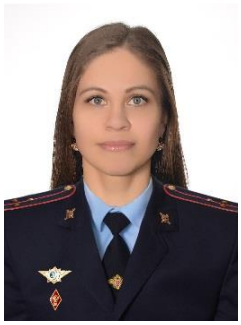
Научная статья
doi: 10.29039/2312-7937-2024-2-38-43



СИДОРОВА ЕКАТЕРИНА ЗАКАРИЕВНА
Восточно-Сибирский институт МВД России (Иркутск, Россия)

ketrik6@mail.ru

ORCID.ORG/0000-0001-5045-2054

УСОВ ЕВГЕНИЙ ГЕННАДЬЕВИЧ
Байкальский институт БРИКС ИРНИТУ (Иркутск, Россия)

usov.evgeniy@list.ru

Основные меры предупреждения цифровой преступности

Аннотация. В статье представлена общая характеристика основных мер предупреждения цифровой преступности. По мнению авторов, к цифровым (кибер) преступлениям следует относить все виды уголовно наказуемых деяний, совершаемых с использованием современных цифровых технологий. А поскольку цифровые технологии широко используются в повседневной жизни, риск стать жертвой цифрового преступления значительно увеличивается. Именно поэтому в современный период развития общества очень важно уделять внимание вопросам профилактики цифровой преступности. Авторы подчеркивают, что в основе предупреждения цифровых преступлений лежит нормативное регулирование отношений в сфере цифровых технологий. Опираясь на действующее законодательство, субъекты профилактики обеспечивают превенцию киберпреступлений. В борьбе с цифровыми преступлениями большое значение имеет институт информационно-аналитического обеспечения, который не ограничивается только использованием СМИ и сети Интернет. Информационно-аналитическое обеспечение предполагает также использование различных информационных банков данных, различного программного обеспечения, направленного на своевременное получение оперативно значимой информации, необходимой для успешного предупреждения и пресечения совершаемых цифровых преступлений. Превенция цифровой преступности невозможна без проведения различных оперативно-розыскных мероприятий, которые осуществляют сотрудники оперативных подразделений. Занимаясь пресечением и раскрытием киберпреступлений, сотрудники данных подразделений реализуют правоохранительную функцию государства. При этом в распоряжении оперативных подразделений органов внутренних дел имеются как гласные (открытые), так и негласные методы проведения оперативно-розыскных мероприятий. В завершении исследования авторы подчеркивают, что пресечение и раскрытие цифровых преступлений носит многоплановый характер. Только комплексный, всесторонний подход к профилактике цифровой преступности способен принести эффективные результаты и снижение показателей данного вида преступности.

Ключевые слова и словосочетания: цифровая преступность, киберпреступления, профилактика, криминологическое предупреждение, превенция, органы внутренних дел.

Для цитирования: *Сидорова Е.З., Усов Е.Г. Основные меры предупреждения цифровой преступности // Вестник ВИПК МВД России. – 2024. – № 2 (70). – С. 38-43; doi: 10.29039/2312-7937-2024-2-38-43.*

SIDOROVA EKATERINA Z.
East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation (Irkutsk, Russia)
USOV EVGENIJ G.
Baikal Institute of BRICS IRNTU (Irkutsk, Russia)

