ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004

НЕКОТОРЫЕ АСПЕКТЫ ИССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Файсханов Ирек Фоатович
АО «Уралтрансмаш», Екатеринбург
Отдел информационной безопасности, начальник отдела
f_irek@mail.ru

Гизатуллин Марат Галимянович
Уральский юридический институт МВД России, Екатеринбург
Кафедра информационного обеспечения органов внутренних дел, начальник кафедры
доцент, к.т.н.
ieee-ural-uisi@yandex.ru

Рубцов Денис Сергеевич
Уральский юридический институт МВД России, Екатеринбург
Факультет подготовки сотрудников полиции, слушатель 5 курса

Столбова Дарья Петровна
Уральский юридический институт МВД России, Екатеринбург
Факультет подготовки сотрудников полиции, слушатель 5 курса

Аннотация

За последние двадцать лет в Российской Федерации наблюдается масштабная информатизация общества, которая внесла серьезные коррективы в жизнь общества, личности, государства. Рассматривая современный период необходимо отметить, что в Российской Федерации отмечается высокий рост преступлений, совершаемых с использованием средств информационно-коммуникационных технологий. С учетом этого обстоятельства, авторами уделяется особое внимание анализу преступлений в информационном пространстве – актуальной и значимой области для исследований.

Ключевые слова: кибер-преступность, компьютерные преступления, сеть Интернет, информационно-коммуникационные технологии, вычислительная техника, информация, правоохранительная деятельность.

SOME ASPECTS OF THE STUDY OF CRIMES COMMITTED USING INFORMATION TECHNOLOGY

Irek F. Faiskhanov
Uraltransmash JSC, Yekaterinburg
Information Security Department, Head of Department
f_irek@mail.ru

Marat G. Gizatullin
Ural Law Institute of the Ministry of the Interior of Russia, Yekaterinburg
Department of Information Support of Internal Affairs Bodies, Head of Department
Associate Professor, Ph.D.
ieee-ural-uisi@yandex.ru

Denis S. Rubtsov
Ural Law Institute of the Ministry of the Interior of Russia, Yekaterinburg
Faculty of Police Training, 5th year student

Daria P. Stolbova
Ural Law Institute of the Ministry of the Interior of Russia, Yekaterinburg
Faculty of Police Training, 5th year student

ABSTRACT

Over the past twenty years, large-scale informatization of society has been observed in the Russian Federation, which has made serious adjustments to the life of society, individuals, and the State. Considering the current period, it should be noted that in the Russian Federation there is a high increase in crimes committed using information and communication technologies. Given this circumstance, the authors pay special attention to the analysis of crimes in the information space – a relevant and significant area for research.

Key words: cyber crime, computer crime, Internet, information and communication technologies, computer technology, information, law enforcement.

Введение

Вторая половина XX века была ознаменована новым направлением деятельности человечества – информационно-коммуникационными технологиями (далее – ИКТ). Колоссальная область для исследований и разработки, масштабное пространство для реализации самых сложных целей и задач, новая отрасль для инвестиций и перспективных дивидендов и многое другое привнесло масштабное развитие ИКТ. Появилась возможность расширить границы исследований науки, автоматизировать сложные технические процессы, оптимизировать технологии практически во всех отраслях деятельности человека. С одной стороны, данный шаг стал новой ступенью развития цивилизации, а с другой стороны – возникло множество отрицательных составляющих, начиная с экологических проблем, заканчивая составляющей правоохранительной деятельности, исследованиям которой посвящена данная работа. Если во второй половине XX века кибер-преступления только начинали процесс активизации, то с конца XX века и по настоящее

время они прочно заняли нишу преступлений, популярность которых в настоящее время только возрастает. Данному факту поспособствовало в немалой мере активное развитие международной сети Интернет [1]. Появление и популяризация использования «всемирной паутины» стала одним из ключевых событий конца XX века – начала XXI века. Интернет стал «модной» тенденцией, определенным укладом жизни.

