Научная статья
УДК 343.985.7
DOI: 10.55001/2587-9820.2023.90.21.022

КЛАССИФИКАЦИЯ СПОСОБОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Альфия Радиковна Сысенко[1], Александр Сергеевич Горденко[2]
[1,2]Омская академия МВД России, г. Омск, Российская Федерация
[1]sysenko_75@mail.ru
[2]alekgordenko@yandex.ru

Аннотация. В статье рассматриваются особенности классификации способов совершения преступлений с использованием информационно-телекоммуникационных технологий.

В ходе исследования делается вывод о том, что классификация способов совершения преступлений в сети Интернет не носит и не может носить исчерпывающего характера в силу многообразия таких способов, а также постоянного развития сферы информационно-телекоммуникационных технологий. В качестве примеров приводятся наиболее актуальные случаи, с которыми в настоящее время сталкиваются практические работники при расследовании преступлений указанной категории.

Ключевые слова: классификация, способы, неправомерный доступ, сетевые преступления, распространение вредоносных программ.

Для цитирования: Сысенко, А. Р., Горденко, А. С. Классификация способов совершения преступлений с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2023. Т. 26. № 2. С. 229–236. DOI: 10.55001/2587-9820.2023.90.21.022

CLASSIFICATION OF METHODS OF COMMITTING CRIMES USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Alfiya R. Sysenko[1], Alexander S. Gordenko[2]
[1,2]Omsk Academy of the MIA of Russia, Omsk, Russian Federation
[1]sysenko_75@mail.ru
[2]alekgordenko@yandex.ru

Abstract. The article discusses the features of the classification of methods of committing crimes using information and telecommunication technologies.

The study concludes that the classification of methods of committing crimes on the Internet is not and cannot be exhaustive due to the variety of such methods, as well as the constant development of the field of information and telecommunication technologies. As examples, the most relevant cases that practitioners currently face when investigating crimes of this category are given.

Keywords: classification, methods, unauthorized access, network crimes, malware distribution.

For citation: Sysenko, A. R., Gordenko, A. S. Klassifikacija sposobov sovershenija prestuplenij s ispol'zovaniem informacionno-telekommunikacionnyh tehnologij [Classification of methods of committing crimes using information and telecommunication technologies]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2023, vol. 26 no. 2, pp. 229–236 (in Russ.). DOI: 10.55001/2587-9820.2023.90.21.022

Введение

Вопрос о противодействии преступлениям, совершаемым в сети Интернет, стоит особенно остро: по данным статистической отчетности ГИЦ МВД России за период с 2018 по 2022 года в России число преступлений, связанных с неправомерным доступом и использованием компьютерной информации, с каждым годом существенно и неуклонно увеличивается[1]. Кроме того, проблему актуализирует также то, что официальная статистика не учитывает высокую латентность данной категории преступлений, а также тот факт, что сегодня с использованием глобальной сети Интернет может быть совершено практически любое преступление, а не только те, которые поименованы в действующем уголовном законодательстве в качестве преступлений в сфере компьютерной информации [1, с. 171].

Для противодействия преступлениям в глобальной компьютерной сети необходима мобилизация сил и средств как на государственном, так и на международном уровнях. В большинстве стран развернуты государственные программы по противодействию данной угрозе, направленные на повышение эффективности деятельности правоохранительных органов, совершенствование законодательной базы и использование профилактических мероприятий. Тем не менее, несмотря на предпринимаемые значительные усилия, рост рассматриваемого вида преступности свидетельствует о недостаточной эффективности этих мер на данном этапе.

Основная часть

Проблемным вопросом применительно к расследованию преступлений в сети Интернет является разграничение способов и средств совершения преступления. Применительно к обычным (несетевым) преступлениям под способом совершения преступления понимают приемы и методы, которые использует преступник при совершении деяния, а под средством совершения преступления – предметы материального мира, которые используются преступником для облегчения совершения деяния [2, с. 118].

Любая (в том числе криминальная) деятельность в сети Интернет носит опосредованный характер: прежде всего, само подключение к сети Интернет требует наличия специального оборудования. Следовательно, любое преступление в сети Интернет связано с использованием как минимум электронно-вычислительной техники.