THE MAIN MEASURES TO PREVENT DIGITAL CRIME

Annotation. The article presents a general description of the main measures to prevent digital crime. According to the authors, digital (cyber) crimes should include all types of criminally punishable acts committed using modern digital technologies. And since digital technologies are widely used in everyday life, the risk of becoming a victim of a digital crime increases significantly. That is why, in the modern period of society's development, it is very important to pay attention to the prevention of digital crime. The authors emphasize that the prevention of digital crimes is based on the regulatory regulation of relations in the field of digital technologies. Relying on the current legislation, the subjects of prevention ensure the prevention of cybercrime. In the fight against digital crimes, the institute of information and analytical support is of great importance, which is not limited only to the use of mass media and the Internet. Information and analytical support also involves the use of various information databases, various software aimed at timely receipt of operationally relevant information necessary for the successful prevention and suppression of digital crimes committed. The prevention of digital crime is impossible without carrying out various operational investigative measures carried out by employees of operational units. Engaged in the suppression and disclosure of cybercrime, employees of these units implement the law enforcement function of the state. At the same time, the operational units of the internal affairs bodies have at their disposal both public (open) and secret methods of conducting operational search activities. At the end of the study, the authors emphasize that the suppression and disclosure of digital crimes is multifaceted. Only an integrated, comprehensive approach to the prevention of digital crime can bring effective results and reduce the indicators of this type of crime.

Key words and word combinations: digital crime, cybercrime, prevention, criminological prevention, prevention, internal affairs bodies.

For citation: *Sidorova E.Z., Usov E.G. The main measures to prevent digital crime // Vestnik Advanced Training Institute of MIA of Russia. – 2024. – № 2 (70). – P. 38-43; doi: 10.29039/2312-7937-2024-2-38-43.*

Как известно, все составы преступлений предусмотрены в Уголовном кодексе Российской Федерации. Иных нормативных правовых актов, обеспечивающих уголовно-правовую охрану общественных отношений, нет. Романо-германская правовая система, на которой строится современная российская правовая база, позволяет сформировать уголовный закон, группируя все составы преступлений в зависимости от охраняемого блага (объекта). Соответственно, Особенная часть Уголовного кодекса России состоит из разделов, глав и статей. Однако, несмотря на то, что преступления, совершаемые с использованием информационных (цифровых) технологий, занимают значительное место в структуре современной преступности, самостоятельного раздела или главы, посвященного данным видам преступлений, в действующем уголовном законе нет. Исключением является только гл. 28 «Преступления в сфере компьютерной информации», однако преступления данной главы составляют только небольшую часть всей цифровой преступности.

По нашему мнению, к цифровым (кибер) преступлениям следует относить все виды уголовно наказуемых деяний, совершаемых с использованием современных цифровых технологий. А поскольку цифровые технологии широко используются в повседневной жизни, риск стать жертвой цифрового преступления значительно увеличивается. Именно поэтому в современный период развития общества очень важно уделять внимание вопросам профилактики цифровой преступности. И прежде, чем раскрыть ключевые меры предупреждения цифровой преступности, отметим, что в научной литературе выделяются различные основания классификации данных мер [13, с. 257].

В частности, если брать за основу такой критерий, как характер реализуемых мер, можно выделить:

1) процессуальные меры и внепроцессуальные меры;

2) запрещающие меры, ограничивающие меры, обязывающие меры.

Взяв за основу критерий масштабности мер, можно выделить:

1) общегосударственные меры;

2) региональные меры;

3) местные меры, реализуемые на уровне муниципального образования;

4) локальные меры, осуществляемые конкретной организацией или иным лицом.

В основе предупреждения цифровых преступлений лежит нормативное регулирование отношений в сфере цифровых технологий. Следует обозначить предписания таких нормативных правовых актов, как: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2], Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 [6], Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [7] и др. При этом важное практическое значение имеет организация контроля за исполнением положений названных нормативных правовых актов, поскольку ключевое значение имеет не только закрепление какого-либо правила в том или ином правовом акте, но и установление механизма его реализации, в том числе путем определения механизма контроля за его исполнением. Контроль осуществляют субъекты, которые наделены соответствующими полномочиями и являются ответственными за исполнение данного полномочия.

В основе современного механизма предупреждения цифровых преступлений лежит также институт информационно-аналитического обеспечения такого предупреждения, правовая основа которого закреплена в ст. 31 Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» [4]. Согласно данной статье, в целях информационного обеспечения профилактики правонарушений субъекты профилактики могут использовать в своей деятельности информационные ресурсы СМИ, сети Интернет и т.д., размещая в цифровом пространстве необходимую информацию.