Цель исследования

Цель исследования состоит в рассмотрении общих и частных вопросов анализа преступлений в Российской Федерации, совершаемых с использованием средств ИКТ.

Материалы и методы исследования

Исследования проводились на базе методов анализа и синтеза, а также сравнительного и проблемно-поискового методов. Информационной базой явился ряд научных публикаций, освещающих рассматриваемую проблематику, например, работы авторов [1, 2, 6-8].

Результаты

Анализируя использование сети Интернет в жизни общества, можно сделать вывод, что интеграция с человеком происходит огромными шагами: если в начале 2000-х гг. Интернет был, по сути своей, стационарным объектом, поскольку мобильное его использование было мало распространено, то в настоящее время доступ к «всемирной паутине» у человека может не прекращаться достаточно долгий промежуток времени. Соответственно, имеется множество положительных аспектов, например, таких как оперативный доступ к необходимой в данный момент информации, отсутствие проблем с коммуникацией, при условии, что лицо в зоне действия базовой станции, практически полное стирание границ между населенными пунктами не только одного государства, но и всего мира.

Анализ положительных составляющих, несомненно, может являться темой еще не одного исследования, однако возвращаясь к теме исследования, стоит отметить, что сеть Интернет дала шаг к развитию нового направления преступности – компьютерным преступлениям, которые в настоящее время являются актуальной проблемой и решение которых должно быть комплексным и всесторонним.

Преступления данной направленности в своем разнообразии многогранны: интернет-мошенничество, DDoS-атаки, создание вредоносного программного обеспечения, нарушение авторских прав и многое другое [2].

Также стоит отметить тот факт, что сети Интернет присущи такие свойства, как виртуальный характер, т.е. отсутствие физических свойств, анонимность, а также удаленность. Данные свойства дают некоторую мотивацию лицу, которое совершает преступление с использованием сети Интернет, поскольку имеется ложная уверенность в том, что правоохранительные органы не обнаружат данного преступника. В том числе и потому, что данное лицо, совершившее преступление может находиться в другом государстве и рассчитывать на то, что данный факт может, если не остановить «правоохранителей», то, как минимум, замедлить.

Однако, как показывает практика, подобные преступления раскрываются, даже вне зависимости от того, где и в каком месте подозреваемый совершал преступное деяние. Например, в октябре 2019 года стало известно об экстрадиции российского хакера, который подозревался в совершении кражи в особо крупном размере [3]. Также, достаточно ярким примером является ликвидация крупнейшей в России группировки, основным

направлением деятельности которой являлось хищение денежных средств с банковских счетов. Одной из важных особенностей является то, что члены данной группировки действовали из 17 регионов Российской Федерации [4].

Согласно ч. 1 ст. 14 УК РФ преступлением признается виновно совершенное общественно опасное деяние, запрещенное настоящим УК РФ под угрозой наказания [5].

Необходимо более детально разобрать данную выдержку из УК РФ.

Термин «деяние» представляет собой действие или бездействие лица, которое привело к общественно опасным последствиям по различным направлениям [5]: жизнь и здоровье личности; свобода, честь и достоинство личности; половая неприкосновенность и половая свобода личности; конституционные права и свободы человека и гражданина; семья и несовершеннолетние; собственность; сфера экономической деятельности; интересы службы в коммерческих и иных организациях; общественная безопасность; здоровье населения и общественная нравственность; экология; безопасность движения и эксплуатация транспорта; безопасность в сфере компьютерной информации; основы конституционного строя и безопасность государства; государственная власть, интересы государственной службы и службы в органах местного самоуправления; правосудие; порядок управления; военная служба; мир и безопасность человечества.

Таким образом, уголовное законодательство содержит широкий перечень видов преступлений, одними из них являются преступления в сфере ИКТ. Преступления данной направленности можно считать достаточно новым типом деяний, исследование которых привлекает внимание многих выдающихся специалистов [6-8].