Совершая различные действия с такой техникой, подключенной к сети Интернет, и (или) программным обеспечением, установленным на такой технике, преступник осуществляет криминальную деятельность. Таким образом, криминальная деятельность в сети Интернет всегда связана с воздействием на электронно-вычислительную технику и (или) соответствующее программное обеспечение, в силу чего имеются основания для того, чтобы такую технику и программные средства относить к средствам совершения преступления, а ту

[1] Статистика и аналитика // МВД России : сайт. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 12.01.2023). Режим доступа: свободный.

совокупность действий, которую преступник осуществляет для использования данных средств, считать способами совершения преступления в сети Интернет. Тем не менее применительно к преступлениям в сети Интернет невозможно провести столь четкое разделение средств и способов совершения преступления, поскольку, как отмечалось выше, достижение каких-либо запланированных результатов деятельности в сети Интернет всегда возможно только в случае наличия определенной интернет-технологии, которая определяет совокупность приемов и способов, пригодных для достижения определенной цели в телекоммуникационной сети. Например, если преступник пытается замаскировать следы совершенного им преступления в сети Интернет, в частности путем сокрытия своего IP-адреса с помощью VPN-сервера, то все совершаемые им для этой цели действия (подключение к сети по протоколу Point-to-Point Tunneling Protocol, использование специальной программы – «клиента» для подключения к частной виртуальной сети и т. д.), а также аппаратура, которая используется для этого, предопределяют специфику способа сокрытия сетевого преступления [3, с. 115]. В случае, если следователь не знаком с технологиями, обеспечивающими функционирование «анонимайзеров» (программ, обеспечивающих сокрытие реального IP-адреса за счет выстраивания длинной цепочки виртуальных адресов), для него будет затруднительно определить обстоятельства, имеющие значение для дела.

Следует согласиться с мнением Л. П. Зверянской, которая обоснованно указывает, что при совершении сетевых преступлений Интернет одновременно является и средой криминальной деятельности, и способом, и средством совершения преступления [4, с. 131].

Таким образом, способ совершения преступления в сети Интернет можно определить как совокупность приемов и методов, с помощью которых преступник осуществляет подключение к сети Интернет, а также совершает или обеспечивает совершение действий по передаче, размещению, использованию информации в сети Интернет. Специфической чертой способа совершения преступления в сети Интернет является то, что такая совокупность приемов и методов придает сетевому преступлению уникальные свойства, не свойственные преступлениям, совершаемым без использования глобальной сети.

Характеристика способов совершения любых преступлений, включая сетевые, обычно производится путем классификации таких способов.

Научный процесс классификации включает прежде всего определение классификационного критерия и разделение всего логического массива по данному критерию на группы таким образом, чтобы совокупность всех разделенных групп по своему логическому объему точно соответствовала исходному массиву. Поэтому в рамках настоящего исследования необходимо отметить, что приведенные далее классификации способов совершения преступлений в сети Интернет не во всех случаях обеспечивают соблюдение данного принципа. Более того, в силу фактического многообразия и постоянной модификации способов совершения преступлений указанной категории приведенные далее классификационные критерии также не являются исчерпывающими.

С целью выявления основных способов совершения все сетевые преступления могут быть разделены на две группы по степени подготовленности.

Для преступлений первой группы умысел возникает внезапно, под влиянием провоцирующей ситуации (например, незащищенности объекта посягательства). Практически все подобные случаи связаны с неправомерным использованием ресурсов

Интернета, например, в результате завладения чужим паролем доступа [5, с. 123].

Вторая группа преступлений характеризуется наличием обдуманного плана, включающего изучение объекта посягательства, подготовку к совершению противоправных действий.

В зависимости от субъектов совершения противоправных действий с помощью сети Интернет все сетевые преступления можно разделить на две группы: совершаемые лицами, имеющими специальные знания в сфере компьютерных наук, техники и информационных технологий, и совершаемые лицами, таких знаний не имеющими.

Так, использование сети Интернет для совершения клеветы не требует, как правило, глубоких технических знаний – для того чтобы разместить на интернет-ресурсе информацию, не соответствующую действительности, достаточно навыков и умений на уровне массового пользователя.

Аналогичным образом могут быть совершены и иные преступления. Например, доведение до самоубийства посредством использования сети Интернет может быть совершено путем систематического размещения комментариев, носящих заведомо нелицеприятный и травмирующий характер, на странице жертвы в социальной сети.