Однако институт информационно-аналитического обеспечения предупреждения цифровой преступности не ограничивается только использованием СМИ и сети Интернет. Информационно-аналитическое обеспечение предполагает также использование различных информационных банков данных, различного программного обеспечения, направленного на своевременное получение оперативно значимой информации, необходимой для успешного предупреждения и пресечения совершаемых цифровых преступлений. В этом и заключается первостепенная цель информационно-аналитического обеспечения предупреждения цифровых преступлений. При этом подчеркнем, что существуют различные базы данных, которые могут и не быть напрямую связаны с совершаемым цифровым преступлением, но могут помочь выявить лицо, совершающее данное преступление. Например, существуют такие банки данных, как Единый реестр нарушителей правил дорожного движения, Паспорт наркотического контроля, Федеральный реестр населения, База данных о паспортных данных граждан РФ, Ведомость недействительных паспортов, Банк данных о судимости лиц, банки данных о лицах, находящихся в розыске, и многое другое [1, с. 374].

Необходимыми элементами аналитической работы являются прогнозирование и планирование борьбы с преступностью. Несомненно, использование современного

информационно-аналитического обеспечения необходимо и объективно обусловлено в целях пресечения совершаемого или совершенного цифрового преступления. Однако долгосрочное предупреждение ориентировано на то, чтобы подобные преступления не совершались вовсе. А для этого важно осуществлять соответствующее криминологическое прогнозирование.

Криминологическое прогнозирование – это предсказание будущего состояния преступности и связанных с ней явлений, а также выявление основных тенденций их развития [11, с. 156].

Объектом криминологического прогнозирования выступают преступность, личность преступника, детерминанты преступности, ее последствия и меры борьбы с преступностью.

Подчеркнем, что в эпоху цифровизации общества возможности для составления наиболее точного криминологического прогноза обширны. В частности, одним из методов составления криминологического прогноза является метод математического моделирования, основу которого составляют различные данные, влияющие на показатели преступности. Благодаря специальной компьютерной программе такие факторы сводятся воедино, и выстраивается примерный прогноз преступности. Однако криминологический прогноз всегда носит вероятностный характер и не всегда сбывается в полном объеме.

Помимо вышесказанного важно также отметить, что в основе борьбы с цифровыми преступлениями должна лежать комплексная программа противодействия цифровой преступности. В настоящее время на территории нашей страны действует государственная программа по противодействию преступности [5]. Однако данная программа не учитывает особенности современной цифровой преступности, в связи с чем, на наш взгляд, требует пересмотра и доработки.

Пресечение и раскрытие киберпреступлений обязано идти в ногу со временем, и порой старые способы и средства проведения превентивных мероприятий носят лишь вспомогательный характер. В научной литературе справедливо отмечается, насколько важно осуществлять профилактику и предупреждение всех видов преступности [10, с. 107]. И цифровая сфера общественных отношений не является исключением. Эффективная борьба с киберпреступностью невозможна без применения новых технологий, способов и средств осуществления профилактики.

Ученые-специалисты А.И. Розенцвайг и В.С. Чертилин подчеркивают, что предупреждение цифровых преступлений невозможно без проведения различных оперативно-розыскных мероприятий [9, с. 131]. Подразделения уголовного розыска и бюро специальных технических мероприятий (далее по тексту – БСТМ) вправе осуществлять оперативно-розыскную деятельность в полном объеме, предусмотренную Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [3]. В этой связи сотрудники данных подразделений, занимаясь пресечением и раскрытием киберпреступлений, реализуют правоохранительную функцию государства.

В практической деятельности оперативных подразделений для пресечения и раскрытия преступлений рассматриваемой категорий наиболее применимы оперативно-технический, агентурный и следственный (уголовно-процессуальный) методы, а также отдельные оперативно-розыскные мероприятия, применяемые по мере необходимости и в зависимости от имеющейся оперативно значимой информации. Рассмотрим их более подробно.

