outline the basic rules of cyber security.

Keywords: fraud, computer technology, computer information, cybercrime, cyber security, personal data.

В настоящее время развитие информационно-телекоммуникационных технологий достигло небывалого уровня и те достижения, которые еще несколько десятилетий назад представлялись человечеству чем-то из области фантастики, теперь прочно закрепились в нашей повседневной жизни. Но, к сожалению, мы пользуемся не только благами плодов цивилизации. Вместе с прогрессом существуют и негативные последствия, заключающиеся в том числе в криминализации новых видов посягательств с применением компьютерных технологий и информационно-коммуникационных средств.

Использование современных технологий для совершения мошенничества в информационной сфере растет стремительно, так как использование компьютерных программ позволяет преступнику скрытно заниматься криминальной деятельностью, но при этом обеспечивает доступ к многочисленным ресурсам. Каждый день большое количество людей становятся жертвами киберпреступников, которые используют различные методы для совершения мошенничеств при помощи информационно-коммуникационных технологий.

В 2012 году в Уголовный кодекс Российской Федерации были внесены изменения. В частности, добавлена статья 159.6 «Мошенничество в сфере компьютерной информации». Предметом преступления являются чужое имущество или приобретение чужого имущества. Модификация, блокирование, удаление, ввод и иные схожие вмешательства в функционирование средств передачи, обработки или хранения данных компьютерной информации являются формами проявления неправомерного деяния [1].

Под данное преступное деяние подпадает довольно много видов киберпреступлений, которые возможно совершить посредством использования современных информационно-компьютерных технологий.

Существует несколько способов неправомерного доступа для получения личной и иной информации. Например, использование чужого имени или пароля, нахождение слабых мест, взлом системы защиты, физическое хищение информационного носителя.

Рассмотрим несколько распространенных видов-методов мошенничества в сфере компьютерной информации.

Одним из наиболее распространенных является фишинг. Данный метод используется для получения доступа к чужим аккаунтам, банковским и электронным кошелькам. Для этого создаются веб-сайты, похожие на оригинальные, при этом киберпреступники отправляют электронные письма с просьбой ввести логин и пароль на этом сайте. После ввода данные попадают в руки мошенников, которые используют их для получения доступа к счету [2, с.154].

Еще одним методом мошенничества является скам, который используется для обмана и получения денег. Скамеры применяют различные способы для получения желаемого результата – обещание быстрого заработка, выигрыша в лотерее – убеждая при этом людей отправить им деньги. Скам-схемы схожи с финансовыми пирамидами и могут иметь разную направленность – от привлечения криптовалюты или других денежных средств до брачных афер. Для достижения своих целей кибермошенники используют телефонные звонки, социальные сети или электронную почту [3].

Вышеперечисленные методы мошенничеств относятся к методам социальной инженерии и являются наиболее распространенными среди методов воздействия на человеческую психику.

Также к формам проявления преступных деяний в рассматриваемой сфере относят использование программного обеспечения, которое устанавливается на компьютер жертвы без ее ведома, что впоследствии позволяет злоумышленникам получить доступ к информации, хранящейся на таком компьютере. К таким вредоносным программам можно отнести, к примеру, Rootkit, Malware и другие.

Говоря о Rootkit-атаке нужно отметить, что она используется с целью получения расширенных прав пользователя и представляет собой сложный цифровой код, действующий скрытно в течение длительного времени, при этом никоим образом не влияя на процесс работы компьютера, и позволяет удаленно контролировать компьютер пользователя [4, с.43].

Malware – это вредоносное программное обеспечение, которое может наносить вред системе, сетям или устройствам или используется для создания среды, в которой могут распространяться вирусы или трояны с дальнейшей целью кражи данных. Malware может быть установлено на компьютер жертвы через электронную почту, через некоторые приложения или встроено в рекламу. Следует отметить, вирусные программы и трояны также являются средством похищения личных данных [5].

Если в целом рассматривать мошенничества в сфере компьютерной информации, то это достаточно серьезная проблема современности, которая может привести к большим финансовым потерям и утечке личных данных. А потому информационная осведомленность общества в данной сфере будет не только способствовать поимке киберпреступников, но и позволит предотвращать преступления подобного рода. «Предупрежден – значит вооружен», – гласит пословица.

Чтобы защитить себя, свои личные данные, свое имущество от мошенничества в сфере компьютерной информации, следует соблюдать несколько основных правил неукоснительно. Во-первых, не переходить по неизвестным и подозрительным ссылкам, не скачивать файлы с неизвестных/ненадежных сайтов, не открывать подозрительные электронные письма, веб-сайты, рекламные объявления. Во-вторых, защитить компьютер антивирусным программным обеспечением с регулярным обновлением. В-третьих, не доверять незнакомым/малознакомым людям, не вступать с ними в переписку и не отправлять им деньги. Быть осторожным в общении в социальных сетях и не раскрывать личную информацию (адрес, финансовые данные, номер телефона и прочее). В-четвертых, следует уделить внимание использованию надежных паролей и их регулярной смене. Не стоит использовать один и тот же пароль для разных аккаунтов и такую личную информацию в качестве пароля, как имя или дату рождения.

Библиографический список

1. Федеральный закон от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 14.04.2023).
2. Страхов А. А., Прокопенко А. Н. Как атакует фишинг? / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей IX Всероссийской научно-практической конференции, Белгород, 20 мая 2022 года. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2022. С. 154–163.
3. Ксения Добрынина. Скам: как распознать и не попасться [Электронный ресурс]. – URL: <https://quote.rbc.ru/news/article/>
4. Рахмонбердиев Б.Б., Куриленко Ю.А. Уровни угроз атаки rootkit и методы борьбы с ними / Противодействие терроризму и экстремизму в информационных сферах: сборник научных статей Всероссийской конференции, Москва, 26 апреля 2022 года. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2022. С. 43–45.
5. Анна Соколова. Что такое Malware и как его удалить? [Электронный ресурс]. – URL: <https://v-mire.net/what-is-malware/>
6. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9–22.

АКТУАЛЬНЫЕ ВОПРОСЫ КИБЕРПРЕСЛЕДОВАНИЯ

Карпика А.Г.,

кандидат технических наук, доцент;

Лемайкина С.В.

(Ростовский юридический институт МВД России)

Аннотация: в статье исследуются проблемы киберпреследования и запугивания через информационно-телекоммуникационную сеть Интернет. Автор характеризует формы киберпреследования, выявляет основные методы борьбы с ним, предлагает пути решения проблемы киберпреследования в России.

Ключевые слова: киберпреследование, интернет-преследование, киберпреступления, цифровые технологии, искусственный интеллект, цифровая криминалистика, социальные сети.

CURRENT ISSUES IN CYBERHARASSMENT

Karpika A.G.,

Candidate of Sciences in Technology, Associate Professor;

Lemajkina S.V.

(Rostov Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: the article deals with the problems of cybercrime and stalking through the data telecommunications network Internet. The author characterizes the forms of cybercrime, identifies the main methods of counteracting it, and suggests ways to solve the problem of cybercrime in Russia.

Keywords: cybercrime, internet harassment, digital technologies, artificial intelligence, digital forensics, social networks.

С ростом зависимости от технологий и цифровых коммуникаций угроза компьютерных преступлений и нарушений информационной безопасности стала серьезной проблемой для частных лиц, предприятий и правительств во всем мире. Проблема противодействия компьютерным преступлениям и обеспечения информационной безопасности в последние годы обострилась в связи с ростом изощренности киберпреступников и появлением новых форм киберугроз.

Компьютерные преступления — это незаконные действия, совершаемые с использованием компьютеров или цифровых технологий. Существует несколько типов компьютерных преступлений, включая взлом, фишинг, кражу личных данных, кибертерроризм, киберпреследование.

Из всех форм различных киберпреступлений хочется выделить киберпреследование (киберзапугивание, киберсталкинг), которое относится к использованию электронных средств связи, таких как социальные сети, текстовые сообщения и онлайн-форумы для запугивания или преследования кого-либо.

Киберпреследование — это отдельная уникальная категория киберпреступлений. Различные виды киберпреследования могут включать в себя сексуальные, религиозные, расовые и пр. домогательства. Домогательство — это преступление, которое охватывает нарушение неприкосновенности частной жизни нетизенов (Гражданин Сети). Такое посягательство на частную жизнь влечет за собой серьезное наказание [2].

Использование технологий для запугивания резко возросло в последние годы, но корни киберзапугивания можно проследить от первых дней Интернета. Первый зарегистрированный случай киберзапугивания произошел в конце 1980 — начале 1990-х годов в первых системах электронных досок объявлений (BBS). Эти системы часто использовались подростками, которые брали анонимные имена пользователей, чтобы преследовать и запугивать других в Интернете. По мере того как Интернет стал более широко использоваться, киберзапугивание начало принимать новые формы. На заре электронной почты люди нередко получали оскорбительные сообщения от незнакомцев или знакомых. В конце 1990-х и начале 2000-х годов стали популярными онлайн-чаты и плат-

формы для обмена мгновенными сообщениями, и они часто использовались хулиганами для нападения на своих жертв. С появлением социальных сетей в середине 2000-х киберзапугивание приобрело новые масштабы. Платформы социальных сетей, такие как Facebook, Twitter и Instagram, позволили хулиганам нападать на своих жертв публично и широко, часто используя поддельные профили или анонимные учетные записи для преследования других.

Сегодня киберзапугивание остается серьезной проблемой, миллионы людей во всем мире ежегодно подвергаются онлайн-домогательствам и оскорблениям. Киберпреследование может иметь серьезные последствия для жертв, включая эмоциональный стресс, ущерб репутации и даже физический вред в некоторых случаях. Интернет-преследование, которое включает использование цифровых технологий для преследования, запугивания или угроз кому-либо, может принимать самые разные формы. Вот несколько общих классификаций киберпреследований:

троллинг – преднамеренное размещение провокационных или оскорбительных комментариев в Интернете с целью спровоцировать жертву. Публикация комментариев или изображений в чьем-либо профиле в социальных сетях, блоге или онлайн-форуме с намерением нанести ущерб репутации пользователя;

доксинг – публичная публикация чьей-либо личной информации в Интернете, часто с намерением запугать жертву, публичное раскрытие чьей-либо личной информации, такой как домашний адрес, номер телефона или адрес электронной почты, с намерением также запугать жертву;

порноместь – публикация или совместное использование откровенных фотографий или видео кого-либо без его согласия, часто с намерением унижить или шантажировать человека.

Важно отметить, что киберпреследование может принимать множество других форм, и бывает трудно провести четкую границу между различными типами поведения. Однако, понимая различные классификации киберпреследований, можно эффективнее выявлять и решать эту растущую проблему.

Использование цифровых технологий для преследования или запугивания человека, также известное как киберпреследование, вызывает растущую озабоченность в современном обществе. С ростом зависимости от технологий и широкого использования платформ социальных сетей киберпреследование стало слишком распространенным явлением. Благодаря анонимности и удаленности, обеспечиваемой цифровыми технологиями, киберсталкеры часто могут действовать безнаказанно, не опасаясь быть пойманными.

Тем не менее, разрабатываются новые методы и технологии, которые помогут расследовать и обнаруживать киберпреследования. Одним из наиболее эффективных методов является цифровая криминалистика, которая включает анализ цифровых устройств и данных для сбора доказательств, которые могут быть использованы в суде. С помощью цифровой криминалистики можно анализировать широкий спектр цифровых доказательств, включая электронные письма, мгновенные сообщения, сообщения в социальных сетях и даже данные GPS с мобильных устройств [1].

Анализируя эти доказательства, сотрудники полиции часто могут установить преступника, совершившего киберпреследование, и возбудить против него уголовное дело. В дополнение к цифровой криминалистике правоохранные органы также могут использовать искусственный интеллект (далее – ИИ) и машинное обучение для выявления и предотвращения киберпреследований. Эти технологии позволяют производить анализ больших объемов данных для выявления моделей поведения, указывающих на киберпреследование [3].

Однако важно отметить, что использование этих технологий должно осуществляться ответственным и этичным образом с соответствующими гарантиями для защиты частной жизни и гражданских свобод.

В целом, несмотря на то, что киберпреследование может быть сложным преступлением для расследования и обнаружения, использование цифровой криминалистики, искусственного интеллекта и машинного обучения может помочь правоохранным органам выявлять и преследовать киберпреследователей, обеспечивая правосудие для жертв и помогая предотвращать будущие преступления.

Однако киберпреследование становится все более серьезной проблемой и в России, и в других странах. По данным МВД России, количество случаев киберсталкинга в России в 2020 году увеличилось на 75% по сравнению с предыдущим годом. Одной из проблем в борьбе с киберсталкингом в России является отсутствие четких юридических определений и правил, касающихся этого вида поведения. Хотя в Уголовном кодексе России есть положения, касающиеся преследований и домогательств, эти положения конкретно не касаются киберпреследований или использования цифровых технологий для преследования или запугивания кого-либо.

Еще одной проблемой является отсутствие осведомленности и образования среди широкой общественности и правоохранных органов о киберпреследовании. Многие люди в России могут не признавать киберпреследование серьезной проблемой, а у правоохранных органов может не быть знаний и ресурсов, необходимых для эффективного расследования и судебного преследования таких случаев.

Киберпреследование – серьезная проблема, которая может иметь разрушительные последствия для ее жертв. Важно повысить осведомленность об этой проблеме и принять меры для ее предотвращения и решения. Это включает в себя информирование людей о рисках киберпреследования, разработку эффективных правовых рамок для решения этой проблемы, а также предоставление поддержки и ресурсов жертвам.

В целом решение проблемы киберпреследования в России потребует многогранного подхода, включающего совершенствование правового регулирования, повышение осведомленности и информированности о проблеме, а также решение проблем, связанных с государственным надзором и конфиденциальностью в Интернете.

Библиографический список

1. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4(13).
2. Статистика киберпреступлений 2023 – Защита от скликивания рекламы [Электронный ресурс]. – URL: <https://clickfraud.ru/statistika-kiberprestuplenij-2022> (дата обращения: 10.04.2023).
3. Iskusstvennyj_intellekt_budushchee_borby_s_kiberprestupnostyu [Электронный ресурс]. – URL: <https://club.cnews.ru/blogs/entry/> (дата обращения: 10.04.2023).

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В КОНТЕКСТЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Меняйло Д.В.,

кандидат юридических наук, доцент;

Меняйло Л.Н.,

кандидат политических наук;

Горковенко В.С.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: на протяжении всей истории информация, которая передавалась различными способами, будь то словесный способ или какое-то письменное извещение, служила значимым источником передачи сведений, несущих в себе как позитивный характер, так и негативный. С развитием общества происходило и преобразование системы обмена информацией, в связи с этим внедрялись и распространяли свое влияние средства массовой информации, сегодня в том числе существующие в виде сайтов, форумов, социальных сетей и блогов. Поэтому основная роль по передаче корректного и правильного отображения действительности в немалой степени отводится сети Интернет. Сама по себе информационная система непосредственно зависит от своего содержания, точности и уместности. Достоверность передаваемых сведений оказывает различное влияние, понимание и восприятие со стороны общества. Именно поэтому необходим тщательный контроль государства за данными процессами.

Ключевые слова: информационное противоборство, противоправный контент, информационная безопасность.

SOME ASPECTS OF INFORMATION SECURITY OF THE ACTIVITIES OF INTERNAL AFFAIRS BODIES IN THE CONTEXT OF INFORMATION WARFARE

Menyailo D.V.,

Candidate of Law, Associate Professor;

Menyailo L.N.,

Candidate of Political Sciences;

Gorkovenko V.S.

(Putilin Belgorod Law Institute of Ministry of the Internal of Russia)

Abstract: throughout history, information that was transmitted in various ways, whether verbal or some kind of written notification, has served as a significant source of transmitting information that carries both a positive and negative character. With the development of society, there was also a transformation of the information exchange system, in connection with this, the mass media, including those existing in the form of websites, forums, social networks and blogs, were introduced and spread their influence. Therefore, the main role in transmitting the correct and correct representation of reality is largely assigned to the Internet. The information system itself directly depends on its content, accuracy and relevance. The reliability of the transmitted information has a different impact, understanding and perception on the part of society. That is why careful state control over these processes is necessary.

Keywords: information confrontation, illegal content, information security.

Современному обществу необходим тщательный контроль государства за процессами обмена информацией. Информация может представлять собой большую силу, сравнимую с оружием массового поражения. Информационная безопасность является одним из важнейших направлений национальной безопасности, особенно в контексте нарастающего информационного противоборства. Могут распространяться, навязываться разные информационные конфликты, искажение или вовсе предоставление субъектами информации ложных сведений, которые способны оказывать значительное влияние на социальные группы. В информационном поле сегодня наблюдается достаточно серьезное информационное противоборство.

При этом под информационным противоборством понимается «противоборство с использованием всего спектра информационных возможностей, осуществляемое в целях достижения информационного превосходства над противником» [1]. Также под информационным противоборством понимается борьба в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы противоборствующей стороны в то же время с защитой собственной информации, информационных систем и информационной инфраструктуры от подобного воздействия. Конечной целью информационного противоборства является завоевание и удержание информационного превосходства над противоборствующей стороной.

По своей сути информационное противоборство – это некие конфликты, которые возникают с разнообразием, выражением и обобщением информации. В науке более распространен термин «информационная война», которая определяется как:

- точное вредоносное воздействие субъектов с помощью всех средств, методов и способов воздействия на социальные процессы и общественные отношения с полномасштабным использованием информационных технологий;
- скрытое влияние информации на индивидуальное, групповое и массовое сознание такими способами, как дезинформация, пропаганда, манипулятивное вкладывание в формирующееся сознание или перепрограммирование разума, дабы сформировать новые «нужные» взгляды на социальную жизнь общества.

Среди объектов информационного противоборства принято выделять системы отношений информационного общества социального, политического и психологического характера [2].

Информационное противоборство в настоящее время больше всего происходит в виртуальном пространстве – сети Интернет. Во Всемирной паутине идет активное «зомбирование» людей как в индивидуальном порядке, так и массово внушается в сознание людей определенная информация, формируются установки.

Западноевропейские представители массмедиа, правительственных кругов в последние несколько лет активно создают негативный образ России в глазах мирового сообщества, переписывают историю, невзирая на достоверность исторических фактов. Пытаются принизить роль СССР в победе над фашизмом. Все это проходит в рамках информационного противоборства.

Помимо искажения исторических фактов со стороны «западных партнеров» в негативном ключе описываются и современные отечественные социально-экономические реалии в России. Такое негативное информационное поле сказывается на неокрепшем сознании российской молодежи, что влияет на уровень и качество преступности, борьба с которой осуществляется сотрудниками органов внутренних дел.

Сотрудники органов внутренних дел в последнее время все чаще сталкиваются с преступными последствиями применения «информационного оружия» – это проявления русофобии и действий экстремистского характера и т.д. Учитывая масштабы информационной агрессии в рамках «информационного противостояния» против всего российского, действий только представителей государственных органов, в том числе и сотрудников органов внутренних дел, недостаточно. Здесь необходимо проводить активную профилактическую работу по противодействию противоправному контенту с привлечением институтов гражданского общества (например, общественных организаций, движений). Распространение получают создаваемые в различных регионах «кибердружину», которые специализируются на выявлении как отдельных видов, так и всего массива незаконной информации, находящейся в сети Интернет. Сотрудничество таких добровольных молодежных формирований с органами внутренних дел осуществляется на регулярной основе.

В последние несколько лет количество фейковой информации, носящей деструктивный характер по отношению к основам российского государства и общества, увеличилось значительно. Такой информации необходимо противостоять информационно и идеологически даже среди самих сотрудников органов внутренних дел: проводить разъяснительные беседы в части особенностей проводимой государством информационной политики и обеспечения информационной безопасности как одного из направлений национальной безопасности.

Деятельность сотрудников органов внутренних дел сопряжена с нахождением в едином информационном пространстве с преступниками. Что негативно сказывается на мировоззрение многих сотрудников и выражается в их профессиональной деформации, которая усиливается пропорционально выслуге лет в ОВД. Стрессовое состояние сотрудника является благодатной почвой для проникновения в его сознание противоправного контента.

С развитием технологий более доступными стали видео- и фотосъемка. В некоторых случаях «недоброжелатели» сотрудников ОВД могут спровоцировать негативно развивающуюся ситуацию. И нередко вырванную из контекста информацию используют в целях порочения деятельности сторонников ОВД.

Немаловажным для сотрудников органов внутренних дел является сохранение государственной и служебной тайны. Особенно в условиях проведения специальной военной операции на территории Украины. Когда возможная цена утечки информации – это человеческая жизнь.

Таким образом, для того чтобы обеспечить информационную безопасность сотрудников и граждан в целом, в первую очередь необходимо заняться реализацией мер информационно-психологической защиты. Настоящие обстоятельства и условия в системе органов внутренних дел показывают отсутствие систематизированной программы работы с кадрами, которая в комплексе обеспечила бы высокую степень защищенности сотрудников от информационных угроз, распространяемых в сети Интернет. Кроме того, в условиях нарастающего противоборства цивилизаций, культур и нападок на сотрудников органов внутренних дел необходимо осуществлять противодействие противоправному контенту.

Библиографический список

1. Еременко В.Т., Рязанцев П.Н. Информационное противоборство в социотехнических системах: учебное пособие. – Орел: ОГУ имени И.С. Тургенева, 2016. – 10 с.
2. Разуваев В.Э. Правовые средства противостояния информационным войнам: автореф. дис. ... канд. юрид. наук. – Москва, 2007. – 24 с.
3. Курдюкова В.Ю. Информационная безопасность сотрудников органов внутренних дел и защита от информационно-психологического воздействия / Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований: материалы Всероссийской научно-практической конференции, Санкт-Петербург, 2002 год. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2022. С. 127–133.

4. Меняйло Д.В. Меры по противодействию противоправному контенту, пропагандирующему наркотические средства в сети интернет / Д.В. Меняйло, О.Е. Карпушин, К.К. Крупенникова / Противодействие незаконному обороту наркотиков в условиях цифровизации общества: сборник материалов Международной научно-практической конференции, Белгород, 17 ноября 2022 года. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2023. С. 96–100.