Размещение иной нелегальной информации (способов изготовления наркотических средств или объявлений о продаже таких средств, размещения информации экстремистского характера и проч.) также, как правило, не требует наличия технических знаний. С другой стороны, такие способы совершения интернет-преступлений, как распространение вредоносных программ, хакинг (взлом Интернет-сайтов, электронной почты и иных электронных хранилищ информации), фишинг (хищение реквизитов банковских карт, электронного кошелька, онлайн-банка путем создания страниц для ввода такой информации, которые по своему внешнему виду имитируют реально существующие легальные страницы), нюкинг (действия по нарушению работоспособности электронных устройств, сайтов, сетей, серверов, реализуемые в виде DOS- и DDOS-атак), безусловно, требует высокой квалификации, глубоких знаний и практических навыков по использованию современных интернет-технологий.

Таким образом, в качестве классификационного критерия можно использовать сложность интернет-технологии, используемой для совершения преступления, и все способы совершения сетевых преступлений разделить на две группы:

– простые, предполагающие использование интернет-технологий массового характера, не требующих применения специальных знаний и доступных любому пользователю сети Интернет;

– сложные, предполагающие наличие у преступников глубоких знаний в сфере информационных технологий и техники.

Особенностью сетевых преступлений является то, что для их совершения могут использоваться не только незаконные с криминалистической точки зрения средства, но и законные. Например, размещение объявления о продаже не запрещенного в обороте товара в социальной сети само по себе не является полностью противоправным действием, однако отсутствие у лица, разместившего такое объявления, реального намерения осуществить передачу оплаченного товара покупателю делает его способом совершения сетевого преступления.

Также специфической чертой сетевых преступлений является широкое использование для их совершения программно-аппаратных и программных средств на фоне сравнительно редкого использования

исключительно аппаратных средств. При этом используемые в криминальной деятельности средства в зависимости от технологии создания таких средств могут подразделяться на готовые, модифицированные и средства собственной разработки [6, с. 164].

Обобщая все указанные подходы, классификационную схему способов совершения преступлений в сети Интернет можно представить следующим образом:

1. По характеру преступных действий в сети Интернет:

1.1. Сетевое мошенничество – имитация преступниками легальной деятельности без намерения ее осуществлять:

– интернет-попрошайничество (публикация призывов о благотворительной помощи с указанием реквизитов для перечисления денежных средств, которые в действительности не являются реквизитами благотворительных организаций);

– мошенничество в сфере интернет-торговли (публикация заведомо ложных сообщений о реализации товара без реального намерения такой товар продать; размещение в сети Интернет сайта, имитирующего интернет-магазин);

– фишинг (хищение конфиденциальной информации пользователей путем введения их в заблуждение относительно ресурсов, на которых преступники побуждают вводить такую информацию). Одним из видов данного способа, набирающим популярность, является создание поддельных (фейковых) интернет-страниц банковских организаций, при переходе на которую пользователь, ошибочно приняв такую страницу за реальную, оставляет в виде cookie-файлов свои логин и пароль от личного кабинета.

1.2. Распространение вредоносных программ:

– размещение кликбэйтных объявлений (при просмотре жертвой сайта какой-либо информации в сети Интернет поверх обозреваемой страницы всплывает информация с предложением перейти по ссылке, при совершении же такого перехода пользователь подвергает собственный компьютер заражению вредоносным программным обеспечением);

– создание инфицированных интернет-страниц, при переходе на которую пользователь, ошибочно приняв такую страницу за реальную, инфицирует компьютер.

1.3. Распространение противоправной информации:

– распространение информации о способах изготовления либо о продаже предметов, запрещенных в обороте;

– распространение инструкций по осуществлению неправомерного доступа к компьютерной информации, а также по созданию вредоносного программного обеспечения;

– распространение информации экстремистского характера;

– интернет-издевательство (распространение угроз или информации, заведомо оскорбительной или унижающей честь и достоинство жертвы);

– распространение материалов порнографического характера;

– распространение информации с нарушением авторских прав или средств для преодоления средств защиты авторских прав.

1.4. Удаленное вмешательство в работу электронных устройств:

– нюкинг;

– хакинг.

2. По стадии совершения сетевого преступления:

2.1. Способы по подготовке сетевого преступления:

– удаленный доступ к устройствам потерпевшего, позволяющий провести анализ уязвимостей;

– установка специальных программ-шпионов, анализирующих защищенность устройств жертвы внешним угрозам;

– установление контакта с жертвой преступления путем

использования социальных сетей, электронной переписки и проч.