Оперативно-технический метод. Суть данного метода заключается в применении оперативными сотрудниками в негласной форме различных оперативно-розыскных мероприятий. Данный метод также включает в себя применение мониторинга и охватывает также неиндексируемый сегмент в поисковых системах (например, Darknet, Dark Web, Deepnet, Deep Web), что применяется для более оперативного обнаружения и реагирования на соответствующие цифровые угрозы.

В соответствии с ч. 1 ст. 14 Федерального закона «Об оперативно-розыскной деятельности» при решении задач, связанных с пресечением и раскрытием преступлений рассматриваемой категории, у сотрудников оперативных подразделений посредством проведения ОРМ возникает обязанность защищать законные интересы пострадавших от преступлений, совершен-

ных с использованием информационно-телекоммуникационных технологий (далее по тексту – ИТТ) [3].

Специфика пресечения и раскрытия киберпреступлений связана с реальным ограничением прав широкого круга лиц на тайну переписки, телефонных переговоров и иных сообщений, передаваемых по сетям электрической связи, а также ограничением их права на банковскую тайну. Как правило, к таким лицам относятся: владельцы различных гаджетов; владельцы интернет-кафе; номинальные директора коммерческих организаций; обладатели сим-карт; лица, обналичивающие денежные средства; и т.п.

Важно отметить, что ограничение конституционных гарантий граждан допустимо на основании судебного решения.

Агентурный метод. Данный метод также актуален в современных условиях для пресечения и раскрытия киберпреступлений, так как, несмотря на дистанционный характер, их все-таки совершают люди, которые имеют определенные социальные связи и круг общения. Однако данные люди ведут, как правило, закрытый, конспиративный образ жизни и имеют высокий уровень анонимности за счет использования технологий шифрования.

Сотрудниками оперативных подразделений продолжают использоваться наиболее доступные и отработанные годами оперативно-розыскные мероприятия, такие как: наблюдение, опрос, оперативное внедрение в среду специалистов в сфере ИТТ. Они изучают культуру хакеров, работают с лицами, осужденными за компьютерные преступления, с их кругом общения.

Следует отметить, что одним из источников информации, получаемой оперативным путем, является наблюдение за IT-специалистами, попавшими в поле зрения правоохранительных органов, а также сотрудничество с ними на конфиденциальной основе. Одним из видов оперативно-розыскных мероприятий (далее по тексту – ОРМ) является наблюдение за местами сетевого общения хакерского сообщества, где осуществляется обмен криминальным опытом, а также информацией о жертвах и способах совершения общественно опасных деяний. Наблюдение и опрос осуществляются самими сотрудниками полиции посредством работы с конфидентами, которые имеют отношение к рассматриваемой преступной среде [12, с. 132].

В случае получения реальной информации о готовящемся либо совершённом преступлении подключается техническая составляющая оперативно-розыскной деятельности и проводятся иные необходимые оперативно-розыскные мероприятия.

При раскрытии преступлений, связанных с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), созданием, использованием и распространением вредоносных компьютерных программ (ст. 273 УК РФ), работа по раскрытию сконцентрирована на сотрудниках организации, где было совершено преступление. В первую очередь отрабатываются связи сотрудника (вид служебной деятельности, близкие, знакомые, семья, хобби, увлечения, уровень доступа к компьютерной информации, а также уровень пользования и владения компьютерными программами).

В процессе раскрытия преступления тщательно проверяется вся информация, ставшая известная сотрудникам уголовного розыска от работников организации на месте. Устанавливаются прямые, промежуточные, случайные и закономерные связи и контакты между сотрудниками юридического лица [8, с. 43].

Организационные основы раскрытия преступлений, совершенных с помощью информационных технологий, строятся, в том числе, на организации взаимодействия между смежными структурами, а также операторами, связи, интернет-провайдерами, кредитно-финансовыми организациями.