ИСПОЛЬЗОВАНИЕ IT-ТЕХНОЛОГИЙ (МЕССЕНДЖЕРА TELEGRAM) В ЦЕЛЯХ ПРАВОВОГО ПРОСВЕЩЕНИЯ НАСЕЛЕНИЯ И ПРОФИЛАКТИКИ КИБЕРМОШЕННИЧЕСТВА

Нестеренко И.С.,

кандидат педагогических наук;

Бровченко С.Ю.

(Краснодарский университет МВД России)

Аннотация: в статье рассматривается проблема правового просвещения населения по вопросам профилактики кибермошенничества, где платформа Telegram выступает как качественный и эффективный инструмент, использование которого определяет актуальность использования данного мессенджера.

Ключевые слова: информационные технологии, платформа Telegram, правовое просвещение, кибермошенничество, киберпреступность.

USING IT TECHNOLOGIES (TELEGRAM MESSENGER) FOR THE PURPOSE OF LEGAL EDUCATION OF THE POPULATION AND PREVENTION OF CYBERBULLYING

Nesterenko I.S.,

Candidate of Pedagogical Sciences;

Brovchenko S.Yu.

(Krasnodar University of the Ministry of Interior of Russia)

Abstract: the article deals with the problem of legal education of the population on the prevention of cyberbullying, where the Telegram platform acts as a high-quality and effective tool, the use of which determines the relevance of the use of this messenger.

Keywords: information technologies, Telegram platform, legal education, cyberbullying, cybercrime.

Социальные сети и мессенджеры уже давно вошли обиход в современном обществе. Помимо возможности общения данные платформы позволяют оперативно обмениваться различным объемом информации в разных форматах.

Стоит отметить, что социальные сети сильно изменились с момента их создания, активное внедрение новых технологий позволяет превратить рассматриваемые платформы в отдельные информационные пространства, на которых появляется возможность осуществлять денежные транзакции, покупать товары и различные услуги, заниматься бизнесом, играть в компьютерные и мобильные игры, обучаться, а некоторые сервисы даже позволяют следить за здоровьем.

Однако активное развитие возможностей и распространенности социальных сетей и мессенджеров привлекает внимание кибермошенников, которые видят в этом благоприятную среду для осуществления преступной деятельности. Злоумышленников привлекает большое количество пользователей, что обуславливает широкий выбор жертвы, также большую роль играют особенности осуществления преступлений в киберпространстве.

Поэтому использование потенциала социальных сетей и мессенджеров для правового просвещения населения на данный момент имеет важное значение, так как появляется возможность осуществлять цели правового просвещения и одновременно предупреждать преступления, совершаемые в киберпространстве.

Для реализации целей правового просвещения населения может быть использована платформа Telegram.

На данный момент это приложение позиционируется как кроссплатформенная система мгновенного обмена сообщениями, иначе говоря, мессенджер с возможностью предоставления информации в текстовой, графической, звуковой форме. Функционал данного мессенджера позволяет пользователю обмениваться, помимо привычных текстовых сообщений, голосовыми и видеосообщениями, стикерами и фотографиями, а также файлами многих форматов.

Определяющим значением использования в процессе правового просвещения рассматриваемого мессенджера является одна из форм коммуникации, которую предоставляет Telegram. Речь идет о telegram-каналах, позволяющих:

- делиться информацией с неограниченным или ограниченным кругом лиц, используя для этого публичные или частные каналы;
- оставаться их создателям и абонентам анонимными, информация о участниках канала будет доступна только его администратору;
- ограничить обратную связь посредством отсутствия возможности у пользователей делиться своим мнением непосредственно в ленте канала, для этого им может быть предоставлен отдельный канал для обсуждений или возможность обсуждать только конкретно определенный пост.

Эти характеристики telegram-каналов позволяют эффективно использовать данный мессенджер как инструмент правового просвещения.

Важно отметить, что для успешного правового просвещения населения необходимо использовать современные виды предоставления профилактической информации, так как это вызывает большую заинтересованность у людей, за счет предоставления информации в формах, с которыми они постоянно встречаются, являющихся для них уже привычными.

Из вышесказанного можно сделать вывод, что в вопросе правового просвещения населения по вопросам профилактики кибермошенничества Telegram выступает как качественный и эффективный инструмент, использование которого определяет актуальность использования данного мессенджера и функционал, который он может предоставить.

Практической частью данной работы является разработка примера telegram-канала с профилактической информацией, направленной на правовое просвещение населения в вопросе профилактики кибермошенничества.

Выбор данного мессенджера, как уже отмечалось, обуславливается:

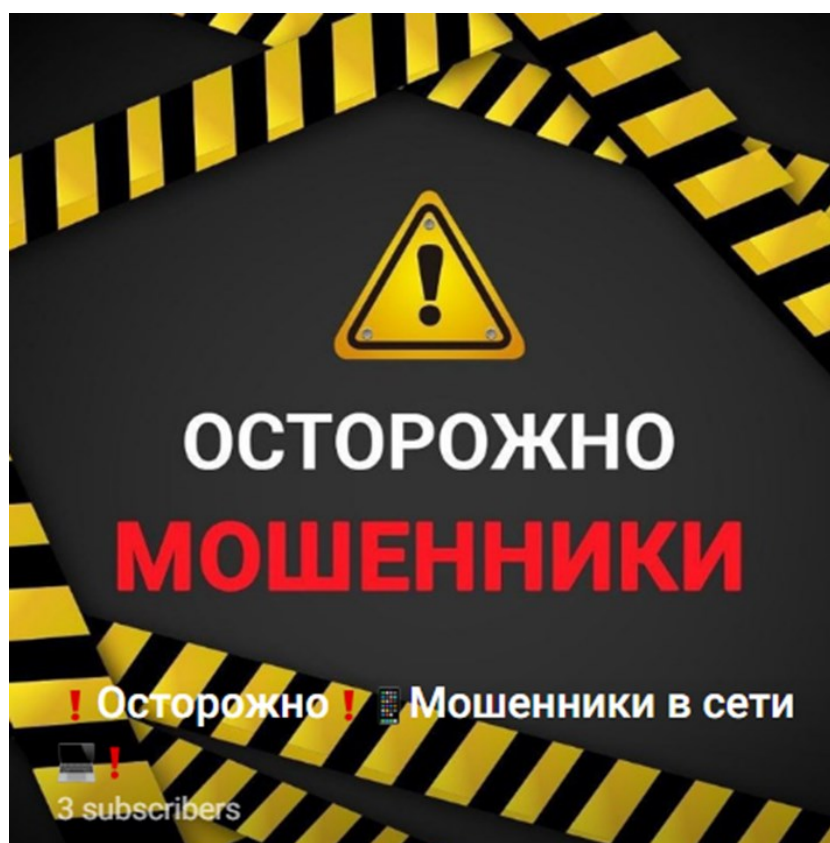
- 1) широкой востребованностью использования данного мессенджера среди пользователей;
- 2) разнообразным функционалом платформы, позволяющим предоставлять профилактическую информацию в различных формах;
- 3) возможностью создателям канала оставаться анонимными;
- 4) распространением информации на неограниченный или ограниченный круг лиц.

Канал создан для того, чтобы показать, каким образом можно осуществлять правовое воспитание населения посредством мессенджера Telegram и представлять профилактическую информацию, которая может быть донесена до сведения пользователей.

Канал называется «! Осторожно! Мошенники в сети!».

Тип канала: частный. Возможность обсуждать посты и оставлять реакции ограничена для подписчиков канала, также имя администратора канала не отображается в подписях к постам. В шапке канала закреплён текст: «Данный канал создан с целью профилактики одной из актуальных проблем современной России – кибермошенничества».

Также имеется ссылка-приглашение для присоединения к каналу: <https://t.me/+NJAjNjKDYSUyZmM6> (см. рис. 1).



 Данный канал создан с целью профилактики одной из актуальных проблем современной  России -  кибермошенничество .
Bio

 <https://t.me/+NJAjNjKDYSUyZmM6>
Link

 Notifications 

Рисунок 1. Скриншот шапки профиля канала

В канале предоставляется контент в форме предупредительных изображений, памяток в виде изображений, пост с ссылкой для перехода на сайт с профилактической информацией, пост с ссылкой на публикацию другого канала, содержащей информацию профилактического характера, пост с ссылкой на видеоролик, размещенный в социальной сети, пост с ссылкой на статью (см. рис. 2).

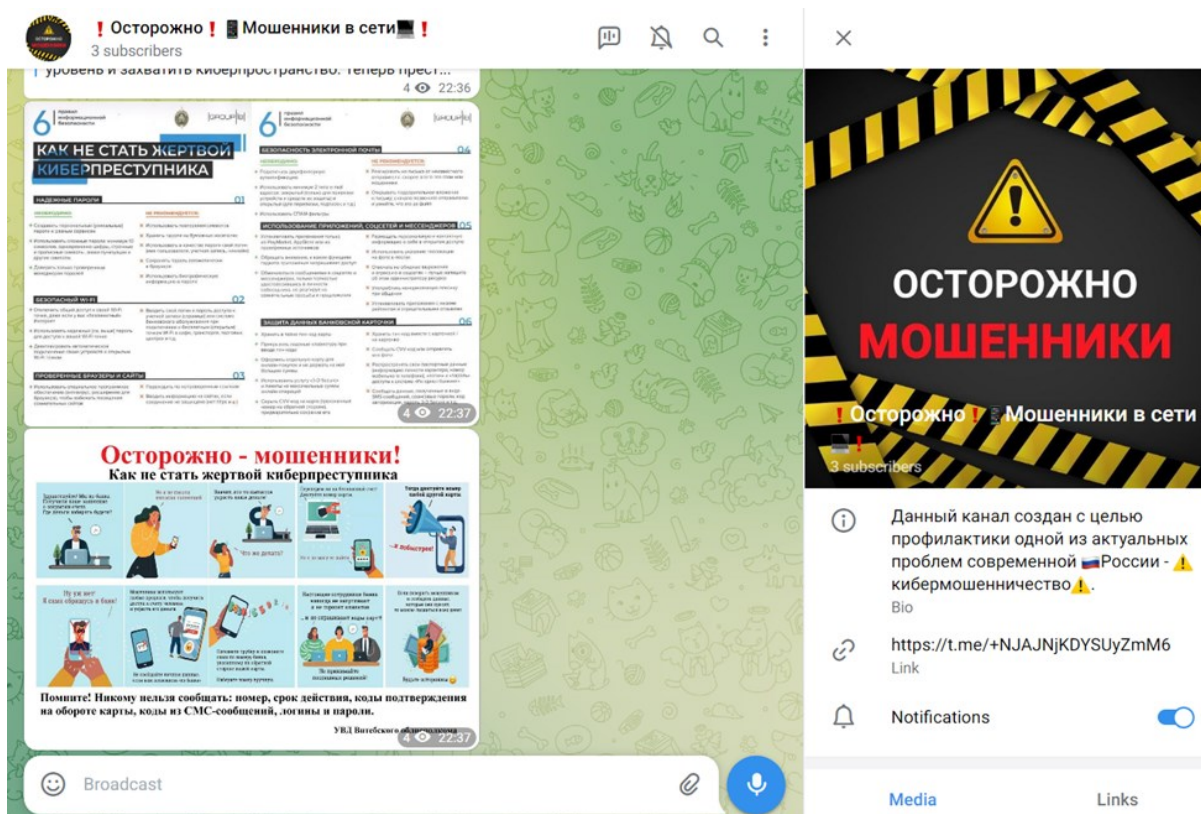


Рисунок 2. Скриншот памяток в виде изображений

На рисунке 2 представлены две памятки, содержащие профилактическую информацию. На первой из них указывается 6 правил информационной безопасности, соблюдение которых позволит не стать жертвой киберпреступников. Памятка разделяется на 6 блоков: надежные пароли, безопасный WI-FI, проверенные браузеры и сайты, безопасность электронной почты, использование приложений, соцсетей и мессенджеров, защита данных банковских карт. К каждому блоку прилагаются соответствующие рекомендации, а также то, что не рекомендуется делать.

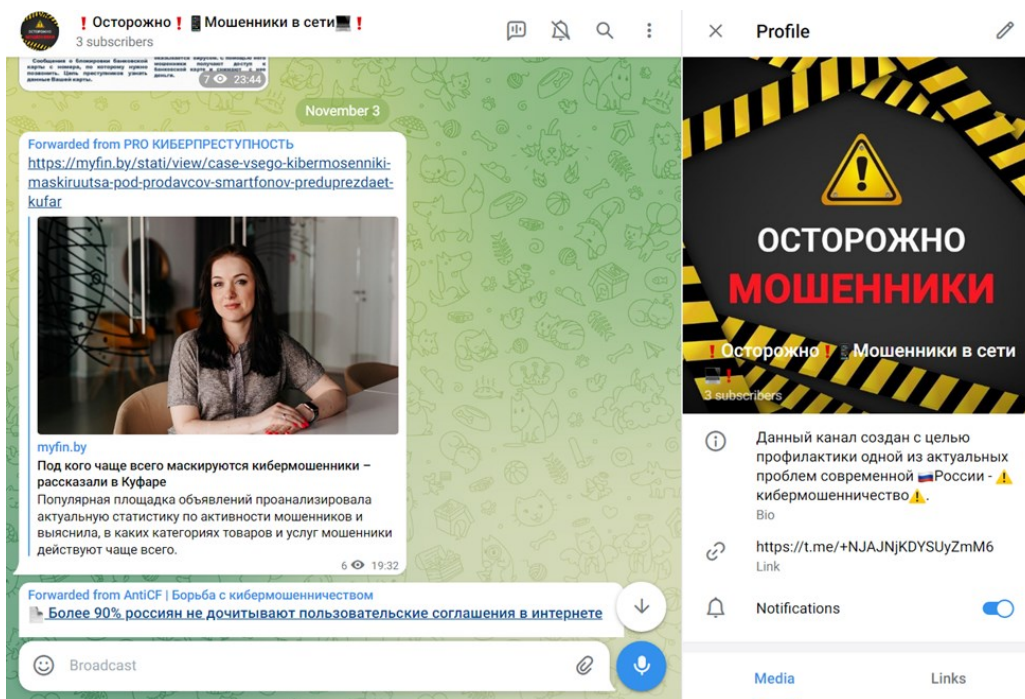


Рисунок 3. Скриншот поста со ссылкой для перехода на сайт с профилактической информацией

На данной иллюстрации показан пост со ссылкой на сайт MYFIN.by, где мы сможем ознакомиться со статьей «Под кого чаще всего маскируются кибермошенники», в которой авторы дают рекомендации по поводу того, на что стоит обращать внимание при проведении сделок. Также предупреждают, что покупая или продавая что-то в интернете, стоит проявлять разумную осторожность и осмотрительность (см. рис. 3).

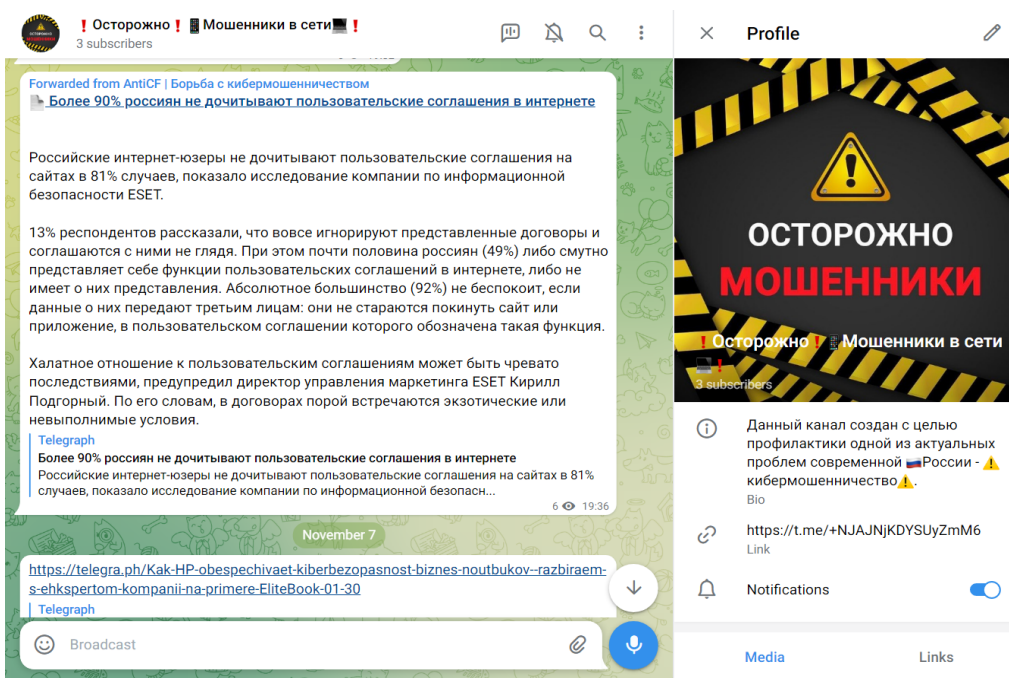


Рисунок 4. Скриншот поста со ссылкой на публикацию другого канала

На рисунке 4 представлен пост со ссылкой на опубликованную статью другим telegram-каналом. В данной статье пользователя предупреждают о том, что необходимо всегда ознакомиться с пользовательским соглашением в интернете прежде, чем его принять.

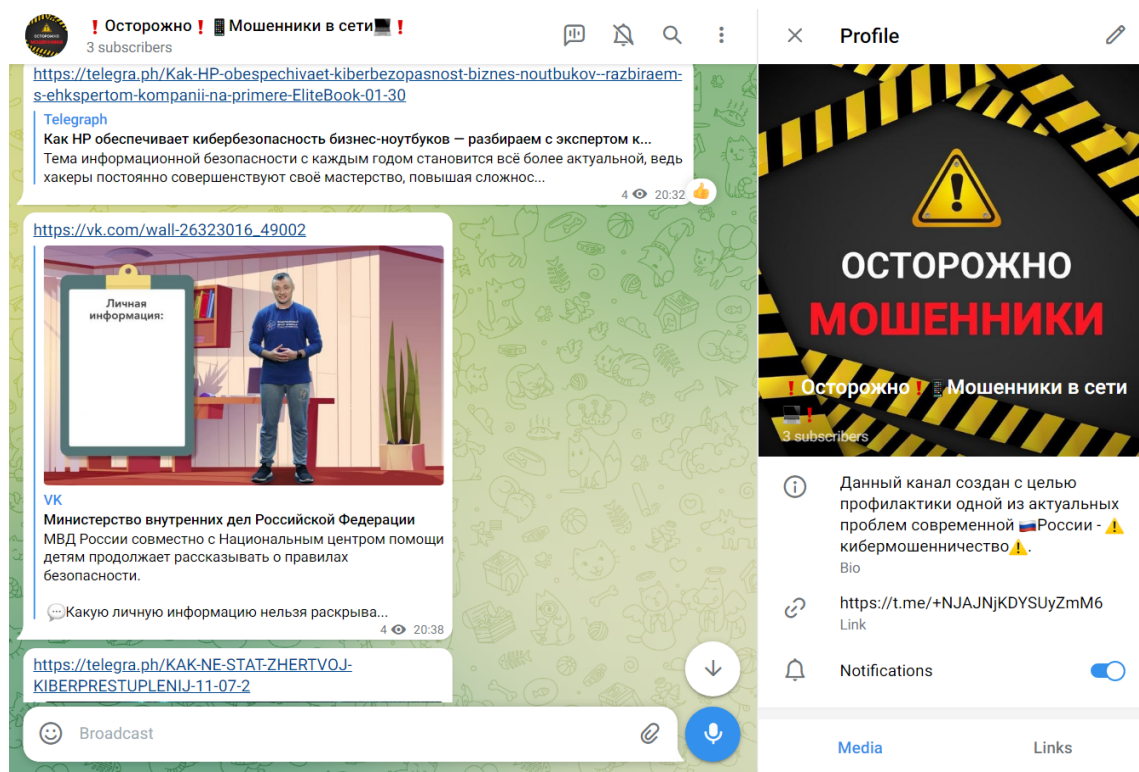


Рисунок 5. Скриншот поста со ссылкой на видеоролик, размещенный в социальной сети

На рисунке 5 можно ознакомиться со ссылкой на видеоролик, который размещен в социальной сети «ВКонтакте».

В данном видеоролике доводится профилактическая информация по безопасности в Интернете, при этом форма подачи информации рассчитана на детскую аудиторию. Вся информация сопровождается анимированными зарисовками, а также пояснениями от представителя «Национального центра помощи детям».

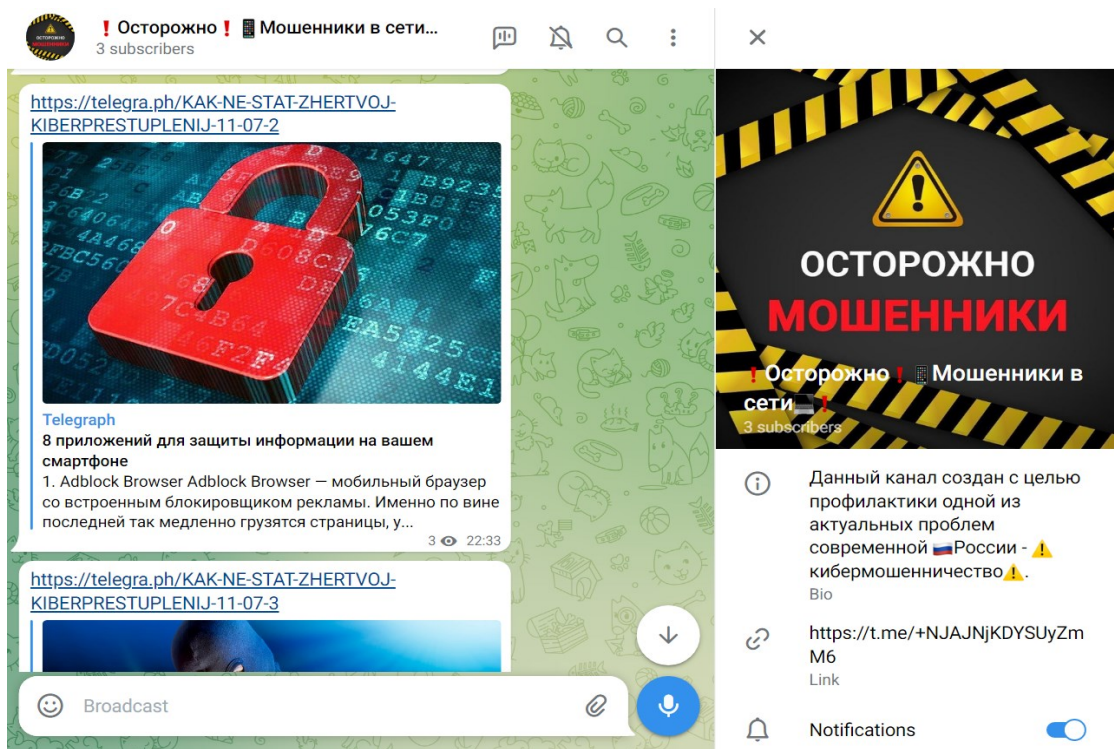


Рисунок 6. Скриншот поста со ссылкой на статью

На рисунке 6 показан пост со ссылкой на статью, в которой рассказывается про приложения, которые позволят пользователю защитить конфиденциальную информацию на своем устройстве, избежать нежелательного прослушивания разговоров, воспрепятствовать шпионским программам и вирусам получить доступ к видеокамере устройства и прочее.