– получение и анализ персональных данных и иной личной информации о потенциальной жертве с помощью слитых информационных баз данных (крупных ритейлеров и государственных сервисов).

2.2. Способы по непосредственному совершению преступного деяния;

2.3. Способы сокрытия преступного деяния в сети Интернет и противодействия следствию:

– использование специальных программ, удаляющих из памяти устройств любые электронные следы по совершению действий в сети Интернет;

– сокрытие реального IP-адреса путем подключения к частным виртуальным сетям по VPN-технологии;

– использование чужих идентификационных данных при подключении к сети.

3. По сложности используемых в криминальной деятельности технологий:

3.1. Простые – с использованием широко распространенных интернет-технологий, применение которых не требует специальных знаний и навыков.

3.2. Сложные – с использованием сложных технологий, применение которых требует специальных познаний и опыта.

4. По объекту сетевого преступления:

4.1. Способы совершения сетевых преступлений, направленные на противоправное использование информации (хищение, незаконное обнародование, несанкционированное удаление и т. д.).

4.2. Способы совершения сетевых преступлений, направленные на противоправное удаленное вмешательство в оборудование и элементы сетевой инфраструктуры.

4.3. Способы совершения сетевых преступлений, направленные на противоправное использование программного обеспечения.

4.4. Способы совершения сетевых преступлений, направленные непосредственно на пользователя сети (интернет-издевательства, угрозы, шантаж).

5. По техническому содержанию:

5.1. Аппаратные способы совершения сетевых преступлений.

5.2. Программно-аппаратные способы совершения сетевых преступлений.

5.3. Программно-логические способы совершения сетевых преступлений.

6. По технологии создания средств совершения преступления:

6.1. Использование в криминальной деятельности готового оборудования и/или программного обеспечения.

6.2. Использование модифицированного преступником оборудования и/или программного обеспечения.

6.3. Использование специально созданного для достижения планируемого результата преступной деятельности оборудования и/или программного обеспечения.

7. По законности использования сети Интернет в криминальной деятельности:

7.1. Законные способы (установление брачным аферистом контакта с жертвой путем общения в социальных сетях с целью вызвать доверие).

7.2. Противозаконные способы.

Приведенная классификация способов совершения преступлений в сети Интернет не носит и не может носить исчерпывающего характера в силу многообразия таких способов, а также постоянного развития сферы информационно-телекоммуникационных технологий [7, с. 183].

Выводы и заключение

Таким образом, сетевые преступления в общем виде характеризуются системообразующим фактором, в котором сеть Интернет выступает одновременно важнейшим элементом

взаимодействия и отражения механизмов подготовки, совершения и сокрытия этих преступных деяний, в качестве среды криминальной деятельности, а также как способ совершения преступления.

Способы совершения преступлений в сети Интернет можно классифицировать по таким критериям, как: характер преступных действий, стадия совершения сетевого преступления; сложность используемой интернет-технологии; объект преступления; технология создания средств совершения преступления; техническое содержание; законность использования сети Интернет в криминальной деятельности.

Отличие способов совершения преступлений в сети Интернет от способов совершения «традиционных» преступлений состоит в следующем:

1) преступное воздействие на объект посягательства всегда носит удаленный характер и обезличено: личность потерпевшего, как правило, не имеет для преступника значения, а потерпевший лишен возможности идентифицировать преступника;

2) криминальная деятельность в сети Интернет осуществляется в виде электронных кодов и сигналов, передаваемых по информационно-телекоммуникационной сети;

3) виртуальные следы преступной деятельности в сети Интернет фиксируются на множестве объектов (устройства преступника и жертвы, устройства провайдера, сервера, оператора связи, промежуточные сетевые узлы) и могут состоять из большого количества отдельных информационных элементов, которые записываются как на одном, так и на нескольких физических носителях цифровой информации, подключенных к одному или нескольким компьютерам, объединенным в информационно-телекоммуникационную сеть.

СПИСОК ИСТОЧНИКОВ

1. *Бессонов, А. А.* Способ преступления как элемент его криминалистической характеристики // Пробелы в российском законодательстве : юрид. науч. журн. Москва : «Юр-ВАК». 2014. № 4. С. 171–173.

2. *Ишин, А. М.* Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта : науч. журн. Калининград : Балтийский федеральный университет им. И. Канта. 2013. № 9. С. 116–123.