Успешное раскрытие киберпреступлений возможно исключительно при осуществлении оперативно-розыскной деятельности и должной ее организации. К субъектам организации данной деятельности относятся: руководители органов внутренних дел на региональном уровне, начальники оперативных подразделений, иные должностные лица. В процессе ее осуществления применяется целый комплекс специальных организационно-управленческих и организационно-тактических мер, который предметно регламентирован и направлен на решение задач по раскрытию преступлений.

Подводя итоги, следует отметить, что пресечение и раскрытие цифровых преступлений носит многоплановый характер.

При этом важное значение имеют возможности органов профилактики и предупреждения. На наш взгляд, противодействие цифровой преступности должно строиться на решении таких задач, как уголовно-правовая характеристика преступлений, совершенных с использованием информационных (цифровых) технологий; определение особенностей квалификации преступлений, совершенных с использованием информационных (цифровых) технологий; анализ уголовной политики в сфере обеспечения цифровой безопасности; криминологический анализ преступности в сфере информационных (цифровых) технологий; выявление особенностей личности преступника, совершающего преступления с использованием информационных (цифровых) технологий, и его жертвы; исследование основ предупреждения преступлений, совершенных с использованием информационных (цифровых) технологий; анализ международного опыта сотрудничества государств по предупреждению преступлений, совершаемых с использованием информационных (цифровых) технологий.

Только комплексный, всесторонний подход к профилактике цифровой преступности способен принести эффективные результаты и снижение показателей данного вида преступности.

1. Мачтаков С.Г., Питолин М.В., Мальцев С.А. Использование возможностей специализированных банков данных МВД России в раскрытии и расследовании преступлений // Пожарная безопасность: проблемы и перспективы. 2015. № 1 (6).
2. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2006. № 31 (Ч. I). Ст. 3448.
3. Об оперативно-розыскной деятельности: федеральный закон от 12 августа 1995 г. № 144-ФЗ // СЗ РФ. 1995. № 33. Ст. 3349.
4. Об основах системы профилактики правонарушений в Российской Федерации: федеральный закон от 23 июня 2016 г. № 182-ФЗ // СЗ РФ. 2016. № 26 (Ч. I). Ст. 3851.
5. Об утверждении государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности»: постановление Правительства РФ от 15 апреля 2014 г. № 345 // СЗ РФ. 2014. № 18 (Ч. IV). Ст. 2188.
6. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.
7. О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 октября 2019 г. № 490 // СЗ РФ. 2019. № 41. Ст. 5700.
8. Осипенко А.Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации // Общество и право. 2018. № 3 (65).
9. Розенцвайг А.И., Чертилин В.С. Формы противодействия киберпреступности // Вестник экономики, права и социологии. 2019. № 4.
10. Сидорова Е.З., Литвинцева Е.А. Профилактика безнадзорности, правонарушений и преступности среди несовершеннолетних в Иркутской области // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2023. № 1 (65).
11. Сидорова Е.З. Примерный прогноз развития криминальной ситуации на объектах транспортной инфраструктуры Восточно-Сибирской железной дороги // Социально-экономический и гуманитарный журнал. 2022. № 3 (25).
12. Харина Э.Н. О возможностях использования сети Интернет при расследовании преступлений // Современное состояние и перспективы развития научной мысли: материалы междунар. науч.-практ. конф. (г. Уфа, 25 мая 2015 г.). Ч. 2.
13. Чепрасова Ю.В., Шмарион П.В. Основные направления противодействия киберпреступности // Вестник Воронежского института МВД России. 2020. № 3.

Информация об авторах:

Е.З. Сидорова, *заместитель начальника кафедры уголовного права и криминологии, кандидат юридических наук*
Е.Г. Усов, *доцент, кандидат юридических наук*

About the authors:

E.Z. Sidorova*, Deputy Head of the Department of Criminal Law and Criminology, PhD in Law*
E.G. Usov, *associate professor, candidate of law*

Статья поступила в редакцию 30.10.2023