Данная разработка может послужить примером того, как может быть реализовано направления правового просвещения в вопросе профилактики кибермошенничества, используя потенциал мессенджера Telegram, также активное научное исследования данного вопроса позволит создавать профилактический контент для размещения в каналах, созданных непосредственно с целью информирования пользователей по вопросам правового просвещения.

Подводя итог, можно отметить, что развитие информационных технологий закономерно ведет и к развитию возможностей киберпреступников, поэтому для борьбы с ними нужно активно изучать данные технологии, чтобы разработать эффективные методы и средства, которые способны будут дать правоохранительным органам возможность противостоять новому виду преступности на должном уровне.

Библиографический список

1. Лебединская А.В. Способы разработки психологического портрета предполагаемого лица, совершившего преступление // Вестник науки и образования. 2019. № 21–2 (75). С. 43–46.

2. Андреева Е.Е., Морозов Г.Б. Об эффективных формах правового просвещения граждан Российской Федерации // Педагогическое образование в России. 2016. № 1. С. 75–81.

3. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45–55.

4. Богданов А.В., Ильинский И.И., Хазов Е.Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15–20.

5. Мяханова А.Н., Гунзынов Ж.П. К вопросу об использовании Telegram-каналов как инструмента профилактики правонарушений // Уголовно-исполнительное право. 2019. Т. 14(1–4). № 4. С. 390–393.

ИНТЕРНЕТ-МАГАЗИН КАК СРЕДСТВО РЕАЛИЗАЦИИ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

Новоселов Н.Г.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются некоторые особенности осуществления деятельности интернет-магазинов по реализации наркотических средств и психотропных веществ. Анализируются технические возможности онлайн-магазинов и использование ими различных платформенных систем и комплексных приложений.

Ключевые слова: интернет-магазин, сбыт, наркотические средства, психотропные вещества, оборот наркотиков.

ONLINE STORE AS A MEANS OF SELLING NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES

Novoselov N.G.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article discusses some features of the implementation of the activities of online stores for the sale of narcotic drugs and psychotropic substances. The technical capabilities of online stores and their use of various platform systems and complex applications are analyzed.

Keywords: online store, sales, narcotic drugs, psychotropic substances, drug trafficking.

На современном этапе преступления в сфере незаконного оборота наркотиков представляют серьезную проблему не только для Российской Федерации, но и для всего мира. Помимо того что наркотические средства и психотропные вещества ведут к наркотизации населения и деградации общества, его культурных и моральных устоев, они еще и являются одной из причин совершения наркозависимыми гражданами корыстных и насильственных преступлений. От того, насколько качественно и эффективно будет организована борьба с незаконным оборотом наркотиков, зависит благополучие всего общества, государства в целом и каждого гражданина в частности.

Сегодня деятельность организованных преступных групп в сфере незаконного оборота наркотиков перешла в бесконтактную плоскость, которая выражается в предоставлении преступных услуг посредством сети Интернет, в том числе с использованием в этой деятельности интернет-магазинов.

Так, например, в соответствии со статистическими данными о результатах деятельности МВД России за 1 квартал 2023 года с использованием информационно-телекоммуникационных технологий совершалось практически каждое третье преступление, три четверти (75,6%) с использованием сети Интернет (152 434 +22,7%), а каждое седьмое – в сфере незаконного оборота наркотиков (21 339, +57,0%) [1].

Осуществление оптовой и розничной торговли наркотиками через интернет-магазин имеет ряд существенных преимуществ для преступников:

- возможность осуществлять свою деятельность по распространению наркотических средств и психотропных веществ во всех регионах страны;
- анонимность при работе в сегменте Интернета;
- конспиративность действий преступников;
- использование в работе лиц, имеющих профессиональные и специальные знания в области высоких технологий.

Онлайн-магазины по реализации наркотиков являются зеркальным отражением обычного среднестатистического интернет-магазина, только находится он не в привычной Сети, а в скрытом сегменте Интернета – DarkNet, в который невозможно попасть при использовании стандартного браузера.

Сайты наркоторговцев осуществляют свою деятельность в лучших традициях современного менеджмента, вырабатывая стратегию продвижения товара на рынок услуг, используя при этом системы рекламных акций, скидок, дегустаций, пробников и др. Кроме того, здесь можно найти нужный наркотик, определить способ его доставки или получения, выбрать удобный способ оплаты. При возникновении каких-либо трудностей помощь окажет опытный менеджер-консультант.

Рассматривая технические возможности онлайн-магазинов, необходимо отметить, что они в своей деятельности активно используют:

- платформенные системы, предназначенные для передачи фотоизображений закладок;
- различные комплексные приложения, позволяющие передавать клиентам точные координаты мест нахождения тайников;

– приложения, имеющие функцию самоудаления и удаления их по желанию отправителя [2];

– приложения, обеспечивающие невозможность определения IP-адресов, с которых осуществляется посещения веб-сайтов;

– шифрованные VPN-соединения, позволяющие обходить блокировку сайта не только государственными органами, но и самими интернет-провайдерами.

Таким образом, располагая знаниями в области технических возможностей и особенностях деятельности интернет-магазинов, осуществляющих реализацию наркотических средств и психотропных веществ, сотрудник оперативных подразделений органов внутренних дел имеет возможность эффективно использовать оперативно-разыскные мероприятия и следственные действия для борьбы с незаконным оборотом наркотиков.

Библиографический список

1. Состояние преступности в России за январь-март 2023 года [Электронный ресурс]. – URL: [http: // www.mvd.ru](http://www.mvd.ru) (дата обращения: 20.01.2022).

2. Земцова С.И. Интернет-магазины, осуществляющие незаконный сбыт синтетических наркотических средств: дифференсация и характерные признаки // Вестник Сибирского юридического института МВД России. 2019. № 1. С. 36–41.

ВНЕДРЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Пантелеева Е.В.;

Куриленко Ю.А.,

кандидат юридических наук

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в современном мире значительную роль играют информационные технологии, с помощью которых люди могут облегчить себе жизнь. За счёт внедрения цифровых технологий во все сферы общественной жизни происходит автоматизация и модернизация человеческой цивилизации, упрощается процесс коммуникации, передача знаний и информации, повышается эффективность работы. В первую очередь это необходимо для повышения качества услуг и замены устаревших способов новейшим цифровым инструментом. В деятельности правоохранительных органов цифровые технологии являются одним из основополагающих факторов, позволяющих облегчить процесс поимки преступников, раскрытия преступлений. В статье авторы обозначают основные направления применения цифровых технологий. Анализируя имею-

щиеся информационные технологии в деятельности правоохранительных органов, авторы приходят к заключению о необходимости подготовки квалифицированных в области цифровых технологий сотрудников правоохранительной деятельности.

Ключевые слова: цифровизация, цифровые технологии, информационные технологии, правоохранительная деятельность, правоохранительные органы.

IMPLEMENTATION OF DIGITAL TECHNOLOGIES IN THE ACTIVITY OF LAW-ENFORCEMENT AGENCIES

Panteleeva E.V.;

Kurilenko Y.A.,

Candidate of Law Sciences,

(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: in the modern world information technologies play a significant role, with the help of which people can make their lives easier. Through the introduction of digital technology in all spheres of social life is automation and modernization of human civilization, simplifying the process of communication, transfer of knowledge and information, increasing the efficiency of work. First of all, it is necessary to improve the quality of services and to replace outdated methods with the latest digital tools. In the activities of law enforcement agencies, digital technology is one of the fundamental factors to facilitate the process of catching criminals, solving crimes. In the article, the authors outline the main areas of application of digital technology. Analyzing the available information technology in the activities of law enforcement agencies, the authors conclude that it is necessary to train law enforcement officers qualified in the field of digital technology.

Keywords: digitalization, digital technology, information technology, law enforcement, law enforcement agencies.

Началом цифровизации принято считать XX век, когда начали появляться первые компьютеры для проведения сложных вычислений в военной и научной сферах. В дальнейшем они совершенствовались, и по мере снижения цен на вычислительную технику становились более доступными и востребованными. С созданием мобильных телефонов люди смогли гораздо быстрее взаимодействовать между собой, распространять информацию. Таким образом, при внедрении цифровых технологий, обеспечивающих передачу и распределение информации в доступной форме на уровне различных телекоммуникационных сетей, во все сферы общественной жизни усовершенствовались и упрощались процессы автоматизации, передачи информации, коммуникации, что значительно повысило эффективность человеческой деятельности.

В деятельности правоохранительных органов цифровые технологии играют немаловажную роль. Безусловно, как и в любой сфере деятельности, в ор-

ганах внутренних дел различают многосторонность применения информационно-коммуникационных технологий. Так, С.Н. Токарева выделяет в информатизации органов правопорядка следующие направления:

- 1) электронный документооборот (ведение электронного делопроизводства);
- 2) организация коммуникации с обществом;
- 3) использование информационных технологий в работе правовых подразделений системы МВД России [1, с. 590].

Комментируя данную классификацию, отметим, что, во-первых, отсутствие бумажной «волокиты», четкая систематизация и упорядочивание данных, «прозрачность» электронного документооборота, бесспорно, позволяют экономить время. Во-вторых, зона доступности правоохранительных органов для общества также весьма расширилась. Цифровые технологии позволяют обеспечить равный доступ к важной информации с помощью социальных сетей и других онлайн-сервисов, информировать о происходящих событиях, изменениях в законодательстве, просить помощи при поимке преступников. Сегодня любой гражданин на сайтах правоохранительных органов может не только найти своего участкового, его телефон, но и обратиться напрямую к руководителю любого уровня посредством электронного сообщения. В-третьих, деятельность правовых подразделений органов внутренних дел связана с большим количеством использования, обработки нормативно-правовой информации, которая постоянно обновляется, дополняется новыми документами. И в этой связи применение информационных технологий, а именно использование в деятельности правовых подразделений МВД России справочно-правовых систем в первую очередь, позволяет не только облегчить работу, но и сэкономить такой важный ресурс, как время.

Но, по нашему мнению, одним из главных направлений по применению цифровых технологий в деятельности правоохранительных органов все же следует определить деятельность по раскрытию и расследованию преступлений, в частности преступлений информационной направленности. Именно информационные технологии позволяют сотрудникам органов внутренних дел с наибольшей точностью находить улики, осуществлять розыск лиц, пропавших без вести и скрывающихся от закона, а также хранить большие объемы информации о преступниках, преступлениях, жертвах и свидетелях. Для этих целей были созданы специализированные автоматизированные информационные системы (АИС), отдельные программные продукты.

Так, говоря о работе судебных экспертов, следует отметить, что использование цифровых технологий в данной деятельности предполагает создание субъективных портретов, проведение экспертизы, снятие отпечатков и следов, обнаружение, фиксацию, изъятие и исследование в целях криминалистической регистрации личности. К примеру, для дактилоскопического учета в 1989 году была создана АДИС «Папилон». В настоящее время данная система получила свое продолжение в системе биометрической идентификации ПАПИЛОН «Фильтр», позволяющей проводить дактилоскопическую идентификацию в режиме реального времени. Специализированная программа «БиоНейроАвтограф», предназначенная для проведения почерковедческой экспертизы, позво-

ляет сравнить несколько образцов почерка с целью идентификации исполнителя. С помощью аппаратно-программного комплекса «ВОКОРД Видеозапись» имеется возможность распознавать лица по фото и видеозаписям по признакам внешности, а также позволяет при помощи корректировки улучшить качество фото и видеозаписей [2, с. 43–44]. Система распознавания лиц помогает бороться с мошенничеством, кражами, обеспечивать эффективную поимку преступников и не допускать ложных обвинений в адрес невиновных лиц, то есть исключить подозреваемых из списка потенциальных преступников.

Следует отметить, что система видеонаблюдения является одним из иллюстрирующих примеров использования информационных технологий в деятельности многих подразделений правоохранительных органов. С её помощью осуществляется процесс визуального наблюдения за территорией: улицы города, общественные места, дома, квартиры, коммерческая недвижимость. Системы видеонаблюдения нужны для того, чтобы обеспечивать безопасность, отслеживать попытки проникновения. С помощью них можно восстановить данные о том, кто и в какой период времени находился рядом с тем или иным объектом, а также предотвратить преступления самим фактом наличия таких устройств.

Кроме того, существенным направлением применения цифровых технологий в деятельности правоохранительных органов является обеспечение взаимодействия между самими сотрудниками, различными отделами и подразделениями. Необходимо владеть информацией, передавать данные и координировать действия при раскрытии преступлений с помощью технических средств, а также специальных программ по обмену информацией.

В рамках рассматриваемого вопроса по внедрению цифровых технологий нельзя не отметить, что важнейшей задачей на сегодняшний момент является подготовка специалистов и сотрудников правоохранительных органов, которые свободно владеют различными информационными технологиями, включая мобильные и интернет-технологии, а также осуществляющие дальнейшее совершенствование в данной сфере.

Использование информационных технологий помогает правоохранительным органам более эффективно бороться с преступностью, повышать точность и оперативность расследования, автоматизировать процесс раскрытия преступлений, идентифицировать преступников, ускорять процесс обработки, хранения, передачи большого количества данных, что значительно упрощает расследование. Немаловажна роль технологий для обеспечения безопасности и информированности граждан и правоохранительных органов. Однако в случае использования информационных технологий в корыстных целях или при недостаточной подготовке сотрудников правоохранительных органов могут возникнуть риски нарушения прав граждан. Поэтому необходимо соблюдать законы и соответствующие правила, принципы этики при использовании цифровых технологий. Только квалифицированные и подготовленные сотрудники при помощи таких технологий для раскрытия и расследования преступлений смогут обеспечить эффективную борьбу с преступностью и защитить права и свободы граждан.

Библиографический список

1. Токарева С.Н. Цифровизация в деятельности органов правопорядка / Россия: тенденции и перспективы развития, Москва, 6–7 июня 2019 года / Институт научной информации по общественным наукам РАН; отв. ред. В.И. Герасимов. Выпуск 14. Ч. 2. – Москва: Институт научной информации по общественным наукам РАН, 2019. С. 590–592.
2. Лебедев М.Д., Саввоев С.А. К вопросу об оптимизации судебно-экспертной деятельности в эпоху цифровизации // Скиф. Вопросы студенческой науки. 2021. № 3(55). С. 41–45.
3. Дюков А.В. О применении информационных технологий в правовом обеспечении организации и деятельности системы МВД России // Вестник Московского университета МВД России. 2009. № 7. С. 152–154.
4. Меняйло Д.В., Малявин Д.В. К вопросу об информационных технологиях на службе правопорядка / Экономическая безопасность: правовые, экономические, экологические аспекты: сборник научных статей 7-й Международной научно-практической конференции. – Курск, 2022. С. 270–272.

ЗНАЧИМОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

**Попадьяина В.А.,
Калашникова А.А.**

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье описываются различные виды информационных технологий, позволяющих выявлять террористическую активность в сети Интернет и бороться с ней. Оценивается значимость и роль информационных технологий в борьбе с терроризмом. Рассматриваются методы противодействия терроризму.

Ключевые слова: информационные технологии, террористическая активность, Интернет.

THE IMPORTANCE OF INFORMATION TECHNOLOGY FOR COUNTERING TERRORISM

Popadina V.A.;
Kalashnikova A.A.

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: the article describes various types of information technologies that allow you to detect and combat terrorist activity on the Internet. The importance and role of information technologies in combatting terrorism is assessed. Methods of countering terrorism are considered.

Keywords: Information technologies, terrorist activity, Internet.

В начале XXI века проблема терроризма приобрела глобальный характер. В последние годы участились попытки террористических актов, что стало одной из самых серьезных проблем на современном цивилизационном уровне. Терроризм оказывает вредоносное влияние на социальную, политическую, религиозную сферы, что позволяет говорить о том, какую угрозу он представляет в мировом масштабе – угрозу не только для государств, но и для человеческой цивилизации в целом. В связи со сложившейся обстановкой в мире государства стали объединять свои организации с целью уничтожения террористического воздействия на жизни людей. Огромную роль в объединении играют процессы глобализации, основу которых составляет сеть Интернет и информационные технологии.

Для борьбы с терроризмом в наше время создается широкий диапазон технологий и средств. Совершенствование информационных технологий является неотъемлемой частью решения проблемы. Информационные технологии (далее – ИТ) представляют из себя совокупность средств и методов хранения, обработки и передачи сведений с целью получения информации нового качества о каком-либо явлении. Инфраструктура ИТ также включает в себя глобальную сеть Интернет, и радиотелекоммуникационные связи, и персональные компьютеры. Что в совокупности помогает проводить анализ и решать проблему террористического влияния на человеческую цивилизацию.

Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» определяет виды террористических действий, которые представлены следующим образом [1]:

- подготовка террористического акта (уже является действием террористического характера);
- финансирование терроризма организациями;
- вооружение, обучение, использование навыков террористов;
- организация террористического акта;
- вербовка террористов и т.д.

Информационные технологии фиксируют террористическую активность в Интернете. Информация о готовящемся преступном деянии может находиться в различных источниках. Сбор, поиск, извлечение и ее обработка позволяют осуществлять манипуляции с данными. Поэтому большое значение приобретает технология визуализации. Она фиксирует данные в виде графических объектов, что повышает простоту ее восприятия и тем самым увеличивает ее эффективность.

Видеоинформация и ее обработка позволяют осуществлять анализ полученной информации о возможно опасных либо вызывающих подозрения действиях людей. Полученные данные, зафиксированные при видеосъемке, позволяют предсказывать дальнейший ход событий, их негативный исход и последствия. Здесь задействованы технологии прогнозирующего моделирования, в которых используют экспертный и событийный опыт.

Технологии манипулирования данными из множества источников информации обеспечивают сбор, извлечение, распространение информации из всей совокупности данных, что позволяет реализовать представления различных аспектов, соответствующих запросу.

Биометрические технологии особенно важны, так как имеют прямое отношение к человеческому фактору. Использование физиологических и поведенческих характеристик человека, таких как отпечатки пальцев, ладони, форма лица во всех проекциях и т.д., помогают идентифицировать человека и выявить его психологическое состояние на момент совершения деяния. Также данное направление развития информационных технологий поможет выявить возможные намерения человека при совершении преступления.

Технологии мониторинга данных оповещают работников о подозрительных активностях в сети Интернет и позволяют предотвратить критический исход планируемых событий.

На сегодняшний день в террористической активности используется и дактилоскопия, и обработка телефонных разговоров, и распознавание лиц по имеющимся фотографиям. Все это оказывает огромное влияние на борьбу с террористической деятельностью.

Актуально можно выделить следующие методы противодействия терроризму:

- блокировку каналов связи и вывод из строя террористических веб-сайтов;
- эксплуатацию информации с террористических веб-сайтов для получения данных о планируемых операциях;
- введение прямых законодательных ограничений.

Таким образом, информационные технологии являются ключевым звеном в современном мире при борьбе с терроризмом. Для устранения этой глобальной проблемы необходимо вырабатывать эффективный комплекс мер. Одной из таких является разработка и совершенствование информационных технологий, которые представляют собой сущность управления всеми критическими элементами инфраструктуры современной цивилизации.

Библиографический список

1. Федеральный закон «О противодействии терроризму» от 06.03.2006 № 35-ФЗ (последняя редакция) // СПС «КонсультантПлюс».
2. Основы противодействия терроризму: учебное пособие для студ. высш. учеб. заведений / Я.Д. Вишняков, Г.А. Бондаренко, С.Г. Васин [и др.]; под ред. Я.Д. Вишнякова. – Москва: Академия, 2006. – 240 с.
3. Противодействие терроризму и экстремизму [Электронный ресурс]. – URL: <https://arbat.mos.ru/countering-extremism/> (дата обращения: 10.04.2023).
4. Шевелев С.Г. Роль информационных технологий в борьбе с терроризмом // Законность и правопорядок в современном обществе. 2016. № 28. С. 53–57.

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

**Рыбальченко А.Ю.,
Коротков А.А.**

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: современное общество стоит на пороге четвертой информационной революции. Процессы глобализации и информатизации с каждым годом только усиливаются, и во все сферы жизни общества стремительно входят информационные технологии. Увеличивается объем и количество передаваемой информации, растет количество способов передачи данных.

Ключевые слова: информационные ресурсы, противодействие преступлениям, информационно-компьютерные технологии, IP-адрес, технические средства.

INFORMATION SUPPORT OF OPERATIONAL INVESTIGATIVE ACTIVITIES IN THE DETECTION OF CRIMES USING COMPUTER TECHNOLOGY

**Rybalchenko A.Yu.,
Korotkov A.A.**

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: modern society is on the threshold of the fourth information revolution. The processes of globalization and informatization are only intensifying every

year and information technologies are rapidly entering all spheres of society. The volume and quantity of transmitted information is increasing, and the number of data transmission methods is growing.

Keywords: information resources, crime prevention, information and computer technologies, IP address, technical means.