3. *Щербаков, А. Ю.* Введение в теорию и практику компьютерной безопасности : пособие для специалистов. М. : изд. Молгачева С. В., 2001. 351 с.

4. *Зверянская, Л. П.* Современные проблемы исследования криминалистических особенностей киберпреступлений // Приоритетные научные направления: от теории к практике : науч. журн. Новосибирск : ООО «Центр развития научного сотрудничества». 2015. № 15. С. 127–132.

5. *Осипенко, А. Л.* Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал : науч. журн. Екатеринбург : Уральская гос. юрид. академия. 2010. № 2(71). С. 121–126.

6. *Поляков, В. В., Лапин, С. А.* Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники : науч. журн. Томск : Томский гос. ун-т систем управления и радиоэлектроники. 2014. № 2(32). С. 162–166.

7. *Сысенко, А. Р., Белова, К. С., Горденко, А. С.* Особенности расследования неправомерного доступа к компьютерной информации (ст. 272 УК РФ) //

Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2022. № 4(24). С. 183–188.

REFERENCES

1. *Bessonov, A. A.* Sposob prestuplenija kak jelement ego kriminal-isticheskoj harakteristiki [The method of crime as an element of its criminal-istic characteristics]. Probely v rossijskom zakonodatel'stve – Gaps in Rus-sian legislation. Moscow, 2014, no. 4, pp. 171-173.

2. *Ishin, A. M.* Sovremennye problemy ispol'zovanija seti Internet v rassledovanii prestuplenij [Modern problems of using the Internet in the in-vestigation of crimes]. Vestnik Baltijskogo federal'nogo universiteta im. I. Kanta – Vestnik of the Baltic Federal University named after I. Kant. Kali-ningrad. 2013, no. 9, pp. 116-123.

3. *Shcherbakov, A. Yu.* Vvedenie v teoriju i praktiku komp'juternoj bezopasnosti [Introduction to the theory and practice of computer security]. Moscow, 2001, 351 p.

4. *Zveryanskaya, L. P.* Sovremennye problemy issledovanija kriminal-isticheskih osobennostej kiberprestuplenij [Modern problems of research of criminalistic features of cybercrimes]. Prioritetnye nauchnye napravlenija: ot teorii k praktike – Priority scientific directions: from theory to practice. No-vosibirsk, 2015, no. 15, pp. 127-132.

5. *Osipenko, A. L.* Osobennosti rassledovanija setevyh komp'juternyh prestuplenij [Features of investigation of network computer crimes]. Ros-sijskij juridicheskij zhurnal – Russian Legal journal. Yekaterinburg. 2010, no. 2(71), pp. 121-126.

6. *Polyakov, V. V., Lapin, S. A.* Sredstva sovershenija komp'juternyh prestuplenij [Means of committing computer crimes]. Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki – Re-ports of Tomsk State University of Control Systems and Radioelectronics. Tomsk, 2014, no. 2(32), pp. 162-166.

7. *Sysenko, A. R., Belova K. S., Gordenko A. S.* Osobennosti rassledo-vanija nepravomernogo dostupa k komp'juternoj informacii (st. 272 UK RF) [Features of the investigation of unlawful access to computer information (Article 272 of the Criminal Code of the Russian Federation)]. Kriminalisti-ka: vchera, segodnja, zavtra – Criminalistics: yesterday, today, tomorrow. Irkutsk, 2022, no. 4(24), pp.183-188. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Сысенко Альфия Радиковна, кандидат юридических наук, доцент, доцент кафедры криминалистики. Омская академия МВД России. 644092, Российская Федерация, г. Омск, проспект Комарова, 7.

Горденко Александр Сергеевич, преподаватель кафедры криминалистики. Омская академия МВД России. 644092, Российская Федерация, г. Омск, проспект Комарова, 7.

INFORMATION ABOUT THE AUTHORS

Alfiya R. Sysenko, Candidate of Law, Associate Professor, Associate Professor of the Department of Criminalistics. Omsk Academy of the MIA of Russia, 7, Komarova Avenue, Omsk, Russia Federation, 7644092.

Alexander S. Gordienko, lecturer of the Department of Criminalistics. Omsk Academy of the Ministry of Internal Affairs of Russia, Omsk Academy of the MIA of Russia, 7, Komarova Avenue, Omsk, Russia Federation, 7644092.