На сегодняшний день одним из ключевых факторов эффективности той или иной деятельности является работа с информацией, в том числе и в правоохранительной деятельности. Должное информационное обеспечение деятельности правоохранительных органов позволяет сотрудникам обеспечивать надежно защищать права и свободы человека и гражданина.

Особую роль информация играет при расследовании преступлений, в том числе с использованием информационно-компьютерных технологий. В целях совершенствования деятельности структурных подразделений МВД России по противодействию преступлениям был реализован ряд мер. Так, в 2006 году была создана Единая информационно-коммуникационная система органов внутренних дел, целью которой стало создание единой информационно-телекоммуникационной системы ОВД путем совершенствования информационного обеспечения МВД России посредством реконструкции и оборудования объектов ОВД новыми и перспективными телекоммуникационными и программно-техническими комплексами [1].

При осуществлении оперативно-разыскной деятельности сотрудники работают с различной информацией, такой как персональные данные граждан, сведения о регистрации, имеющихся транспортных средствах, оружии, действующих и утраченных паспортах, сведения о привлечении к уголовной и административной ответственности, похищенных номерных вещах, о выписке из единых государственных реестров юридических лиц и индивидуальных предпринимателей и многое другое.

Информационные ресурсы ОВД формируются не только из ведомственных учетов, но также из информации, предоставляемой различными государственными и муниципальными учреждениями, организациями. Своевременное получение информации существенно ускоряет многие вопросы, возникающие в процессе осуществления оперативно-разыскной деятельности.

Анализ статистических данных указывает на то, что, несмотря на существенное улучшение систем, обеспечивающих информационную безопасность, нельзя говорить о достаточности информационного обеспечения в системе МВД России. Сегодня имеется ряд вопросов, требующих внимания. К таким вопросам относится противодействие преступлениям, совершаемым с использованием информационно-компьютерных технологий. В целях противодействия таким преступлениям, правоохранительные органы должны иметь высокий профессиональный опыт и знания в области тактики и методики выявления указанных преступлений, раскрытия и расследования уголовных дел.

Остается актуальной проблема противодействия кражам и мошенничествам, совершенным с использованием информационно-компьютерных техно-

логий. Преступления такого рода характеризуются высокой степенью анонимности лица и его местоположения. Анонимность достигается путем смены IP-адреса с помощью сторонних программ (VPN, SSL, TOR) [2, с. 167]. Зачастую используются различные технологии для смены абонентского номера с помощью IP-телефонии. Таким образом, раскрыть преступления, совершенные с помощью информационных технологий, становится значительно труднее.

Первоначальными действиями при раскрытии преступлений с использованием компьютерных технологий являются оперативно-разыскные мероприятия, проводимые сотрудниками подразделений, специально-технические мероприятия. Такие оперативно-разыскные мероприятия связаны с использованием технических средств и включают в себя прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации.

На сегодняшний день многие сотрудники сталкиваются с проблемой своевременного получения информации. Основными проблемами в этой сфере остаются:

1. Несвоевременность получения информации о соединениях между абонентами и (или) абонентскими устройствами, особенно в случаях, когда информация необходима от оператора связи, не имеющего представительств в регионе местонахождения инициатора запроса.

2. Длительность получения информации от интернет-провайдеров, а также от владельцев и администраторов различных интернет-ресурсов.

3. Сложность идентификации и обнаружения фактических собственников, а также администраторов и пользователей некоторых интернет-ресурсов.

На наш взгляд, решением этой проблемы будет внесение изменений в нормативно-правовые акты, регламентирующие порядок взаимодействия ОВД с операторами связи и интернет-провайдерами. Сегодня существует около более 30 таких нормативных правовых актов. Самым значимым в этой области нормативным актом был Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», установившие расширение полномочий правоохранительных органов, новые требования к операторам почтовой связи.

На сегодняшний день отсутствуют механизмы получения оперативно значимой информации от банковских организаций, интернет-провайдеров, операторов связи, социальных сетей и мессенджеров [3, с. 86]. Существует множество лицензиатов на оказание услуг связи, значительное количество оперативно-разыскных мероприятий, связанных с получением информации, передаваемой посредством сетей электросвязи, предполагает детальное регламентирование взаимодействия операторов связи с уполномоченными органами, осуществляющими оперативно-разыскную деятельность, органы федеральной службы безопасности осуществляют взаимодействие с операторами связи при проведении оперативно-разыскных мероприятий, связанных с использованием технических средств.

Подводя итог, следует заметить, что действенными инструментами борьбы с преступлениями, совершаемыми с использованием компьютерных технологий, остается:

1. Тактически грамотная организация и проведение оперативно-разыскных мероприятий.
2. Оперативно-разыскная методика выявления и раскрытия киберпреступлений, включающая комплекс негласных сил, средств и оперативно-разыскных мероприятий.

Также необходимо отметить важность методического обеспечения IT-подразделений при проведении различных мероприятий. Необходимо повышать профессионализм сотрудников в сфере компьютерной информации, т.к. большое количество преступлений переходит в режим дистанционных.

Библиографический список

1. Кузьмин И.А. Отдельные вопросы информационного обеспечения оперативно-розыскной деятельности при выявлении и раскрытии преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2017. № 4 (4).
2. Озеров К.И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2021. № 1(89). С. 167–171.
3. Иванов П.И. Оперативно-розыскное противодействие киберпреступлениям (проблемы и пути их решения) // Труды Академии управления МВД России. 2022. № 4(64). С. 83–96.

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ КИБЕРТЕРРОРИЗМА

Савотченко С.Е.,

доктор физико-математических наук, доцент;

Желанов А.А.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: век информационных технологий не только облегчил жизнь и профессиональную деятельность людей посредством внедрения в повседневную жизнь достижений компьютерных технологий, но и подготовил мощный плацдарм для кибертеррористов. Главной задачей всех государств стала выработка механизмов, способных противостоять нависшей угрозе, однако для этого необходимо изучить те средства, которые преступники используют для подготовки и реализации кибератак. В данной статье авторы реализуют попытку

анализа некоторых информационных технологий, которые могут быть использованы для реализации актов кибертерроризма.

Ключевые слова: информационная безопасность, глобальные угрозы, кибертерроризм, кибератаки, виртуальное пространство.

MODERN CYBERTERRORISM TECHNOLOGIES

Savotchenko S.E.,

Doctor of Physical and Mathematical Sciences, Associate Professor;

Zhelanov A.A.

(Putilin Belgorod Law Institute of Ministry of the Internal of Russia)

Abstract: the age of information technology has brought not only significant relief to people's lives through the introduction of computer technology into everyday life, but also prepared a powerful springboard for cyberterrorists. The main task of all states has become the development of mechanisms capable of countering the impending threat, but for this it is necessary to study the means that criminals use to prepare and implement cyber attacks. In this article, the authors attempt to analyze some information technologies that can be used to implement acts of cyberterrorism.

Keywords: information security, global threats, cyber terrorism, cyber attacks, virtual space.

Одной из глобальных проблем, с которой человечество шагнуло в XXI век, является терроризм. Во всех своих проявлениях он с каждым днем все больше угрожает безопасности каждого гражданина, государства и всего мира в целом, а также влечет за собой значительные политические, экономические и моральные потери, унося за собой тысячи жизней невинных людей.

Общественные отношения развиваются достаточно интенсивными темпами. Не обошел прогресс стороной и преступный мир. Террористы реализуют свои преступные намерения все более и более изощренными способами, применяя новейшие методы и средства, еще не выявленные правоохрнительными органами, что значительно усложняет задачу противодействия террористической деятельности.

Безусловно, данная проблема нуждается в особом внимании. С этой целью правоохрнительные органы наделены полномочиями от лица государства по борьбе с терроризмом. Одним из важнейших направлений деятельности современной полиции является как раз противодействие терроризму, что и обуславливает актуальность выбранной темы.

XXI век по праву был назван веком информационных технологий. Автоматизация множества привычных процессов значительно упрощает тысячам людей жизнь, экономя время и силы. При этом информационные технологии активно внедряются в преступную деятельность террористов, открывая для них новые возможности, а также позволяя оставаться анонимными.

Активное использование новейших информационных технологий дало виток образованию нового опаснейшего явления – кибертерроризма.

Кибертерроризм – это преступные деяния, направленные на совершение активных действий против жизни и здоровья людей, выведения из строя объектов инфраструктуры, интернет-ресурсов, создания общественного страха и напряжения, дезинформирование населения [1, с. 111].

Современный кибертерроризм не имеет четких территориальных границ, равно как Интернет, распространившийся по всему миру. Кроме того, использование Интернета делает практически невозможным отслеживание источника кибератаки, а также позволяет преступникам уничтожать собственные цифровые следы, оставляемые в виртуальном пространстве.

Ярким примером кибертерроризма являются кибератаки хакерской группировки Anonymous на государственные сайты Российской Федерации 26 февраля 2022 года. Целями кибератаки были выбран Российский сайт «ГосУслуги», сайты Кремля, Государственной думы, Первого канала, правительства России и Роскосмоса, на которые за один день были совершены около 50 Ddos-атак, мощностью не менее 1 Тбайт (1 Тбайт – 1 024 гигабайт). В результате кибератаки сайты перестали временно функционировать на одни сутки. К тяжким последствиям эти кибератаки не привели, однако, проанализировав данную информацию, можно предположить, как могут навредить кибератаки базам данных и системам управления министерства обороны и ядерной энергетики [1, с. 112].

В настоящее время отсутствует официальная классификация видов кибертерроризма. Однако условно его подразделяют на простой, расширенный и комплексный.

Так, простой кибертерроризм предполагает использование программ, уже ранее созданных другим лицом в целях реализации преступного умысла. Атаки простого, или неструктурированного, вида являются наиболее легкими в противодействии, вред от них минимален. Например, использование различного рода мессенджеров с применением технологии VPN позволяет преступникам «замести» цифровые следы, но подготовить масштабную атаку с применением указанных средств вряд ли возможно.

Атаки расширенного типа носят структурированный характер, они более сложны, чем атаки первого вида. Вместе с тем реализация таких атак предполагает создание собственных инструментов для взлома, поэтому вред от структурированных атак намного больше. В качестве примера созданного инструмента для взлома можно привести компьютерный вирус – «червь».

Комплексные атаки представляют собой наиболее сложный вид кибертерроризма, поскольку с их помощью преступники способны вызвать массовое нарушение системы безопасности государства. Атаки комплексного типа производятся «специализированными» преступными организациями, обладающими сложной иерархической структурой. Для комплексных атак используется целая совокупность различных средств: программы, позволяющие оставаться анонимным в виртуальном пространстве, различные компьютерные вирусы, сайты и др. Безусловно, массовость и разнородность используемых средств способна нанести непоправимый ущерб обществу и государству.

Особенностью кибертерроризма является его мобильность. Преступная деятельность ведется на сайтах, которые невозможно отследить и уничтожить, поскольку постоянно появляются новые сайты под новыми адресами, а старые бесследно исчезают. Киберпространство позволяет террористам диктовать свои правила, навязывать идеологию и ценности, рекламировать свой антиобщественный образ жизни.

Пропаганда террористических идей ведется посредством постоянного выпуска видеоматериалов, публикации фотографий, оправдывающих терроризм и призывающих присоединиться. Наиболее беззащитными к такой вербовке являются несовершеннолетние, не обладающие способностями «фильтрации» сведений, публикуемых в Интернете.

Кибертеррористы активно используют собственные «обучающие сайты». Целью такого продукта является вербовка и обучение кандидатов. Они содержат подробные информации по изготовлению взрывчатых веществ и оружия из подручных средств и способах проникновения на сайты государственных структур, взломах почтовых адресов и т.д. Большое внимание уделяется психологической подготовке новобранцев. Сайты имеют детальные сведения о способах проезда в лагеря террористов. Таким образом, сайты террористов выполняют функции дистанционных учебных баз по военно-диверсионной подготовке террористов.

Также информационно-телекоммуникационные технологии используются кибертеррористами в целях сбора денежных средств. В частности, специалисты указывают на сайт Иранской республиканской армии, в котором имеется специальный раздел, где собираются пожертвования. По сведениям заместителя Секретаря Совета Безопасности Российской Федерации В.П. Назарова, самой богатой террористической организацией являлось «Исламское государство», в распоряжении которой был бюджет в 2,3 миллиардов долларов [2, с. 33].

Можно констатировать, что использование кибертеррористами возможностей современных информационных технологий позволяет подготавливать кибератаки нового масштаба. В своей деятельности преступники используют не только уже существующие технологии, но и создают свои собственные на базе ранее известных [3, с. 70].

Так, наиболее распространенной формой вывода из строя информационной инфраструктуры является разработка и использование компьютерных вирусов. Кража паролей осуществляется посредством активного внедрения вирусов-троянов. Противодействие таким атакам видится в создании системы фильтрации, обнаружении и блокировании вредоносного элемента, а также иных подозрительных активностей благодаря мониторингу всего входящего, а также исходящего интернет-трафика.

В зависимости от используемых средств кибертерроризм подразделяется на простой, структурированный и комплексный. Простые кибератаки предполагают использование уже ранее созданных программ, структурированные атаки производятся на основе собственных продуктов (компьютерные вирусы), комплексные атаки сочетают в себе применение средств как первого, так и второго типа, поэтому представляются наиболее опасным.

Борьба с кибератаками сводится к построению мощной защиты информационных систем, что позволит свести к минимуму возможность их захвата злоумышленниками.

Библиографический список

1. Овчаренко К.А., Антонец Н.Д. Кибертерроризм как угроза безопасности информационно-телекоммуникационной сети интернет / Хроники цифровых трансформаций: материалы межкафедрального круглого стола, Москва, 19–26 мая 2022 года. Выпуск 4. – Волгоград: Сириус, 2022. С. 111–114.
2. Ташпекова А.Т., Ташпек Г.А. Информационные технологии и кибертерроризм / Экономическая трансформация и инновационные технологии: сборник материалов I Международной научно-практической конференции, Москва, 22 марта 2018 года. – Москва: НАУКА ПЛЮС, 2018. С. 33–37.
3. Шивдяков Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма // Защита информации. Инсайд. 2009. № 2 (26). С. 64–72.

МЕСТО И РОЛЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ

Савотченко С.Е.,

доктор физико-математических наук, доцент;

Смирнов П.А.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассмотрены некоторые проблемные вопросы противодействия незаконному обороту наркотических средств с использованием информационно-телекоммуникационной сети Интернет на современном уровне. Внедрение информационно-телекоммуникационных систем послужило средой для развития удаленного (бесконтактного) сбыта наркотических средств. Определены пути решения обозначенных проблем, которые, по мнению многих экспертов, будут эффективно способствовать противодействию наркопреступности.

Ключевые слова: незаконный оборот наркотических средств, программное обеспечение, информационно-телекоммуникационная среда, сеть Интернет, наркопреступность.

THE PLACE AND ROLE OF SOFTWARE IN COUNTERING CRIMES IN THE FIELD OF DRUG TRAFFICKING

Savotchenko S.E.,

Doctor of Physical and Mathematical Sciences, Associate Professor;

Smirnov P.A.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article discusses some problematic issues of countering illicit drug trafficking using the Internet information and telecommunications network at the modern level. The introduction of information and telecommunication systems has served as an environment for the development of remote (contactless) sales of narcotic drugs. The ways of solving the identified problems have been identified, which, according to many experts, will effectively contribute to countering drug crime.

Keywords: illicit drug trafficking, software, information and telecommunication environment, Internet, drug crime.

Современные тенденции формирования информационного общества, а также внедрение современных технических средств в повседневную жизнь способствовали развитию научно-технического прогресса человечества, а также широкому продвижению информационно-телекоммуникационных систем. В настоящее время практически невозможно обойтись без информационных технологий. Их участие прослеживается во всех сферах жизни общества, не исключая даже преступную сферу. Правонарушителям намного проще совершать противозаконные действия в удаленном формате за счет того, что аккаунты сложнее отследить, как и найти обоснованные доказательства для привлечения к ответственности.

Так, одним из наиболее часто встречающихся видов преступлений, направленных против жизни и здоровья граждан в информационно-телекоммуникационной среде, является незаконное распространение наркотических средств, так как развитие современных технологий поспособствовало более быстрому и бесконтактному способу продажи и покупки наркотических средств. На протяжении последнего десятилетия произошли многие события, деформирующие сознание человека. Если раньше граждане взаимодействовали только в офлайн-режиме, то сейчас практически все связи стали производиться через электронные носители. Как коронавирусная инфекция, так и специальная военная операция способствовали перемещению фокуса внимания правонарушителей в онлайн-пространство. В настоящее время создается огромное количество анонимных аккаунтов, распространяющих информацию о размещении и способе получения запрещенных наркотических средств. Многие люди молодого возраста поддаются влиянию правонарушителей и становятся теми, кто нарушает закон в сфере незаконного оборота наркотиков.

Кроме того, широко распространяется цифровизация, то есть внедрение цифровых технологий. С помощью криптотехнологий данное преобразование «лишает правоохранителя физического и юридического контроля за нелегальным наркооборотом и финансовыми операциями, проводимыми с ними» [1, с. 93].

Так, на январь – декабрь 2022 года зарегистрировано 177 741 преступлений в рассматриваемой нами области. Это 9,04% преступлений от общего количества зарегистрированных. Конкретно в Белгородской области процент составляет 8,73%. Показатели довольно значительные, учитывая то, что они стабильно сохраняются на протяжении многих лет. При этом важно учитывать, что именно данный тип преступлений является одним из актуальнейших среди преступников, осуществляющих незаконную деятельность в информационной среде [2].

Именно поэтому перед правоохранителями встает вопрос организации борьбы с рассматриваемым нами видом преступности. Одним из вариантов является использование современного технического оборудования программного обеспечения органами внутренних дел. Так, в 2011 году был образован Департамент по материально-техническому и медицинскому обеспечению МВД России и утверждено Положение о Департаменте по материально-техническому и медицинскому обеспечению МВД России¹.

Основная задача данного подразделения заключается в том, чтобы централизованно поставлять правоохранителям материально-технические средства для организации деятельности МВД России. Информационным обеспечением правоохранительных органов в соответствии с Распоряжением Правительства от 19.08.2011 1474-р занимается ФКУ ГИАЦ МВД России².

В данной статье мы рассмотрим роль и место программного обеспечения в борьбе с незаконным оборотом наркотиков. Программное обеспечение представляет собой комплекс средств программного и документального характера, предназначенных для «создания и эксплуатации систем обработки данных [3]. Это компьютерные программы и их файлы, способствующие нормальному функционированию компьютера. Так, ставится вопрос о разработке рекомендаций по организации программного обеспечения и наделении системностью действий правоохранительных органов.

Несмотря на трудности идентификации личности преступника в информационной среде, МВД России разработало определенный комплекс действий с использованием программного обеспечения. Даже такой мессенджер, как Telegram не может обеспечить полную анонимность правонарушителям. Так, например, при регистрации аккаунта указывается номер телефона, что может способствовать обнаружению места нахождения правонарушителя. Кроме того,

¹ Положение о Департаменте по материально-техническому и медицинскому обеспечению МВД России: Приказ МВД России от 24.06.2011 № 722 (ред. от 28.03.2022) // СПС «КонсультантПлюс».

² О создании федерального казенного учреждения путем изменения типа существующего федерального государственного бюджетного учреждения с сохранением его основных целей деятельности и предельной штатной численности: Распоряжение Правительства Российской Федерации от 19.08.2011 № 1474-Р (ред. от 13.12.2019) // СПС «КонсультантПлюс».

Telegram запрашивает информацию при регистрации, к которой должен получить доступ. К такой информации относятся номера телефонов, звонки, сообщения и фотографии. Все это исключает полную анонимность пользователя [5, с. 70].

Таким образом, для борьбы с незаконным оборотом наркотиков через сеть Интернет правоохранительным органам необходимо научиться активно использовать программное обеспечение в своей деятельности, а также разработать конкретный алгоритм действий при документировании фактов незаконного оборота наркотиков.

Возникает необходимость проведения анализа используемого программного обеспечения для противодействия противоправным действиям, его актуальности, уровня защиты, а также его места и роли в обеспечении борьбы правоохранительных органов с ростом числа преступлений в сфере незаконного оборота наркотиков.

В свою очередь, это обуславливает необходимость актуализации применения программного обеспечения и информационных технологий для формирования информационно-технологической компетентности сотрудников ОВД.

Библиографический список

1. Хамидуллин Р.С. Обеспечение национальной безопасности путем противодействия преступлениям, связанным с незаконным оборотом наркотических средств и психотропных веществ, совершаемым с использованием информационно-телекоммуникационных технологий // Вестник Уральского юридического института МВД России. 2022. № 1. С. 93–97.
2. Портал правовой статистики // Официальный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс]. – URL: http://crimestat.ru/offenses_chart (дата обращения: 10.02.2023).
3. Программное обеспечение компьютера // Информатика [Электронный ресурс]. – URL: http://psk68.ru/files/metod/uchebnik_Informatika/po.html (дата обращения: 10.02.2023).
4. О создании федерального казенного учреждения путем изменения типа существующего федерального государственного бюджетного учреждения с сохранением его основных целей деятельности и предельной штатной численности: Распоряжение Правительства Российской Федерации № 1474-Р от 19.08.2011 (ред. от 13.12.2019) // СПС «КонсультантПлюс».
5. Петухов А.Ю., Куликов К.С. Проблемы противодействия использованию компьютерных технологий в незаконном обороте наркотиков // Вестник Краснодарского университета МВД России. 2020. № 1 (47). С. 68–71.

КРИМИНАЛЬНЫЙ ПОТЕНЦИАЛ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Страхов А.А.

(Московский университет МВД России имени В.Я. Кикотя);

Прокопенко А.Н.,

кандидат технических наук, доцент

(Академия Государственной противопожарной службы МЧС России)

Аннотация: в статье рассматриваются вопросы использования систем искусственного интеллекта в преступных целях. Авторы анализируют применение программного обеспечения криминальным сообществом для совершения преступлений. Рассматриваются такие направления, как подделка аудио и видео с использованием дипфейка, использование систем искусственного интеллекта и чат-ботов в методах социальной инженерии, в том числе для сбора и анализа информации о потерпевших. Также анализируется использование в преступных целях робототехнических устройств, преимущественно беспилотников, в том числе для совершения терактов.

Ключевые слова: искусственный интеллект, киберпреступления, нейросети.

CRIMINAL POTENTIAL OF ARTIFICIAL INTELLIGENCE

Strakhov A.A.,

(Kikot Moscow University of the Ministry of the Interior of Russia);

Prokopenko A.N.,

Candidate of Technical Sciences, Associate Professor

(Academy of the State Fire Service of the EMERCOM of Russia)

Abstract: the article examines the use of artificial intelligence systems for criminal purposes. The authors analyze the application of software by the criminal community to commit crimes. Areas are considered such as faking audio and video using deepfake, the use of artificial intelligence systems and chatbots in social engineering methods, including for collecting and analyzing information about victims. It also analyzes the use for criminal purposes of robotic devices, mainly drones, including for committing terrorist attacks.

Keywords: artificial intelligence, cybercrimes, neural networks.

Развитие в последние десятилетие систем искусственного интеллекта сопровождается неоднократными попытками преступных элементов использовать эти информационные технологии для криминальной деятельности. Совершение незаконных деяний посредством использования различного программного обеспечения не является новостью и используется десятилетиями. Однако си-

стемы искусственного интеллекта предоставляют для криминальной среды новые, ранее недостижимые возможности.

Например, в последние годы появился новый жанр порнографии – deepnudes, который набирает все большую популярность в цифровом пространстве. Началось все в декабре 2017 года на бесплатном видеохостинге Sendvid, где был размещен видеоролик с популярной израильской актрисой и моделью Галь Гадот. В незатейливом сюжете голливудская звезда, тренер по боевой подготовке армии обороны Израиля и многодетная мать занимается сексом со своим сводным братом. Позднее на форуме Reddit были выложены порноролики с участием Скарлетт Йохансон, Мэйси Уильямс, Тейлор Свифт и Обри Плаза. Список знаменитостей якобы снявшихся в видео, рос, атмосфера в обществе накалялась.

Журналистское расследование выявило, что подделки созданы не голливудской студией спецэффектов, а одним из редакторов Reddit с никнеймом deepfakes, который впоследствии стал нарицательным. По словам deepfakes, видеоролики создавались на основе изображений в Google, стоковых фотографий и видео с YouTube с помощью инструментов машинного обучения с открытым исходным кодом, которые находятся в свободном доступе.

Как это работает? Например, приложение FakeApp использует технологии искусственного интеллекта для подмены лиц в три этапа: накопление, обучение и слияние. С помощью нейросети FakeApp анализирует тысячи кадров с поддельным персонажем, взятых из фото- и видеоисточников, определяет, как будет выглядеть выражение лица при разном освещении, типичную мимику и т.п. Как только программа наберет нужный объем знаний, она накладывает поддельное лицо на подлинное.

Указанная технология незамедлительно начала использоваться в преступных целях, причем благодаря возможностям технологии глубоких подделок преступления становятся более изощренными. Среди них можно выделить следующие направления:

- 1) шантаж и вымогательство за счет угрозы опубликования поддельного компромата;
- 2) обман систем идентификации и контроля доступа по биометрическим параметрам;
- 3) платежи на подставные банковские счета и другие несанкционированные действия сотрудников по телефонному распоряжению голосом руководителя;
- 4) подделка новостей и манипулирование обществом и т.п.

В 2019 году The Wall Street Journal опубликовал сюжет, в котором генеральный директор неназванной энергетической фирмы из Великобритании получил по телефону указание босса, исполнительного директора немецкой материнской компании, и перевел 220 000 евро на банковский счет указанного поставщика. Генеральный директор узнал «тонкий немецкий акцент» и мужскую «мелодичность» голоса босса, а на самом деле по телефону разговаривал совсем другой человек. Мошенник звонил в компанию три раза: первый – чтобы инициировать перевод, во второй раз подтвердил получение денег на поддель-

ный счет, а в третий раз потребовал еще один перевод, после чего был заподозрен, но первый платеж уже ушел безвозвратно.

Для осуществления подделок не требуется внесения существенных изменений, причем таких, которые видны невооруженным глазом. Однако вера людей в информацию, полученную из Интернета, оказывается более сильной, чем их критическое мышление. Так, видео с выступлением «пьяного» американского спикера Палаты представителей Нэнси Пелоси в 2019 г. фактически стало вирусным и набрало более 2 млн просмотров. Причем из-за данного инцидента над Пелоси долгое время издевались республиканцы, а единственная монтажная уловка, обманувшая миллионы американцев, заключалась в воспроизведении обычного видео на замедленной скорости (75%).

Весной 2021 года двое мошенников в Китае были арестованы за совершение налоговых махинаций путем присвоения фальшивых удостоверений личности с использованием технологии дипфейка. По данным китайской полиции дуэт с 2018 года выдавал клиентам поддельные налоговые накладные и сумел заработать на мошенничестве около 80 млн долларов.

В апреле 2021 года двум россиянам удалось использовать дипфейк, чтобы выдать себя за лидера российской оппозиции Алексея Навального. Имитаторам удалось поучаствовать в различных частных беседах, дать интервью популярным латвийским СМИ, организовать видеосвязь с парламентами Великобритании, Латвии, Эстонии и других европейских стран. Позже шутники опровергли обвинения в их связи с Кремлем и утверждали, что это были всего лишь розыгрыши.

Появление на рынке простых в использовании инструментов для создания качественных аудио- видеоподделок привело к тому, что их производство превратилось в прибыльный бизнес, в том числе противозаконный. Качественные дипфейки с участием политиков, государственных деятелей, артистов, спортсменов и иных знаменитостей в Интернете найти несложно, и это указывает на то, что люди не в состоянии отличить фальшивки от реальных изображений в виртуальном мире. Многие западные СМИ не стесняются распространять подобные подделки со ссылкой на «достоверные» источники, по принципу «хайли лайкли» (highly likely – весьма вероятно).

Глубокие фэйки и боты влияния активно используются политиками и пропагандистами как в интересах государств, так и в экстремистских целях. Они способны переключить внимание общества, организовать массовую поддержку или протест, заставить людей поверить любой информации. На поддельных видеороликах изменяют изображения, голоса, текст, чтобы манипулировать восприятием событий или выставить в негативе своих противников. Нанося ущерб репутации публичных политиков и государственных деятелей, можно манипулировать общественным мнением, например на выборах, снижать рейтинговые баллы поддержки социальных проектов и т.п. Многие знают о подобных технологиях, однако, несмотря на многочисленные мемы фотошопа, люди привыкли верить тому, что они видят и слышат.

К основным техникам криминального дипфейка относятся:

1) синтез высокоточных видеоподделок внешности и поведения людей на основе анализа больших данных и машинного обучения;

2) клонирование знакомого жертве голоса для управления ее поведением по телефону;

3) подстройка мимики и движения губ подлинных персонажей на видеоизображениях под конкретный речевой контент.

Согласно многочисленным прогнозам специалистов в настоящее время дипфейковые технологии способны коренным образом изменить ландшафт киберугроз.

Возможности социальной инженерии не имеют границ, т.к. в любой киберсистеме самым уязвимым звеном является человек. Чтобы это понять, достаточно взглянуть на биографии наиболее известных мошенников, применявших в своей деятельности методы социальной инженерии:

Кевин Митник, про которого на суде сказали, что он способен «начать ядерную войну, свистнув в телефон-автомат», никогда не использовал хакерские программы для взлома компьютеров, все пароли и коды доступа добывались методами социальной инженерии;

«Желтый кидала» Джозеф Уэйл с помощью социальной инженерии на фиктивном банке заработал 400 тыс. долларов;

Фрэнк Абигнейл Младший за 5 лет заработал 2,5 млн долларов на фальшивых чеках, обналичив их в 26 странах;

Виктор Люстиг несколько раз сумел продать Эйфелеву башню и т.п.

Причем вышеперечисленные мошенники были пойманы и судимы, а среди непоиманных наверняка есть те, кто «заработал» больше денег. Использование систем искусственного интеллекта позволяет значительно повысить эффективность методов социальной инженерии и усилить «убедительность» техник обмана.

Технологии умного анализа больших данных позволяют узнать о жертве практически все. Все большую популярность в преступной среде набирают инструменты и комплексные сервисы OSINT (Open Source INTelligence), которые упорядочивают и автоматизируют сбор данных об интересующих объектах на пространстве Интернет. Сами по себе разрозненные данные о той или иной потенциальной жертве большого практического значения не имеют, ценность представляет их обобщение и корреляция с другими данными, для чего используется специализированное ПО. Например, технологии Data Science, используя алгоритмы машинного обучения, могут построить модель жертвы, предложить оптимальную стратегию манипулирования и контролировать ее поведение на протяжении всего сценария фишинговой атаки.

Современные социальные сети, мессенджеры, сайты услуг и электронной коммерции активно используют чат-боты (Chat-Bot) – это специализированное ПО интеллектуальной поддержки пользователей с помощью текстовых или голосовых диалогов. В круг функций чат-ботов обычно входит встреча пользователя на первой линии, уяснение поставленной задачи и ее решение в автоматическом или интерактивном режиме. Нередко в процессе диалога чат-бот может

предложить пользователю ответить на некоторые вопросы, скачать дополнительные материалы или выполнить иные действия в программе. Вообще по данным американской компании Barracuda Networks, занимающейся кибербезопасностью, в первом полугодии 2021 года 64% интернет-трафика сгенерировали боты.

В 2020 году компания MalwareHunterTeam обнаружила фишинговую аферу с использованием чат-бота службы поддержки клиентов. В письме от имени компании United Center Money Transfer российским клиентам предлагалась компенсация за неиспользованные услуги Интернета и сотовой связи в размере 2 100 долларов США. Для получения компенсации требовалось перейти по ссылке и зарегистрироваться на международном портале компании: ввести имя, адрес, последние четыре цифры номера паспорта и реквизиты платежной. После ввода указанных данных чат-бот сообщает жертве, что запись о пользователе с такими реквизитами отсутствует в системе, и нужно пройти регистрацию повторно. Независимо от того, совпали повторно введенные реквизиты или нет, чат-бот подтверждает, что запись найдена и предлагает жертве перейти на другой сайт, где уже нужно ввести имя, номер телефона и данные банковской карты для получения компенсации.

В конце аферы злоумышленники имеют: имя жертвы, адрес электронной почты, реквизиты банковской карты с привязанным номером телефона и последние четыре цифры номера паспорта. В ряде случаев этого достаточно для получения несанкционированного доступа к учетным записям жертвы и нанесения ущерба.

Некоторые фишинговые боты обходятся без сложных мошеннических схем, а просто рассылают потенциальным жертвам почтовые сообщения с вредоносный кодом, а затем после его активации эксплуатируют полезную нагрузку (payload), такую, как кража данных, блокировка компьютеров или участие в DDoS-атаках.

Использование ботов в мессенджерах – один из наиболее эффективных каналов коммуникации с потенциальными клиентами. Имитируя живое общение, чат-боты задают пользователю наводящие вопросы, уточняют профильную информацию и формулируют персонально ориентированные предложения. Люди настолько доверяют машинам, что практически не задумываются о возможном мошенничестве. Вместе с тем для несанкционированного использования персональных чат-ботов в социальных сетях или мессенджерах мгновенных сообщений достаточно захватить аккаунт, на который был заведен токен-ключ управления чат-ботом.

Весной 2022 года с началом СВО в компанию «Искусство автоматизации», специализирующуюся на разработке чат-ботов, стали поступать нетипичные запросы от их владельцев. Свыше 30 клиентов пожаловались на спам, который роботы рассылали без их ведома, а некоторые даже попросили удалить слишком «умные» программы, вышедшие из-под контроля. Расследование инцидента выявило, что владельцы инструментальных платформ для создания чат-ботов решили без ведома клиентов по их базе сделать рассылку материалов в рамках информационной войны против нашей страны. Другими словами, лю-

ди доверили сервису свою базу данных, а владельцы сервиса стали использовать ее в противоправных и антигосударственных интересах. При этом следует учесть, что простого метода для удаления сообщения, отправленного чат-ботом, например в мессенджере Телеграмм, не существует.

Американский бизнесмен Илон Маск при покупке Twitter в апреле 2022 года своими оценками и сообщениями вызвал панику среди пользователей соцсетей. Например, Маск заявил, что до 90% аккаунтов Twitter принадлежит «армии ботов» и сделка не состоится, пока поддельные пользователи не будут вычищены. Его заявление косвенно подтверждается тем фактом, что еще в 2017 году английские ученые из Колледжа лондонского университета во время анализа сети Twitter случайно обнаружили «спящий» сегмент из 350 000 ботов. Ученые заметили, что из мест, где люди обычно не живут (моря, пустыни, зона Арктики), изредка отправлялись твиты – цитаты из «Звездных войн». Создатели и цель создания данной структуры до сих пор не известна.

Еще одним нарастающим трендом использования искусственного интеллекта в криминальных целях является робототехника, в частности беспилотные летательные аппараты.

В 2022 году израильская компания Elbit Systems выпустила скоростной маневренный интеллектуальный квадрокоптер (дрон) Lanius с функциями ведения разведки, картографирования местности, классификации и уничтожения целей. Lanius оснащен многочисленными датчиками и камерами, а также встроенным модулем Nvidia Jetson AI system для предварительной интерпретации видеоданных. В зону работы он доставляется по земле или на материнском носителе. Вместе с полезной нагрузкой весит чуть больше килограмма и может действовать как индивидуально, так и в составе боевого роя из нескольких дронов под управлением ПО Legion-X – «автономного сетевого боевого решения» компании Elbit Systems.

Lanius способен самостоятельно идентифицировать интересующие объекты, помечать их на карте, находить двери и окна, проникать в здания и обыскивать их без непосредственного контроля оператора. При обнаружении людей умный дрон может классифицировать их как дружественных или враждебных, комбатантов или некомбатантов, вооруженных или невооруженных. В случае возникновения угрозы безопасности может поразить цель, используя имеющееся на борту вооружение, в том числе в стиле камикадзе. Еще одна тактическая функция дрона – работа из засады. Lanius может тихо приземлиться в заданном месте и наблюдать, например, за закрытой дверью. Если дверь откроется и появившийся объект идентифицируется как цель, то срабатывает механизм ее уничтожения. По заявлению разработчиков окончательную команду на летальное применение оружия дает оператор, но в отдельных случаях решение может приниматься программным обеспечением самого устройства.

Ударные дроны-камикадзе с искусственным интеллектом иногда называют барражирующими боеприпасами. Способ их применения довольно прост. Сначала вооруженный БПЛА запускается в зону действия, а затем он самостоятельно ищет цель. Зачастую барражирующий боеприпас работает в паре с дро-

ном-разведчиком, который с большой высоты осуществляет осмотр местности, поиск целей и наведение барражирующих боеприпасов по координатам.

Согласно общей концепции умные беспилотники конструируются как комплексы, состоящие из нескольких БПЛА и наземной станции управления. По аналогии с интернетом вещей летают только датчики и исполнительные механизмы – «глаза», «уши» и полезная нагрузка, а основные «цифровые мозги» и люди-пилоты размещаются на земле. По сравнению с полезной нагрузкой «искусственный разум» весит много, требует места и энергии. Если умная программа ведет себя неадекватно, управление БПЛА можно переключить на ручной режим. Но, если БПЛА теряет канал связи с землей, то его поведение определяется внутренним ПО, интеллектуальные возможности которого весьма ограничены.

Примеров использования дрогов-камикадзе в полностью автономном режиме, когда он самостоятельно принимает решение о применении, достаточно. Например, в марте 2023 года эксперты ООН сделали доклад о недопустимых фактах применения автономных дронов-камикадзе в Ливии, где турецкие БПЛА Kargu 2 после потери связи с оператором занимались свободной охотой, самостоятельно выслеживали и уничтожали цели по собственному усмотрению. В ответ на возмущение общественности сотрудник Национального консорциума по изучению терроризма и ответных мер на терроризм при Университете Мэриленда в Колледж-Парке Закари Калленборн дал типичный человеконенавистнический американский ответ: «Автономное оружие как концепция не так уж и нова. Наземные мины, по сути, тоже являются простым автономным оружием. Вы наступаете на них, и они взрываются». Его коллега Калленборн из отдела нетрадиционных вооружений и технологий добавил: «Уверяю вас, умные беспилотники являются более гуманным оружием, чем другие виды».

Другой проблемой использования боевых роботов является обучение искусственного интеллекта, управляющего ими. Изначально машина с нейросетью и базовыми наборами данных не знает, чем солдат врага отличается от своего солдата или от муляжа в камуфляже, а здравого смысла у нее нет. При этом во время обучения умных машин давно забыт первый закон робототехники, сформулированный американским ученым и писателем-фантастом российского происхождения Айзеком Азимовым: «Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинен вред». Соответственно, недостаточно качественно обученные роботы будут атаковать все подряд и могут нанести существенный вред не только противнику, но и своим владельцам.

Активно начали использовать современные достижения робототехники в целом и беспилотные аппараты в частности террористические организации. Это обусловлено тем, что использование ударных дронов позволяет совершать теракты, оставаясь в стороне от эпицентра взрыва, что повышает риск совершения терактов в охраняемых зонах. Например, в августе 2018 года злоумышленники с помощью дронов с взрывчаткой совершили покушение на президента Венесуэлы Николаса Мадуро во время торжественного выступления в Каракасе. Один беспилотник был сбит снайпером, несколько взорвались на площади, вызвав ранения и панику. Президента телохранители закрыли пуленепробиваемыми щитами.

Кроме заказных убийств, умные беспилотники используются в преступных целях для слежки за людьми, доставки контрабанды и наркотиков и т.п. Так, пограничниками США регулярно пресекаются попытки переправки наркотиков и другой контрабанды из Мексики с помощью мини-дронов. В 2015 году беспилотник, пролетая на высокой скорости над исправительным учреждением в Мэнсфилде штат Огайо, сбросил во двор тюрьмы груз с наркотиками, что вызвало драку среди заключенных.

Использование беспилотников для доставки наркотиков и мобильных телефонов в российские тюрьмы является одной из основных проблем в деятельности ФСИН России. Например, в 2022 году четверо мужчин пытались при помощи квадрокоптера передать мобильные телефоны и наркотики в исправительную колонию под Иркутском.

Кроме вышеперечисленного, хакеры используют дроны входа в зону сетей Wi-Fi или Bluetooth с малым радиусом действия, в том числе при кибератаках на умные дома и другие объекты интернета вещей. Причем сфера применения умных дронов преступным сообществом постоянно расширяется, чему во многом способствует появление на рынке относительно дешевых моделей. В настоящий момент основной режим управления дронами пока ручной, но смена оператора-человека на киберсистему с искусственным интеллектом – дело ближайшего будущего.

Резюмируя вышесказанное, можно провести классификацию использования систем искусственного интеллекта в преступных целях:

- 1) подделки аудио и видео с использованием дипфейка;
- 2) использование систем искусственного интеллекта и чат-ботов в методах социальной инженерии, в том числе для сбора и анализа информации о потерпевших;
- 3) использование в преступных целях робототехнических устройств, преимущественно беспилотников, в том числе для совершения терактов.

В заключение следует подчеркнуть, что цифровой искусственный интеллект – это не друг и не враг, а набор программ. Это инструмент, который способен решать задачи без участия человека, набирать собственный опыт и самосовершенствоваться. Но ни один искусственный интеллект никогда не будет думать как человек. В искусственном интеллекте нет эмоций, нет преступных пороков, он не создает коварные алгоритмы, чтобы навредить тому или иному человеку. Просто умные машины обучаются решать поставленные задачи хорошо, но сами по себе технологии не являются злом. Поэтому люди должны контролировать использование искусственного интеллекта и не допускать его применения в преступных целях.

Библиографический список

1. К чему привело повальное увлечение порно с голливудскими звездами [Электронный ресурс]. – URL: <https://lenta.ru/articles/2018/02/09/deepfake/>
2. AI-Assisted Fake Porn Is Here and We're All Fucked [Electronic resource]. – URL: <https://www.vice.com/en/article/gydydm/gal-gadot-fake-ai-porn>

3. A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000 [Electronic resource]. – URL: <https://www.forbes.com/>
4. Deepfake crime life in new virtual reality [Electronic resource]. – URL: <https://deepfakechallenge.com/2021/10/27/10469/>
5. Беспилотники самостоятельно охотятся на людей [Электронный ресурс]. – URL: <https://www.9111.ru/questions/>
6. Дроны-«преступники». Как люди используют гаджеты в незаконной деятельности [Электронный ресурс]. – URL: <https://www.mn.ru/smart/>
7. Сложная фишинговая афера использует чат-бота поддержки для «помощи» жертвам [Электронный ресурс]. – URL: <https://www.bleepingcomputer.com/news/>
8. Нечеловеческая опасность. Как боты захватили социальные сети и можно ли их победить [Электронный ресурс]. – URL: <https://secretmag.ru/>

ЭЛЕМЕНТЫ ФОРЕНЗИКИ – СОСТАВЛЯЮЩАЯ ЦИФРОВОЙ ГРАМОТНОСТИ СОТРУДНИКА ОВД

Федосеев А.Э.,
Назаренко И.С.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматривается актуальность обладания специальными знаниями сотрудниками правоохранительных органов в условиях роста киберпреступности. Описывается важность применения сотрудниками некриминалистических подразделений элементов форензики. Указывается на значимость цифровой грамотности в качестве элемента профессиональной подготовки.

Ключевые слова: киберпреступность, форензика, компьютерная криминалистика, цифровая грамотность.

FORMALIZATION OF THE APPROACH TO THE METHODOLOGY OF DIGITAL TRACES IDENTIFICATION AND FIXATION

Fedoseev A.E.,
Nazarenko I.S.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article discusses the relevance of having special knowledge by law enforcement officers in the context of the growth of cybercrime. The importance of the use forensic elements by employees of non-criminalistic units is described. The significance of digital literacy as an element of professional training is pointed out.

Keywords: cybercrime, forensics, computer forensics, digital literacy.

Компьютеризация, охватившая все стороны человеческой жизни, цифровая трансформация [1] как государственное направление в развитии общественных отношений – все это подтверждает повышение роли информационных технологий в жизни как каждого человека в отдельности, так и общества в целом. Положительные аспекты, вносимые технологиями, лежат в основе причин их повсеместного применения, а также неостанавливающегося развития. Но, к сожалению, достижения используются не только в созидательных целях. Инновации различных областей человеческой деятельности применяются против человека, против направлений его деятельности, против государственного устройства. Обратная сторона прогресса – высокотехнологичная преступность. Деятельность правоохранительных органов нацелена на противодействие противоправным проявлениям. В том числе новым проявлениям, новым способам реализации, новым вариантам использования технологий.

В рамках расширенной коллегии Министерства внутренних дел Российской Федерации по итогам 2022 года В.В. Путин отметил наличие соответствующих знаний у граждан в качестве одного из способов противодействия высокотехнологичной преступности: «...важно постоянно информировать граждан о новых разновидностях подобных преступлений, учить, как обезопасить себя от этих преступлений, в целом повышать цифровую грамотность людей...» [2].

Рост количества преступных проявлений в специфической форме способствует совершенствованию ответных мер. Правоохранительные органы в своей деятельности применяют обновленные тактические элементы и методики в противодействии видоизменяющимся преступлениям. Изменения коснулись составных частей расследования и оперативной составляющей, в том числе и криминалистики. Новые технологии пополняют и арсенал противодействия преступности применяемыми в разных отраслях инструментами OSINT и форензики. Сам термин имеет происхождение от forensics сокращенной формы английского сочетания forensic science, интерпретируемого как «судебная экспертиза» или криминалистика. Несмотря на существование самостоятельного термина computer forensics, в своем составе несущего определение «компьютерная», форензика без определения рассматривается как криминалистика, ориентированная именно на компьютерную сферу [3]. Форензика определяется как подраздел криминалистики [4], как прикладная наука, рассматривающая методы поиска, получения, закрепления и исследования цифровых доказательств. Зарубежная часть computer forensics относится непосредственно к криминалистическим исследованиям, связанным с локальными компьютерами: нахождению следов и артефактов в оперативной памяти, внешних сопряженных носителях, элементов журналирования программного обеспечения, реестра. Это один из элементов, присутствующих в классификации [5] направлений исследования. К другим компонентам классификации относят:

- Network forensics, рассматривает расследования в сегменте сетевого трафика информационных систем.
- Forensic data analysis, рассматривает направления анализа данных, получаемых в виде следов (для преступлений, инцидентов).

– Mobile device forensics, рассматривает мобильный сегмент с особенностями данных в системах Android, iOS и им подобных.

– Hardware forensic, рассматривает аппаратную составляющую, наиболее сложную по реализации, например в виде анализа низкоуровневых данных микроконтроллеров, частот Wi-Fi-устройств или аппаратных закладок.

Помимо узких направлений внутри форензики, ее практическая сфера применения охвачена не только криминалистической деятельностью в рамках расследования проявлений компьютерной преступности. Локализация и исследование цифровых следов используются также в гражданских правоотношениях, касающиеся компьютерной информации или электронных доказательств в рамках разбирательств по гражданским делам. Разбирательства по нарушениям в сфере страхования, касающиеся компьютерной информации или информационных систем, тоже связаны с форензикой, как и процесс реагирования на инциденты информационной безопасности в компаниях и организациях. Элементы форензики применяются в рамках реализации информационного противодействия при решении задач даже военной или разведывательной направленности, а также на бытовом уровне организации гражданами защиты своих прав и частных интересов в отношении информации в электронном виде и электронных документов.

Форензика в органах внутренних дел по своей сути имеет непосредственное отношение к деятельности криминалистических подразделений. Одним из видов экспертиз, проводимых ими, являются компьютерно-технические экспертизы. Специалист, исследуя соответствующим образом изъятую технику, устанавливает наличие определенной следовой картины цифровой природы, изучает ее и документирует для возможности использования в качестве доказательной базы в судебном производстве. Вопросы, на которые необходимо ответить специалисту, формулирует следователь. Они носят юридический характер, так как полученная информация должна подтверждать факты нарушения определенных правовых норм и являться значимой в рамках рассматриваемого судом дела. Уголовно-процессуальное законодательство регламентирует эксперту указание в заключении «примененных методик» [6] наряду с результатами исследований. Эта сторона знаний носит уже технический характер. Таким образом, эксперт при реализации своей служебной деятельности должен опираться на разные области знаний.

С другой стороны, возможны ситуации формирования доказательной базы на основе цифровых следов, получаемых оперативным путем. Процесс документирования регламентируется нормативными документами, требующими соблюдения юридических норм, однако фактически сам процесс получения цифровой информации от смены должностного лица не изменился и также требует наличия знаний в области технических наук.

Еще одна норма федерального законодательства выражает обязанность полиции «...обеспечивать сохранность следов преступления, административного правонарушения, происшествия...» [7]. Это общее требование относится к сотрудникам полиции различных подразделений, т.е. к представителям тех служб, которые будут реализовывать указанную функцию. Как правило, на ме-

сто происшествия первым прибывает наряд патрульно-постовой службы или соответствующий участковый уполномоченный. Для реализации мероприятий по сохранению обстановки, следов и других вещественных доказательств на месте происшествия этим сотрудникам необходимо как минимум иметь представление о природе следов, их локализации и о действиях, способных повредить следы или даже уничтожить.

Природа цифрового следа как отличительная характеристика не позволяет однозначно определить его наличие или отсутствие органами человеческих чувств. Необходимо понимание сущности проявления этих специфических следов в виде, неотделимом от носителей, представление о носителях, реализованных в виде самостоятельных устройств, о способах формирования следов и, соответственно, способах их удаления (заметания), искажения и потери. Эти знания помогут в качественном выполнении возложенных на полицию обязанностей и в недопущении к искажению следовой картины по причине некомпетентных действий, основанных на отсутствии знаний.

Глубина знаний о физических процессах не нужна для реализации указанной обязанности. Понимание того, что, наступив на отпечаток обуви на месте происшествия, можно исказить следовую картину или потерять вовсе, должно существовать по аналогии и для цифровых следов. Например, школьная информация о способности магнита намагнитить или размагнитить определенные материалы. Этот же принцип лежит в природе создания накопителей на жестких магнитных дисках (он же НЖМД, HDD, винчестер или жесткий диск). В совокупности эта информация сформирует знания о том, что поднесение магнита к такому носителю способно исказить или уничтожить информацию на нем, а следовательно, и непосредственно цифровой след, что приведет к потере элементов доказательной базы. Или знания о том, что оперативная память является энергозависимой, должны принести понимание того, что обесточивание компьютера на месте происшествия также способно уничтожить находящуюся в ней информацию (следовую картину).

Мы говорим о всепоглощении информатизацией всех сторон жизни и, соответственно, наличии определенных знаний у человека для возможности использования этой информатизации для облегчения производственных процессов и для реализации цифровых благ в частной жизни. Почему же необходимость технической грамотности вменяют только специалисту? Глубокие знания, несомненно его прерогатива, но знаниями отдельных элементов форензики должен обладать значительно больший круг сотрудников, что подтверждают вышеуказанные примеры. Повышение уровня раскрываемости, в том числе высокотехнологичных преступлений, связывается с изменением уровня специальных знаний среди сотрудников [8].

При реализации основных профессиональных образовательных программ высшего образования, например программ бакалавриата по направлению подготовки 40.03.02 «Обеспечение законности и правопорядка», федеральный государственный образовательный стандарт высшего образования предписывает в качестве одной из общепрофессиональных компетенций сформировать у выпускника способности понимать принципы работы современных информаци-

онных технологий и использовать их для решения задач профессиональной деятельности (ОПК-12) [9]. Те самые элементы технических знаний, которые будут содействовать служебной деятельности будущего сотрудника, получающего юридическое образование, учтены в базовом документе, предъявляющем требования к этому образованию. Подобные требования можно встретить в ряде других нормативных документов, касающихся и профессионального обучения сотрудников, впервые принимаемых на службу в органы внутренних дел, и в дополнительных профессиональных программах повышения квалификации. В 2022 году в результате организационно-штатных мероприятий в системе МВД России создан новый главк по работе с личным составом. По словам министра внутренних дел Российской Федерации генерала полиции Российской Федерации В.А. Колокольцева, «среди его функций – повышение качества подготовки сотрудников полиции к профессионально грамотным действиям в условиях любой оперативной обстановки» [2].

Систематическое развитие информационных технологий и их роли во всех областях деятельности человека, рост высокотехнологичной преступности – значимые социальные явления. Повышение роли информационной компетентности в профессиональных знаниях, ведомственный акцент на значимости качества подготовки сотрудников – закономерная реакция в вопросах противодействия новым противоправным проявлениям. Все в совокупности – взаимосвязанные проявления. Ведь новые технологии – это новые знания, использование новых технологий, эффективное их применение и тем более развитие невозможны без обладания знаниями. А раз мы говорим о новых этапах в развитии информационных технологий, то и знания должны быть именно из этой области. Из области информатики – в широком смысле, в узком – в виде навыков оператора прикладных программ или тех самых элементов компьютерной криминалистики.

Знания помогают не только использовать блага технологий, но и развивать их. В условиях тенденций роста количественной и качественной характеристик киберпреступности неоспоримы актуальность использования, а также развития форензики как инструмента противодействия. Однако недостатки в уровне знаний из области информационных технологий не позволяют реализовать в правоохранительной деятельности весь потенциал, в том числе и компьютерной криминалистики. Что в очередной раз подтверждает важность реализации элементов цифровой грамотности при подготовке сотрудников органов внутренних дел.

Библиографический список

1. Распоряжение Правительства Российской Федерации от 20.02.2021 № 431-р (ред. от 07.06.2021) «Об утверждении Концепции цифровой и функциональной трансформации социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, на период до 2025 года» // Собрание законодательства Российской Федерации. 2021. № 10. Ст. 1634.

2. Расширенное заседание коллегии МВД России 20.03.2023 [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/transcripts/70744> (дата обращения: 28.03.2023).

3. Федотов Н.Н. Форензика – компьютерная криминалистика. – Москва: Юридический Мир, 2007. – 432 с.

4. Форензика [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/Форензика> (дата обращения: 28.03.2023).

5. Пискунов И. Искусство форензики. Теория, книги, курсы, полезные материалы // Журнал Хакер [Электронный ресурс]. – URL: <https://hacker.ru/2018/04/03/forensics-guide-1/> (дата обращения: 28.03.2023).

6. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023) (п. 9. ч. 1 ст. 204) // Собрание законодательства Российской Федерации. 2001. № 52. Ч. 1. Ст. 4921.

7. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» (ред. от 28.12.2022) // Собрание законодательства Российской Федерации. 2011. № 7. Ст. 900.

8. Архипцев И.Н. Кибербезопасность и компьютерная грамотность в правоохранительных органах / И.Н. Архипцев, А.Э. Федосеев, А.Э. Федосеев [и др.] // Пробелы в российском законодательстве. 2021. № 4. С. 276–279.

9. Приказ Минобрнауки России от 27.07.2021 № 677 «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 40.03.02 Обеспечение законности и правопорядка» (зарегистрировано в Минюсте России 19.08.2021 № 64694) // СПС «КонсультантПлюс».

АКТУАЛЬНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПОЛИЦИИ В НАПРАВЛЕНИИ БОРЬБЫ С ДИСТАНЦИОННЫМ ХИЩЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ

Худяков В.В.,

Костюнина В.А.

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: вопросы правового регулирования деятельности полиции в направлении борьбы с дистанционным хищением денежных средств в настоящее время занимают одну из ведущих позиций в государстве. Такая необходимость объясняется тем, что вред от преступлений, совершаемых дистанционным способом, оценить и предотвратить почти невозможно и это значительно усложняет ситуацию в их расследовании и обеспечении безопасности во всем киберпространстве. В целом анализ совершенных мошеннических действий дистанционным способом позволяет отметить, что происходящий в современном мире процесс цифровизации значительно повлиял как на преступника и совер-

шаемые им деяния, так и на правоохранительные структуры и уровень подготовки специалистов, препятствующих совершению преступлений.

Ключевые слова: цифровизация, киберпреступления, дистанционное мошенничество, хищение безналичных денежных средств, мошенничество, IT-технологии.

CURRENT ISSUES OF LEGAL REGULATION OF POLICE ACTION TO COMBAT REMOTE MONEY THEFT

**Khudyakov V.V.,
Kostunina V.A.**

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: issues of legal regulation of police activity in direction of combating remote money embezzlement nowadays occupy one of the leading positions in the state. Such necessity, is explained by that harm from crimes made a remote way is almost impossible to estimate and prevent, and it, considerably complicates a situation in their investigation and maintenance of safety in all cyberspace. Overall, analysis of remote frauds allows us to note that the process of digitalization occurring in today's world has significantly affected both the offender and his acts, as well as law enforcement structures and the level of training of professionals that prevent the commission of crimes.

Keywords: digitalization, cybercrime, remote fraud, theft of non-cash funds, fraud, IT-technologies.

Институты частной собственности согласно ст. 35 Конституции Российской Федерации охраняются законом. Так, с развитием новых IT-технологий безналичные денежные средства стали популярным средством для цифрового гражданского оборота, в связи с чем, государство должно осуществлять правоохранительную политику по профилактике и предотвращению преступлений, направленных на посягательство на данную собственность в киберпространстве.

Особая актуальность проблемы преступлений, которые совершаются дистанционным способом, обусловлена их распространением, сложностью квалификации и предупреждения. Это больше относится к компьютерному мошенничеству, совершаемому дистанционным способом, но значительное место в их числе занимает мошенничество в сфере банковских технологий, связанных с использованием поддельных банковских карт и телефонных звонков на номера потенциальных жертв.

Происходящий в современном мире процесс цифровизации повлек изменение, характерное для структуры всей преступности. Сами же дистанционные хищения безналичных денежных средств следует рассматривать как преступления, которые характеризуется особым способом и орудием совершения преступления в виде использования информационных и технических средств [3, с. 93].

Сама организация борьбы с дистанционными преступлениями и тактика ее осуществления сотрудниками полиции имеет свои особенности, выраженные в том, что поступление сообщения о совершении дистанционным способом уголовно-наказуемого деяния в анализируемой сфере еще до возбуждения уголовного дела требует своей проверки. На этом этапе возникает множество вопросов, требующих тщательного анализа, в том числе и о месте окончания преступления, так как от этого зависит решение вопроса о территориальной подследственности преступления [2].

Дистанционные преступления составляют значительную часть всех преступлений, им присущи высокая латентность, сложность выявления следов и доказывания преступной деятельности. Так, интернет-площадка может стать и местом преступления, и орудием совершения противоправных действий. Таким преступлениям присущи следующие признаки:

- крупный ущерб;
- особый субъект преступления;
- часто международный, транснациональный характер преступления, что весьма затрудняет борьбу с ними.

Вместе с тем причиной роста большого числа мошеннических посягательств послужила тяжелая эпидемиологическая обстановка, которая началась в марте 2020 г., и благодаря чему преступность ушла в киберпространство, а также постоянное совершенствование новых способов хищения денежных средств, которые не отстают от процессов цифровизации всех сфер общественной жизни. Раскрытие преступлений, совершенных дистанционным способом, усложняется использованием преступниками при совершении своих противоправных действий новейших технических средств и способов конспирации. В связи с отмеченным действующее правовое обеспечение деятельности, осуществляемое подразделениями полиции по борьбе с дистанционными хищениями безналичных денежных средств, должно соответствовать современным реалиям.

Является показательным следующий пример. Так, гражданин З., обладая познаниями в области информационных технологий, использования компьютерных средств и оборудования, путем применения программного обеспечения, способного перехватывать управление мобильными устройствами, в операционной системе которых уже имеются вредоносные файлы, без ведома владельца мобильного устройства, получил возможность управления некоторыми гаджетами. Убедившись в том, что эти устройства используются их владельцами для работы с программным приложением «Мобильный банк», принадлежащим ПАО «Сбербанк России», З. удаленно отправил с мобильных устройств СМС-сообщения на короткий номер «900» автоматизированного СМС-сервиса для перевода денежных средств со счета жертв на подставной банковский счет с целью последующего обналичивания похищенных средств [3].

В связи с подобными ситуациями рекомендуется проведение разъяснительной работы с клиентами банка об особенностях использования некоторых сервисов, в частности об опасности разглашения посторонним субъектам своих личных данных.

Дополнительно, с целью усиления мер по борьбе с дистанционными преступлениями, 19 декабря 2019 года руководителем Следственного комитета России подписан приказ о создании в составе Главного следственного управления отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий. Такое решение обусловлено ростом числа киберпреступлений в Российской Федерации за последние годы, как сообщили в пресс-службе ведомства. Следователи созданного отдела специализируются в расследовании преступлений указанной категории, отличающихся особой спецификой. По данным этого ведомства, расследование киберпреступлений представляет особую сложность, поскольку оно обусловлено не только спецификой и неочевидностью, «но и присущей ему межрегиональной и международной характеристической особенностью» [8].

Следует отметить также положения уголовно-процессуального закона Российской Федерации, которые регламентируют взаимодействие указанных субъектов. Так, в п. 4 ч. 2 ст. 38 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) следователь наделен правом дачи органу дознания письменных поручений обязательного характера не только о проведении оперативно-разыскных мероприятий, но и о производстве отдельных следственных действий. Данная норма позволяет следователю давать поручения об исполнении постановлений, направленных на задержание, привод, арест соответствующего лица и на выполнение иных действий, предусмотренных уголовно-процессуальным законом [6, с. 92–98].

Борьба с дистанционными хищениями безналичных денежных средств, в особенности совершенных мошенническим путем, требует преодоления препятствий, которые зависят прежде всего от пользователей глобальной Сети и к числу которых относятся:

1. Слабая научная база в рассматриваемой области.
2. Недостаточная квалификация лиц, осуществляющих расследование преступлений соответствующей группы.
3. Недостаточная практика расследования мошенничеств и хищений, совершаемых в глобальной сети Интернет.

Слабая научная база находит свое проявление в том, что изучению проблем мошенничества в Интернете, как и другим IT-преступлениям, в научной литературе достаточного внимания до сих пор не уделяется. Следует отметить, что довольно трудная ситуация складывается тогда, когда определяется место окончания дистанционного хищения безналичных денежных средств: место, с которого был осуществлен их перевод на счет преступника или место, в котором эти деньги были им похищены. Решение этих вопросов требует больших затрат времени, что порождает затягивание начала расследования по уголовному делу. Возможная причина этой проблемы может быть в отсутствии необходимых знаний в области информационных технологий. Такая подготовка даже среди молодых специалистов встречается редко, поэтому труды о проблемах мошенничества в Интернете в юридической периодике практически не публикуются [7, с. 40].

Выявлением и раскрытием преступлений в сфере высоких технологий занимаются специальные подразделения органов внутренних дел, которые специализируются только на подобного рода преступлениях. Так как результат раскрытия преступления на практике часто зависит от своевременности принятого решения, оперативные сотрудники, специализирующиеся на раскрытии мошенничества в сети Интернет, должны совершенствовать свои правовые знания параллельно с изучением IT-технологий, которые обеспечивают эффективное выявление и раскрытие преступлений данного вида. Компенсировать недостаточную практику в выявлении и раскрытии таких преступлений возможно при сотрудничестве и обмене опытом, в том числе и с иностранными коллегами на научно-практических мероприятиях.

Профилактическая разъяснительная работа персонала банков со своими клиентами об особенностях использования некоторых сервисов и соблюдение гражданами элементарных требований информационной безопасности значительно сократит число возможных дистанционных мошенничеств. Консолидация действий правоохранительных органов и финансовых организаций на незамедлительное реагирование, направленное на пресечение действий мошенников, позволит в обозримом будущем создать благоприятные условия для защиты вкладов российских граждан от действий злоумышленников.

Решение обозначенной проблемы нуждается в комплексном подходе с разработкой и внедрением универсальной методики, содержащей необходимую информацию и рекомендации по мошенничествам, совершенным дистанционным способом, вообще и отдельным его видам в частности, что позволит повысить число выявляемых случаев, а также качество их раскрытия и расследования. Наличие такой методики позволит:

- частично алгоритмизировать деятельность оперативных сотрудников и следователей, что облегчит расследование;
- создать рекомендации по эффективному планированию раскрытия и расследования преступлений.

Таким образом, представленные доводы позволяют сделать вывод о том, что в современных условиях особую значимость приобретает правовое регулирование и необходимость совершенствования деятельности, которую осуществляют подразделения уголовного розыска по борьбе с уголовно наказуемыми деяниями, совершенными дистанционным способом. Объясняется это тем, что вред от преступлений, совершаемых дистанционным способом, оценить почти невозможно, и это, вне сомнения, значительно усложняет ситуацию. В целом анализ способов совершения дистанционных мошеннических действий позволяет отметить, что происходящий в современном мире процесс цифровизации повлек изменение, характерное для структуры всей преступности. Мошенники получили возможность использовать инновации при совершении преступлений с применением всемирной глобальной Сети и дистанционных средств связи. Перечисленные способы мошенничества исчерпывающего характера не носят, поскольку развитие цифровых технологий позволяет им совершенствоваться.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ, от 06.10.2022). // СПС «КонсультантПлюс».
2. Письмо МВД России от 13.07.2015 №1/5562 «Об организации работы по противодействию отдельным видам мошенничества» [Электронный ресурс]. – URL: <http://oaji.net/articles/2017/3996-1524422643.pdf> (дата обращения: 30.04.2023).
3. Приговор Уссурийского районного суда Приморского края от 6 июня 2017 г. № 1-513/2017 от 6 июня 2017 г. по делу № 1–513/2017 [Электронный ресурс]. – URL: <http://sudact.ru/regular/doc/P8NIXBB0caLC/> (дата обращения: 05.02.2022).
4. Демин Ю.В. Вопросы совершенствования правовых основ деятельности оперативных подразделений органов внутренних дел по раскрытию дистанционных хищений денежных средств // Вестник Всероссийского института повышения квалификации сотрудников МВД России. 2020. № 3(55). С. 92–98.
5. Савченко М.М. Проблемы уголовно-правовой защиты безопасности денежных средств физических лиц, размещенных на счетах в банках // Юридическое образование и наука. 2021. № 4. С. 34–40.
6. Лунева А.В., Клименко А.К. Алгоритм действий следователей на стадии предварительного расследования уголовного дела о хищении, совершенном бесконтактным способом, путем использования дистанционного банковского обслуживания // Российский следователь. 2021. № 11. С. 34–37.
7. Демидова А.С. Мошенничество в сети Интернет как угроза экономической безопасности молодежи // Наука и образование сегодня. 2017. № 12(23). С. 44–49.
8. В СКР сформирован отдел по расследованию киберпреступлений [Электронный ресурс]. – URL: <https://sledcom.ru/press/events/item/> (дата обращения: 23.05.2023).

ИНФОРМАЦИОННЫЕ СРЕДСТВА ПРОТИВОСТОЯНИЯ ЭКОНОМИЧЕСКИМ ПРЕСТУПЛЕНИЯМ

**Худяков В.В.,
Шелепина В.А.**

(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: экономические преступления являются одним из наиболее болезненных процессов для любого государства, независимо от их масштабов и причиненного ущерба. Это могут быть как финансовые преступления в отношении граждан с причинением незначительного по сумме финансового ущерба, но весьма ощутимого, если рассматривать случаи мошеннических действий, направленных на пенсионеров и малоимущих людей, так и значительные преступления экономической направленности, в результате которых причиненный ущерб государству измеряется сотнями миллионов рублей. Предупреждение подобного рода преступлений – одна из основных задач правоохранительных органов нашей страны. Целостность и сохранность финансовых сбережений позволяет всем гражданам и организациям сфокусироваться на их зарабатывании, а следовательно, повышать благосостояние и экономику всей нашей страны. В статье описаны некоторые решения, позволяющие обеспечить защищенность сбережений и проведение безопасных финансовых операций, широкое применение которых поспособствует значительному снижению экономических преступлений.

Ключевые слова: шифрование, электронная подпись, хэширование, договорные обязательства, контракт, экономические преступления, мошеннические схемы, дистанционное мошенничество

INFORMATION TOOLS FOR COUNTERING ECONOMIC CRIME

**Khudyakov V.V.,
Shelepin V.A.**

(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: economic crimes are one of the most painful jabs for any state, regardless of their scale and the damage caused. These can be financial crimes against citizens with infliction of insignificant financial damage, but very tangible, if we consider cases of fraudulent actions aimed at pensioners and poor people, and significant economic crimes, as a result of which the damage caused to the state is measured in hundreds of millions of rubles. Prevention of such crimes is one of the main tasks of law enforcement agencies of our country. The integrity and safety of financial savings allows all citizens and organizations to focus on their earnings, and therefore increase the welfare and the economy of our entire country. The article describes some solutions, which allow to provide security of savings and secure financial transac-

tions, wide application of which will contribute to significant reduction of economic crimes.

Keywords: encryption, electronic signature, hashing, contractual obligations, contract, economic crimes, fraud schemes, remote fraud.

Актуальность вопроса применения информационных средств в борьбе с экономическими преступлениями является центральной темой многих научно-исследовательских работ. Стоит отметить, что способы совершения экономических преступлений видоизменились. Причина этого – быстро развивающиеся компьютерные технологии и переход общества к новому технологическому укладу. Общественные отношения во многом изменили свой формат и перешли в цифровую среду. На фоне перехода как раз и возросло количество преступлений в экономической сфере, а способ их совершения трансформировался и опосредовал необходимость внедрения цифровых средств противостояния экономическим преступлениям. Экономическое преступление по российскому законодательству представляет собой совокупность общественно опасных деяний, которые направлены на совершении различных махинаций с финансами. Для противостояния им на различных уровнях создаются информационные средства, позволяющие защититься от экономических преступлений. Рассмотрим некоторые из них более подробно и определим их достоинства и недостатки.

Симметричное шифрование – это метод шифрования, при котором один и тот же ключ используется для шифрования и дешифрования информации. Это обеспечивает конфиденциальность, так как только тот, у кого есть ключ, может прочесть зашифрованный текст. Симметричное шифрование может помочь противостоять финансовым махинациям, предоставляя защиту конфиденциальной информации, такой как пароли, банковские реквизиты и другие финансовые данные. При использовании симметричного шифрования данные могут быть зашифрованы с помощью ключа, который известен только уполномоченным пользователям.

Также стоит отметить, что актуальны преступления, целью которых является незаконное получение данных, составляющих коммерческую, налоговую или банковскую тайну. Так, коммерческая тайна представляет собой информацию, которая может быть использована для получения прибыли, увеличения своих доходов. Для недопущения несанкционированного доступа к таким данным многие организации устанавливают программное обеспечение, создающее условия для хранения и передачи конфиденциальных сведений. Для защиты баз данных используются DLP-системы (в переводе с английского Data Leak Prevention – предупреждение хищения сведений). Как отмечают А.Ю. Гречанная и А.Д. Тастенов, основная задача систем DLP – обеспечение выполнения принятой в организации политики конфиденциальности (защита информации от утечки) [2, с. 24]. К основным элементам DLP-системы относятся следующие: сетевой шлюз DLP-систем, которые устанавливаются в Internet-периметр, центр управления и мониторинга, а также агенты на рабочих станциях пользователей. Одним из минусов DLP-систем является то, что они могут создать

ложные срабатывания или блокировать легитимную передачу информации, что может привести к задержкам в работе сотрудников и снижению производительности. Например, система может неправильно классифицировать некоторые данные как конфиденциальные, что приведет к их блокированию при попытке передачи, даже если эти данные не содержат конфиденциальной информации. Кроме того, DLP-системы требуют регулярного обновления и настройки, чтобы они могли обнаруживать новые типы угроз и предотвращать новые методы атак. Это может потребовать дополнительных затрат на обучение сотрудников и поддержку системы. Также, некоторые эксперты отмечают, что DLP-системы не всегда могут защитить от утечек данных, связанных с намеренными действиями злоумышленников или внутренними угрозами. Например, если злоумышленник обходит систему, используя нешифрованный канал связи или крадет данные физическим путем, то DLP-система может быть бесполезной в этом случае.

Криптографические хэш-функции – это математические функции, которые преобразуют входные данные произвольной длины в хэш-код фиксированной длины. Как отмечает в своем исследовании П.Г. Ключарев, криптографические хэш-функции являются одним из важнейших классов криптографических алгоритмов. Они широко используются в задачах обеспечения информационной безопасности [3, с. 161]. Цель такой функции – получить уникальный идентификатор входных данных, который будет сложно или невозможно восстановить, и даже небольшие изменения во входных данных должны приводить к значительным изменениям в хэш-коде. Это делает хэш-функции важными инструментами для защиты информации. Криптографические хэш-функции широко применяются в криптографических протоколах и системах защиты информации для обеспечения целостности, аутентификации и конфиденциальности данных. Например, они могут использоваться для создания цифровых подписей, хранения паролей, защиты файлов и данных в транзакциях.

Эффективная криптографическая хэш-функция должна обладать следующими свойствами:

1. Стойкость к коллизиям. Это означает, что сложно найти два различных набора входных данных, которые дают одинаковый хэш-код.
2. Стойкость к восстановлению, когда невозможно восстановить входные данные по хэш-код.
3. Стойкость к обратной связи. Это отсутствие возможности найти входные данные, которые дают заданный хэш код.
4. Быстрота вычислений. Хэш-функция должна работать достаточно быстро, чтобы не замедлять работу системы.

Наиболее известные криптографические хэш-функции: MD5, SHA-1, SHA-2 и SHA-3. Однако, некоторые из них сейчас считаются небезопасными и должны быть заменены на более современные.

Помимо уже перечисленных преступлений в экономической сфере, актуальными остаются общественно опасные деяния, направленные на регистрацию незаконных сделок с недвижимостью. Главной мотивацией преступников является корыстная заинтересованность, извлечение для себя или других выгоды

имущественного характера. Добавляет актуальности использование онлайн-платформ, выступающих в качестве агрегаторов и выполняющих роль посредника между покупателем и продавцом. Именно на таких платформах, как «ЦИ-АН», «Яндекс-Недвижимость», «Домклик» и другие, происходят обманные действия, направленные на искажение данных при заключении сделки. Данные исследования Финансового университета при правительстве России, проводимые на протяжении пяти лет, показывают, что количество преступлений, связанных с недвижимостью, увеличилось на 18%. В 2015 году было зафиксировано 6 208 таких случаев, а в 2019 году – уже 7 340. Преступления в крупном и особо крупном размере выросли на 28%. В 2020 году эта тенденция продолжилась: 4 129 преступления, зарегистрированные за первое полугодие года, что составляют 56% от прошлогоднего показателя. Мошенничество в особо крупном размере составляет 62% от случаев за весь 2019 год [4]. С развитием информационных технологий мошенники нашли новые способы обмана людей в сфере недвижимости. Они создают фейковые сайты, которые по интерфейсу похожи на известные агрегаторы, и убеждают людей переводить им деньги в качестве залога или предоплаты за аренду квартиры. Мошенники также размещают объявления о продаже жилья и затем уговаривают покупателей перевести им гарантийный взнос или полную стоимость квартиры через систему быстрых переводов. Некоторые мошенники используют новые схемы, такие как мошенничество, под видом сотрудников банков, которые предлагают заключение договоров купли-продажи жилья онлайн с помощью электронной подписи. Еще одной новой схемой мошенничества является предложение заключить договор онлайн, при этом мошенники утверждают, что находятся за границей и выманивают деньги у доверчивых людей [5, с. 27]. В связи с этими новыми способами обмана людей эксперты рекомендуют быть более бдительными при совершении онлайн-операций в сфере недвижимости. Для борьбы с регистрацией незаконных сделок с недвижимым имуществом можно использовать криптографические средства, такие как блокчейн. Эта технология представляет собой выстроенную по определенным правилам непрерывную последовательную цепочку блоков (связный список), содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга [6, с. 27].

При использовании блокчейна для регистрации сделок с недвижимым имуществом каждая сделка, будет записана в блокчейн как транзакция, содержащая информацию о продавце, покупателе, объекте недвижимости и других существенных деталях сделки. Каждая транзакция будет подписана цифровой подписью, которая будет использоваться для проверки подлинности и целостности данных. Таким образом, использование блокчейна позволит создать прозрачную и безопасную систему регистрации сделок с недвижимым имуществом, где каждая сделка будет защищена криптографическими средствами и не сможет быть изменена или удалена без соответствующих прав и разрешений.

Подводя итог вышесказанному можно утверждать, что в настоящее время использование высокотехнологичных средств в противостоянии экономиче-

ским преступлениям является фундаментальной необходимостью. В рамках работы были рассмотрены такие информационные средства, как симметричное шифрование, DLP-системы, криптографические хэш-функции, а также технологии блокчейн. Кратко представлены достоинства каждого из решений для обеспечения защищенности финансовых операций, указаны их недостатки. Приведены примеры экономических преступлений, которым противостоят современные информационные средства. Финансовые махинации эффективно пресекаются инструментами симметричного шифрования, как наиболее оптимальный способ защиты персональных данных. Для противостояния преступлениям в сфере коммерческой, налоговой и банковской тайны многие компании используют DLP-системы, защищающие конфиденциальную информацию. Во избежание регистрации незаконных сделок с имуществом, эффективным инструментом остается блокчейн.

В конечном итоге необходимо понимать, что решающим фактором в противостоянии остается использование актуальных информационных технологий, высокий уровень квалификации сотрудников информационной безопасности, неукоснительное выполнение требований норм, направленных на сбережение конфиденциальной информации и пресечение незаконных действий.

Библиографический список

1. Мешкова Е.В. Симметричное шифрование. Стандарт шифрования данных DES // 2016. № 1(42). С. 278–281.
2. Гречанная А.Ю., Тастенов А.Д. DLP-системы и их роль в защите от утечек конфиденциальной информации // Наука и техника Казахстана. 2015. № 3-4. С. 23–27.
3. Ключарев П.Г. Криптографические хэш-функции, основанные на обобщенных клеточных автоматах // Машиностроение и компьютерные технологии. 2013. С. 161–172.
4. Официальный сайт РБК [Электронный ресурс]. – URL: <https://realty.rbc.ru/news/5f5a31649a794786a2c82a1b> (дата обращения: 09.04.2023).
5. Удел продаж: за год число мошенничеств с жильем в России выросло на 18% [Электронный ресурс]. – URL: <https://iz.ru/1378911/mariia-perevoshchikova/udel-prodazh-za-god-chislo-moshennichestv-s-zhilem-v-rossii-vyroslo-na-18> (дата обращения: 09.04.2023).
6. Балдов Д.В., Петрова С.Ю., Лебедев А.А. Использование технологии блокчейн для защиты данных // International Journal of Open Information Technologies. 2021. С. 27–34.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ СОВЕРШЕНИИ ТЕРРОРИСТИЧЕСКИХ АКТОВ И АКТОВ ЭКСТРЕМИЗМА

Челядинов Д.В.,

кандидат технических наук;

Полякова В.А.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: информационная среда в деятельности правоохранительных органов имеет ключевое значение. Возможности функционирования правоохранительных органов благодаря информационным системам значительно расширяются. Само функционирование информационных баз данных и специализированных программ позволяет органам внутренних дел выявлять, предупреждать, пресекать и раскрывать преступления самых различных категорий. Эта особенность раскрывается во взаимодействии с науками более широкого профиля. К таким наукам принято относить: криминалистику, криминологию и науку оперативно-разыскной деятельности. В своем большинстве информационные технологии и достижения технических разработок используют в работе оперативные подразделения органов внутренних дел на транспорте. Транспортная полиция принимает во внимание опасность совершения актов незаконного вмешательства в работу транспортных комплексов, что требует обязательного использования не только стандартных аппаратур для выявления незаконного провоза предметов, но и инновационных технологий по изучению действий людей, прибывающих на территорию объектов транспорта.

Ключевые слова: информационные технологии на объектах транспорта, террористический акт, акты незаконного вмешательства, деятельность правоохранительных органов по пресечению террористических актов.

INFORMATION TECHNOLOGIES IN THE COMMISSION OF TERRORIST ACTS AND ACTS OF EXTREMISM

Chelyadinov D.V.,

Candidate of Technical Sciences;

Polyakova V.A.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the information environment in the activities of law enforcement agencies is of key importance. The possibilities of functioning of law enforcement agencies thanks to information systems are significantly expanding. The very functioning of information databases and specialized programs allows the internal affairs bodies to identify, prevent, suppress, and solve crimes of various categories. In particular, this feature is revealed in interaction with the sciences of a broader profile.

Such sciences usually include: criminology, criminology and the science of operational investigative activities. For the most part, information technologies and achievements of technical developments are used in their work by operational units of internal affairs bodies in transport. The transport Police takes into account the danger of committing acts of unlawful interference in the operation of transport complexes, which requires the mandatory use of not only standard equipment for detecting illegal transportation of items, but also innovative technologies for studying the actions of people arriving at the territory of transport facilities.

Keywords: information technologies at transport facilities, terrorist act, acts of unlawful interference, activities of law enforcement agencies to suppress terrorist acts.

Складывающаяся на территории страны оперативная и криминогенная обстановка заставляет органы внутренних дел более активно реагировать на те или иные факторы, которые проявляются на подведомственной территории.

Высокий риск совершения террористических актов и актов незаконного вмешательства, риск развития экстремистских движений на территории Российской Федерации крайне велик [5]. Учитывая специфику функционирования нашего государства в условиях специальной военной операции, требуется особобдительное несение службы в приграничных районах. Такой является работа Белгородского ЛО МВД России на транспорте.

Приграничное положение субъектов Российской Федерации всегда считалось наиболее опасным с точки зрения сохранения национальной безопасности страны, которое обусловлено тремя основными элементами: сохранением безопасности личности, общества и государства в целом. Основные элементы национальной безопасности требуют особого контроля для предотвращения террористических актов и актов незаконного вмешательства в работу транспортных комплексов.

Раскрывая сущность исследуемой темы, важно обратить внимание на то, посредством чего могут совершаться уголовно наказуемые деяния, такие как террористический акт и экстремизм [1].

Учитывая уровень развития информационных технологий и переход общества на путь информатизации жизни, важную роль в данный период имеет взаимодействие человека с глобальной сетью Интернет. Высокий уровень зависимости населения от социальных сетей и Интернета говорит о том, что современная работа и выполнение коммуникационных связей между людьми невозможно без социальных сетей.

Однако наряду с положительными факторами социальных сетей существуют значительные «минусы», которые в той или иной степени влияют на становление преступности.

Вместе с совершенствованием современных технологий преступность развивается ускоренными темпами и переходит в социальную среду через средства коммуникационных взаимодействий (смартфоны, персональные компьютеры) [2].

Преступность, переходящая из материального мира в виртуальный, носит новое название «киберпреступность».

Киберпреступность – такой вид преступных посягательств, который развивается благодаря социальным сетям и глобальной сети Интернет. Развитие ее обуславливается несколькими факторами, которые влияют на организаторов и исполнителей преступлений:

1. Возможность скрыть свою личность. Проявляется в тех случаях, когда лицо намеренно использует неправдоподобные данные или фейковые аккаунты для приведения в действие плана по реализации террористических актов и актов экстремистского вмешательства в жизнь населения [4].

2. Широкое распространение персональных мобильных и стационарных устройств, благодаря которому человек постоянно находится в зоне контроля посторонних лиц. Доступ к геолокации гаджета позволяет контролировать и координировать перемещение лица, его использующего.

3. Повсеместный доступ в сеть Интернет. Практически в каждом общественном заведении имеется стационарный доступ к сети Интернет, что позволяет скрывать свою геолокацию от раскрытия. В том числе появляется возможность скрывать свою личность посредством работы в компьютерных клубах [3].

Так, рассмотрев ряд факторов, можно сделать вывод о том, что преступность в среде информационных технологий развивается и продолжает оставаться в тени не до конца разработанных систем информационного обслуживания.

Инновационные технологии представляют собой такие современные устройства и гаджеты, посредством которых злоумышленники могут совершать преступления и оставаться безнаказанными очень долгое время [1]. При всем этом есть риск того, что преступник не прекращает свою деятельность, даже зная, что его разыскивают. Возможность курировать новые преступления и вовлекать в круг своего взаимодействия новые лица является основной целью преступлений, совершаемых через сеть Интернет.

Наиболее актуальными в этой связи являются преступления, направленные на подрыв государственной целостности и конституционного строя, – террористические акты и акты экстремизма.

Указанные противоправные действия имеют особую специфику по характеру их совершения в сети Интернет.

Осуществляя незаконную деятельность по вербовке лиц для совершения террористических актов, организаторы работают с социальными сетями потенциальных исполнителей. Многочасовые изучения личности, контакт через мессенджеры, устрашения и установка правил в общении приводят к тому, что лица на добровольной основе переходят в организованные преступные группы и самостоятельно планируют, организывают и исполняют указания по совершению террористических актов [3].

Экстремистская деятельность, в свою очередь, раскрывается посредством разжигания тех или иных конфликтов на территории Российской Федерации. Важно учесть, что Россия – многонациональная страна, которая объединяет множество народов, языков, вероисповеданий. Разжигание межнациональной

розни не является сложным делом для организаторов террористических и экстремистских движений.

Зачастую проводя свою работу по вербовке, сами организаторы находятся далеко за пределами России. Из-за рубежа совершается более 15% всех преступных посягательств на конституционный строй Российской Федерации [6]. Так, можно прийти к выводу, что работа преступных элементов напрямую связана с социальными сетями и вербовкой потенциальных исполнителей через глобальную сеть Интернет.

Повсеместное распространение Интернета позволило не только значительно облегчить жизни людей, но и создало новые возможности для проведения незаконных операций по совершению преступлений из-за рубежа.

Без особой сложности у организаторов появляется возможность изучать личности людей, анализировать их активную деятельность в социальных сетях и в последующем вербовать их для организации террористических актов.

Террористические акты, совершаемые жителями Российской Федерации, наиболее часто являются спонсируемыми из-за рубежа. В то время как спонсирование экстремистской деятельности проявляется не только из стран зарубежья, но и с территории нашей страны. Разжигание межконфессиональных и межнациональных конфликтов порождает нестабильность в социальном строе Российской Федерации.

Работа правоохранительных органов зачастую предусматривает анализ социальных сетей на предмет экстремистских высказываний. Посредством работы с информационными технологиями и современными техническими средствами правоохранительные органы могут предпринимать попытки в пресечении крупных террористических актов, а также работать над раскрытием личностей, организующих и спонсирующих террористические акты на территории страны.

Библиографический список

1. Демидов О. Применение международного права в киберпространстве // Индекс безопасности. 2019. № 3(114). Т. 21. С. 107.
2. Институт административной ответственности: монография / С.Г. Камолов, Е.А. Кириллова, А.В. Павлюк. – Москва: Актуальность.рф., 2020. – 208 с.
3. Камолов С.Г., Коржов И.А. Проблемы повышения квалификации государственных и муниципальных служащих // Право. Журнал Высшей школы экономики. 2021. № 3. С. 185–189.
4. Номокова В.А., Тропинина Т.Л. Киберпреступность как новая криминальная угроза // Криминалистика. Вчера. Сегодня. Завтра. 2012. № 1(24). С. 45–55.
5. Кузнецов С. Кибербезопасность в XIX веке / Открытие системы СУБД [Электронный ресурс]. – URL: <http://www.osp.ru>
6. Официальный сайт МВД России [Электронный ресурс]. – URL: <https://мвд.рф/mvd/> (дата обращения: 16.05.2023).

АКТУАЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РАЗЫСКОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Черняков С.А.,

кандидат юридических наук, доцент

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в основе эффективной и результативной деятельности по выявлению, пресечению и раскрытию преступлений лежит информационно-аналитическое обеспечение субъектов оперативно-разыскной деятельности, в особенности на первоначальном этапе оперативных проверок. Полнота сведений о событиях, фактах, обстоятельствах произошедшего, особенностях лиц, имеющих отношение к материалам проверки, во многом определяет возможность объективности и вероятности формирования версий и планирования проведения оперативных мероприятий. Однако далеко не всегда субъекты оперативной деятельности в силу профессиональной компетенции или по причине организационных просчетов имеют возможность получать сведения в объеме, достаточном для качественного оперативного анализа. В статье в упрощенном виде определена система официальных и неофициальных информационных сервисов, которые могут быть использованы оперативными сотрудниками органов внутренних дел для получения сведений, представляющих интерес для нужд оперативно-разыскной деятельности.

Ключевые слова: оперативно-разыскная деятельность, информационно-аналитическое обеспечение, учеты, базы данных.

ACTUAL ASPECTS OF INFORMATION SUPPORT OF OPERATIONAL AND INVESTIGATIVE ACTIVITIES OF THE INTERNAL AFFAIRS BODIES OF RUSSIAN FEDERATION

Chernyakov S.A.,

Candidate of Law, Associate Professor

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the basis of effective and efficient activities for the detection, suppression and disclosure of crimes is the information and analytical support of the subjects of operational investigative activities, especially at the initial stage of operational inspections. The completeness of information about the event, facts, circumstances of the incident, the characteristics of persons related to the verification materials largely determines the possibility of objectivity and probability of forming versions and planning operational activities. However, it is not always the subjects of operational activity, due to professional competence or due to organizational miscalculations, have the opportunity to receive information in an amount sufficient for qualita-

tive operational analysis. The article, in a simplified form, defines a system of official and unofficial information services that can be used by operational officers of the internal affairs bodies to obtain information of interest to the needs of operational investigative activities.

Keywords: operational investigative activity, information and analytical support, records, databases.

Динамика изменения криминогенной обстановки, развития криминальных угроз и, соответственно, процессов, протекающих в системе МВД России, предъявляют особые требования к организации информационно-аналитического обеспечения оперативно-разыскной деятельности [3, с. 60].

От правильной организации сбора, систематизации и хранения данных, достоверности, полноты, точности и своевременного обеспечения органов внутренних дел оперативной информацией напрямую зависит эффективность противодействия преступности [1].

В настоящее время для информационного обеспечения органов внутренних дел (далее – ОВД) создаются и используются различные информационные системы, в основе которых лежит учет точных сведений о разнообразных объектах, представляющих оперативный интерес. Информационному обеспечению деятельности ОВД способствуют также информационные системы (учеты) других ведомств, предприятий и организаций.

Главным назначением информационных систем (учетов) является преобразование всех видов информации в целостную систему, позволяющую обеспечить возможность неоднократного обращения к ней пользователей в целях предупреждения и раскрытия преступлений, розыска преступников, установления личности неопознанных трупов, лиц, скрывающих анкетные данные и пр. [2, с. 166].

К настоящему времени сложилась следующая система официальных и неофициальных информационных сервисов, которые могут быть использованы оперативными сотрудниками органов внутренних дел для получения сведений, представляющих интерес для нужд оперативно-разыскной деятельности. Данная система состоит из трех условных элементов: «Сервисы ИСОД МВД России», «Ведомственные информационные сервисы», «Информационные сервисы иных ведомств и учреждений».

Раздел «Сервисы ИСОД МВД России» предусматривает возможность общего ознакомления с порядком подключения к сервису с использованием учетных данных, реестром доступных информационных ресурсов, функциональными возможностями сервисов и основами работы с ними.

Данным разделом обеспечивается ознакомление с такими информационно-поисковыми сервисами, как «Следопыт-М», «Ксенон – 2», «ПТК – "Розыск – Магистраль"», «Сервис НОИ» и др., предназначенными для поиска, сбора, обработки и предоставления сотрудникам оперативных подразделений информации, получаемой из разнородных информационных систем и баз данных.

Раздел «Ведомственные информационные сервисы» предназначен для ознакомления с основами работы сервисов и ресурсов, предоставляемых МВД России, а также изучения их особенностей и перечня получаемых сведений.

В данном разделе представлена возможность изучения подсистем интегрированной базы данных федерального уровня «Опознание (биометрическая идентификация)» и «Дистанционное мошенничество»; интегрированного банка данных коллективного использования регионального уровня (ИБД-Р); онлайн-сервисов ГИБДД МВД России, ГУВМ МВД России и др.

Раздел «Информационные сервисы иных ведомств и учреждений» позволяет ознакомиться с порядком функционирования, особенностями поиска и обработки информации в различных сервисах, а также перечнем получаемых сведений.

В этом разделе представлены сервисы Минсельхоза России, МЧС России, Казначейства России, ФССП России и др., а также ряд интернет-ресурсов, посредством которых может быть получена оперативно значимая информация.

Таким образом, можно прийти к выводу о том, что для информационного обеспечения оперативно-разыскной деятельности органы внутренних дел создают и используют различные информационные системы, в основе которых лежит оперативный учет точных сведений о разнообразных объектах, попадающих в сферу оперативно-разыскной деятельности.

Следует, однако, иметь в виду, что информационному обеспечению ОРД способствуют также учеты (информационные системы) других государственных и негосударственных предприятий, организаций России, а также международных полицейских организаций и органов зарубежных государств, взаимодействующих с российскими правоохранительными органами на основе международных договоров.

Библиографический список

1. Приказ МВД России от 12 мая 1993 г. № 229 «О мерах по реализации Концепции развития системы информационного обеспечения органов внутренних дел в борьбе с преступностью» // СПС «КонсультантПлюс».
2. Саркисян Г.Г. Информационное обеспечение деятельности оперативных подразделений органов внутренних дел // Труды Академии управления МВД России. 2018. № 2(46). С. 165–169.
3. Япаров Р.М. Проблемы информационно-аналитического обеспечения оперативно-разыскной деятельности органов внутренних дел // Вестник Уфимского юридического института МВД России. 2013. № 1(59). С. 59–63.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ С УЧЕТОМ СОВРЕМЕННЫХ РЕАЛИЙ

Чижов И.А.,

кандидат юридических наук, доцент;

Якусик А.А.

(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются угрозы информационной безопасности информационных систем, используемых в деятельности органов внутренних дел Российской Федерации в условиях роста киберпреступности и проведения специальной военной операции, а также классификация угроз информационной безопасности. Уделено внимание нарушению информационной безопасности с учетом поступающих из внутренней и внешней среды угроз, которые могут приводить к множеству негативных последствий.

Ключевые слова: информация, информационное пространство, информационная безопасность, обеспечение безопасности.

THREATS TO INFORMATION SECURITY IN INTERNAL AFFAIRS BODIES TAKEN INTO CONSIDERATION OF MODERN REALITIES

Chizhov I.A.,

Candidate of Law, Associate Professor;

Yakushik A.A.

(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article discusses the threats to information security of information systems used in the activities of the internal affairs bodies of the Russian Federation in the context of the growth of cybercrime and the conduct of a special military operation, as well as the classification of threats to information security. Attention is paid to the violation of information security, taking into account the threats coming from the internal and external environment, which can lead to many negative consequences.

Keywords: information, information space, information security, security.

При рассмотрении тематики научной статьи первоначально необходимо обозначить основные термины и понятия.

Так, для наибольшего понимания сути проблематики, требуется обширное объяснение термина «информационная безопасность».

Информационная безопасность – это система, разработанная для обеспечения безопасного пользования информационной средой. Действительная прак-

тика, предотвращающая искажение, порчу, раскрытие и изменение информации, хранящейся в базе данных.

Информационная безопасность, представленная в виде целостной системы, имеет определенные характеристики и основные черты. Как система, поддерживаемая с помощью работы человека и компьютера, информационная безопасность имеет ряд задач, функций и целей своего функционирования.

Так, целью работы информационной системы и целью существования информационной безопасности выступают следующие положения – обеспечение конфиденциальности, подлинности, доступности и целостности. В ряде случаев присуще такое свойство, как особая секретность.

Разбирая цель по основным положениям, важно отметить, что целостность и конфиденциальность зачастую становятся наиболее уязвимыми секторами работы системы.

Конфиденциальность может быть нарушена в целях рассекречивания информации, нарушения целостности работы системы, а также в целях уничтожения или управления засекреченными данными.

Целостность, представляемая в виде совокупности информационных ресурсов или документов, нередко оказывается под угрозой. Нарушить целостность того или иного документа можно при помощи одного символа или изменения структуры документа.

Говоря об основных рисках, с которыми может сталкиваться человек или персональный компьютер при работе с информационной системой или базой, стоит уделить особое внимание рискам:

1. Риск утечки информации.

Они могут возникать в результате неправомерного внедрения в работу информационной системы. Утечка информации – одна из наиболее опасных угроз информационной системе в целом. Частичное или полное оглашение информации ограниченного доступа может представлять угрозу информационной базе всего ведомства.

Применительно к работе системы органов внутренних дел можно говорить о том, что утечка информации может привести не только к потере данных, но и к раскрытию государственной либо другой иной, охраняемой законодательством Российской Федерации, тайны. Любые неконтролируемые потоки информации, распространенные за пределы информационной среды (в которой они были размещены), включая организации, помещения, здания, какую-либо территорию, а также определенный круг лиц, могут представлять опасность для системы информационного обеспечения.

2. Риск потери или недоступности важных данных.

Вне зависимости от природы образования угрозы потеря либо искажение информации могут приводить к сбоям в работе целостных систем. Органы внутренних дел строят свою работу на основе информационных баз данных.

Риски, связанные с применением пиратства, хакерских атак и массированного информационного потока, – все эти действия могут приводить к потере или искажению информации.

3. Риск использования искаженной или недостоверной информации.

После получения информации в искаженном виде, без достаточной проверки и без усиленного контроля за достоверностью, существует риск использования искажений в реальном ведении дел.

Информационные потоки, подвергнутые искажению и ставшие несправедливыми, могут вредить не только системе баз данных ОВД Российской Федерации, но и гражданскому населению, которое получает информацию от Министерства внутренних дел Российской Федерации.

По мнению некоторых ученых, информационная безопасность представляет собой комплекс мер, направленный на защиту информации от различного вида угроз.

Применительно к тематике информационной безопасности в органах внутренних дел стоит отразить важность понимания понятия «информационных гроз».

Информационные угрозы – внешние и внутренние факторы, которые могут влиять на работу информационной системы. Такие угрозы могут влиять на систему как одномоментно, так и на постоянной основе.

Принимая во внимание факт нынешнего положения нашей страны – проведение на территории России Специальной военной операции, важно сказать о том, какие угрозы могут возникать для всей информационной базы и системы МВД России в соответствии с текущей оперативной обстановкой. Важно понимать, что особенностью работы информационных баз данных во многом зависит от успешной работы российских военных формирований и армии России в целом. Насколько будет успешной оборона законных границ страны, настолько же и качественной будет защита стратегических объектов на территории проведения СВО.

Работа противовоздушной обороны, работа органов ФСБ, таможенный контроль и многая другая деятельность профессионалов могут вносить весомый вклад в сохранение целостности информации и в сохранение важных информационных баз данных.

Кроме работы ПВО России, необходимо отметить и противодиверсионную работу в органах внутренних дел. Поскольку такая отрасль работы позволяет пресекать террористические акты на территории законных границ Российской Федерации, можно сказать о том, что множество стратегически важных наземных объектов находятся в защищенном положении.

Проведение СВО на территории Российской Федерации представляет особые условия функционирования МВД России, что приводит к появлению новых угроз, а как следствие, и новые решения возникающих проблем. При защите информации и при обеспечении информационной безопасности, важное положение занимают те подразделения системы МВД России, которые курируют инженерно-техническую часть работы специальных подразделений.

Важно понимать, что угрозы информационной безопасности могут быть двух видов:

1. Внешние угрозы.

Важно учесть, что данную классификацию стоит основывать на физическом положении угрозы.

Внешние угрозы приходят из других государств, влияние на которые без особой нормативно-правовой регламентации невозможно. Недружественные страны, стремления которых основаны на подчинении своей воле информационных потоков, достаточно усердно проводят политику противодействия информационной безопасности объектов.

Приводя пример и исходя из современных реалий, стоит отразить работу установок противовоздушной обороны страны. Ссылаясь на работу ПВО, можно привести такие случаи, когда атака дронов-камикадзе приводит к нарушению целостности линий электропередач, разрушению объектов и зданий. Нередки случаи применения беспилотных летательных аппаратов, которые совершают террористические акты, направленные на объекты инфраструктуры.

Нарушая целостность объектов МВД России, а также зданий и сооружений гражданского массива, у недружественных стран появляется реальная возможность приведения в негодность информационных систем, в том числе приводящих к сбоям в той или иной информационной базе МВД России.

2. Внутренние угрозы.

Те угрозы, которые совершаются на территории одной страны.

Так, сюда можно отнести хакерские атаки, совершаемые с целью хищения той или иной информации. Цель работы хакеров в одном государстве с объектами преступного посягательства проста – извлечение выгоды из большого информационного потока.

Также, используя в качестве примера работу ПВО, можно сказать о существенных рисках. Успешная работа противовоздушной обороны – это сбитые БПЛА и пресечение террористических атак с воздуха. Когда воздушная цель перехвачена ракетами ударных установок ПВО России, осколки и части сбитых воздушных целей оказываются на земле, нередко принося урон наземным объектам.

Так, успешная работа ПВО может приводить к разрушениям меньшего масштаба, однако существуют риски и повреждения стратегических объектов на земле.

Затрагивая классификацию угроз по различным признакам, можно выделить следующие аспекты:

1. По размерам наносимого ущерба:

Данная классификация содержит в себе три основных положения:

а) общие. Вред, наносимый данной подкатегорией, представляет собой сложную систему воздействия на информационную безопасность системы органов внутренних дел в целом. Причинение вреда направлено на целостный объект обеспечения информационной безопасности. Вред, наносимый указанным типом, оценивается как значительный.

б) локальные. Причинение вреда локальным типом представляет собой такой вред, который будет нанесен только определенной части объекта информационной безопасности. Как правило, такой вред наносится самой малозащищенной или наиболее подверженной риску части. Такой вред оценивается как вред средней тяжести.

Однако нередко случаи хакерских атак и серьезных покушений на информационную безопасность, когда вред, наносимый локально, приводит к риску для всей системы объекта. Через наиболее слабое звено может произойти влияние на всю информационную систему;

в) частные. Такой тип угрозы характеризуется нанесением вреда отдельным свойствам элементов объекта информационной безопасности. Вред причиняемый такой незначительной «частной» угрозой также может приводить к подрыву безопасности полноценной системы.

2. По степени воздействия на информационную систему.

а) пассивные. Такой тип угроз, при котором содержание и структура информационной системы не подвергается изменениям или значительным утратам. Такие угрозы характеризуются относительно недолгим влиянием на систему и кратковременной нестабильностью объекта информации;

б) активные. Угрозы, несущие в себе особую опасность. Такие угрозы информационной системе, могут менять не только структуру и содержание объекта безопасности, но и наносить различный вред охраняемой информации.

3. По природе возникновения.

а) естественные. Такие угрозы, в природе которых не был заинтересован человек и ее происшествие не было направлено от человека. Угрозы такого характера включают в себя физические процессы и стихийные бедствия, которые не могут зависеть от воли человека.

б) искусственные. Угрозы информационной системе, которые произошли вследствие тех или иных действий человека. В свою очередь, искусственные угрозы принято делить:

– на преднамеренные (действия человека, которые привели к ошибке в системе): специальное изменение структуры, искажение исходной информации, раскрытие кодов доступа, изменение в структуре доступа к системе, разработка внедрение вирусных программ;

– непреднамеренные (действия или бездействия человека, не носящие в себе прямого умысла – подрыв информационной безопасности): неосторожность в использовании ключей доступа, раскрытие информации ограничено в открытом доступе.

Подводя итог всему вышеизложенному, стоит отметить, что системы информационной безопасности представляют собой целостную и защищенную комплексную программу, так называемый объект информационной политики государства.

Множество рассмотренных угроз свидетельствуют о том, что современные условия развития мира требуют наиболее кропотливого полноценного рабочего процесса по защите информации.

Информационные системы органов внутренних дел Российской Федерации представляют наиболее широкий спектр возможностей для борьбы с противоправными атаками с целью извлечения выгоды. Так, наиболее актуальным направлением можно обозначить совершенствование системы безопасности информации и обеспечение защиты информационных систем органов внутренних дел Российской Федерации.

Библиографический список

1. Громов Ю.Ю. Информационная безопасность и защита информации: учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2019. – 384 с.
2. Запечников С.В., Милославская Н.Г. Информационная безопасность открытых систем. В 2-х т. Т. 1. Угрозы, уязвимости, атаки и подходы к защите. – Москва: ГЛТ, 2019. – 536 с.
3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – Москва: ГЛТ, 2021. – 280 с.
4. Семененко В.А. Информационная безопасность: учебное пособие. – Москва: МГИУ, 2022. – 277 с.
5. Чипига А.Ф. Информационная безопасность автоматизированных систем. – Москва: Гелиос АРВ, 2019. – 336 с.
6. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – Москва: ИД ФОРУМ, НИЦ ИНФРА-М, 2021. – 416 с.

СОДЕРЖАНИЕ

Аветисян К.Р., Аветисян Б.Р.	Совершенствование механизма информационного противоборства незаконной организации и проведению азартных игр 3
Акапьев В.Л., Горбатовская М.С.	Методики расследования преступлений в сфере информационных технологий 6
Акапьев В.Л., Кнутарев А.В.	Использование информационных технологий и систем в мероприятиях по обнаружению наркотических веществ 14
Александров А.Н.	Уголовно-процессуальные и организационные аспекты производства допроса путем использования систем видео-конференц-связи (статья 189.1 Уголовно-процессуального кодекса Российской Федерации) 18
Беспалова А.О., Челядинов Д.В.	Особенности расследования преступлений, совершенных с использованием сети Интернет 23
Борисенко А.В.	Человеческий фактор в системе кибербезопасности 27
Гаврющенко А.П.	Кибербезопасность. Проблемы мотивации обучения 31
Гончар В.В., Аветисян К.Р., Аветисян Б.Р.	Деанонимизация правонарушителей в сети: проблемы и отдельные пути решения 38
Григорусь Л.Н., Мамутов Э.Э.	Роль рекламного и PR-текста как формы массовой коммуникации на примере киноиндустрии 47
Дрога А.А., Горковенко В.С.	Особенности классификации киберпреступлений 53
Дрога А.А., Хоробрая А.В.	Раскрытие и расследование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий 59

Дубинина Н.М., Войтухова А.А.	Искусственный интеллект и обучающие системы в образовании 64
Дунаев Р.А., Перепелкин И.Н.	О некоторых аспектах информационной безопасности в условиях киберпространства 68
Емельянова О.В.	Использование искусственного интеллекта для обнаружения преступлений 72
Жмурко Д.Ю., Иванов И.П.	Вероятные этапы цифровой трансформации в правоохранительной деятельности России 77
Захаров Д.С., Бельчиков Н.С.	Актуальные вопросы дистанционного производства по уголовному делу 91
Зинченко Д.С.	Использование возможностей сетевых ресурсов в целях деанонимизации преступников, совершающих незаконный оборот наркотиков в виртуальной среде 95
Ивануха И.С.	Возможности и недостатки сервисов ИСОД МВД России 99
Калашникова А.А., Ершова Е.Ю.	Правовое регулирование применения электронных сервисов в деятельности правоохранительных органов 105
Калашникова А.А., Орлов М.А.	Роль информационных технологий в предотвращении политических экстремистских действий 108
Ковалева Е.Г., Бессонов Д.И.	Проблемы обнаружения признаков совершения преступлений в сфере незаконного оборота наркотиков в компьютерных сетях 112
Ковалева Е.Г., Рыбальченко М.А.	Проблемы раскрытия информационных преступлений 115
Ковалева Е.Г., Ткач П.А.	Методы поиска признаков совершения преступлений в сфере незаконного оборота наркотиков в компьютерных сетях 118
Кургузов А.В.	Технологии искусственного интеллекта в правоохранительной деятельности 121

Куриленко Ю.А., Любаева Д.С.	Мошенничества в сфере компьютерной информации	125
Карпика А.Г., Лемайкина С.В.	Актуальные вопросы киберпреследования ...	128
Меняйло Д.В., Меняйло Л.Н., Горковенко В.С.	Некоторые аспекты информационной безопасности деятельности органов внутренних дел в контексте информационного противоборства	132
Нестеренко И.С., Бровченко С.Ю.	Использование IT-технологий (мессенджера Telegram) в целях правового просвещения населения и профилактики кибермошенничества	136
Новоселов Н.Г.	Интернет-магазин как средство реализации наркотических средств и психотропных веществ	144
Пантелеева Е.В., Куриленко Ю.А.	Внедрение цифровых технологий в деятельность правоохранительных органов	146
Попадьина В.А., Калашникова А.А.	Значимость информационных технологий для противодействия терроризму	150
Рыбальченко А.Ю., Коротков А.А.	Информационное обеспечение оперативно-разыскной деятельности при раскрытии преступлений с использованием компьютерных технологий	153
Савотченко С.Е., Желанов А.А.	Современные технологии кибертерроризма	156
Савотченко С.Е., Смирнов П.А.	Место и роль программного обеспечения в противодействии преступлениям в сфере незаконного оборота наркотиков	160
Страхов А.А., Прокопенко А.Н.	Криминальный потенциал искусственного интеллекта	164
Федосеев А.Э., Назаренко И.С.	Элементы форензики – составляющая цифровой грамотности сотрудника ОВД	172

Худяков В.В., Костюнина В.А.	Актуальные вопросы правового регулирования деятельности полиции в направлении борьбы с дистанционным хищением денежных средств	177
Худяков В.В., Шелепина В.А.	Информационные средства противостояния экономическим преступлениям	183
Челядинов Д.В., Полякова В.А.	Информационные технологии при совершении террористических актов и актов экстремизма	188
Черняков С.А.	Актуальные аспекты информационного обеспечения оперативно-разыскной деятельности органов внутренних дел Российской Федерации	192
Чижов И.А., Якусик А.А.	Угрозы информационной безопасности в органах внутренних дел с учетом современных реалий	195

НАУЧНОЕ ИЗДАНИЕ

**Проблемы информационного обеспечения деятельности
правоохранительных органов**

Сборник статей 10-й Международной научно-практической конференции
19 мая 2023 года

Редактор
Комп. верстка

О.И. Шановал
И.Ю. Чернышева, Н.В. Булгакова

Подписано в печать 2023 г., Формат 60х90/16
Усл. печ. л. 12. Тираж 27 экз. Заказ 53

Отпечатано в отделении полиграфической и оперативной печати
Белгородского юридического института МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-513-6