Стоит отметить, что разнообразие механизмов преступных посягательств постоянно обновляется, преступники используют все более изощренные способы для реализации преступных замыслов. Однако, несмотря на это, большинство преступлений данной направленности остаются достаточно примитивными в плане своей реализации.

Рассмотрим пример из судебной практики. Согласно одному из дел, было установлено, что гражданин совершил умышленное преступление из корыстной заинтересованности, с целью продажи информации аутентификационной составляющей для доступа к сети Интернет при помощи компьютерных технологий. Он подобрал логин и пароль, тем самым совершил неправомерный доступ к охраняемой законом компьютерной информации, после чего поменял данные пользователя, что повлекло за собой блокировку компьютерной информации, содержащейся на данном сайте сети Интернет. Преступник был привлечен к ответственности по ч. 2 ст. 272 УК РФ. В Постановлении был сделан вывод о том, что преступление относится к категории преступлений средней тяжести.

Необходимо отметить, что такие действия как копирование информации, изменение информации, передача информации могут привести к уголовной ответственности и при совершении подобного вида преступлений данные лица не всегда понимают не только всю серьезность совершаемых деяний, но и то, что данные деяния находятся за рамками закона. Поэтому одна из задач для минимизации подобного рода преступлений – это доведение до граждан информации о том, что подобного рода действия являются незаконными и могут привести к возбуждению уголовного дела.

Продолжая анализ роста количества уголовных дел, связанных с ИКТ стоит также отметить тот факт, что одной из причин является то, что сами пользователи относятся безразлично к собственной информационной безопасности. Большинство пользователей всерьез не рассматривают проблему кибер-угроз, не принимают никаких действий, направленных на защиту конфиденциальной информации, а также не предполагают, что используемое техническое устройство (средство) заражено вредоносной программой,

поскольку нет никаких предпосылок в виде замедления работы устройства и иных, свидетельствующих о возможном внедрении вирусного программного обеспечения.

Другой немаловажной причиной роста преступлений является существующая законодательная база. Проблема законодательства даже не в том, что она слабо развита, а в том, что она не в полной мере учитывает текущие реалии, например, определение местоположения абонента сотовой сети связи может растянуться на несколько недель, тоже самое касается и идентификация IP-адресов. Поэтому в настоящее время отмечается негативная тенденция при расследовании дел информационной направленности.

Еще одной причиной является невысокое количество экспертов-криминалистов в области компьютерных преступлений. Специалисты в области компьютерных преступлений вынуждены иногда по сути своей становиться, если не первооткрывателями тех или иных направлений, то теми редкими специалистами, кто расследует данное направление. Например, расследуя преступления в закрытом сегменте сети Интернет – Darknet, специалисты вынуждены осваивать новые направления, поскольку веб-ресурсы данного сегмента анонимны и установить владельца сайта не всегда возможно. Соответственно, если «специалисты-правоохранители» в области информационных технологий иногда сталкиваются с новыми направлениями, то сотрудники, деятельность которых не связана с ИКТ, вынуждены в оперативной обстановке осваивать новые темы и незамедлительно принимать решения.

Рассматривая исторические особенности, необходимо учитывать, что ИКТ в Российской Федерации развивались иным путем в отличие от ряда зарубежных стран-передовиков в этом направлении. Соответственно Российская Федерация ответ на вызовы сегодняшнего дня (кибер-преступления) начала давать не сразу, так как это было выстроено, например, у ряда зарубежных стран-передовиков. В начале «нулевых годов» отставание в развитии ИКТ в Российской Федерации в этом направлении сократилось, в связи с чем Российская Федерация только начинала активно включаться в борьбу с данного рода преступлениями.

Заключение

Рост преступлений компьютерных и с использованием ИКТ достаточно высок. Данному факту способствует значительный рост пользователей в сети Интернет, большинство из которых не предполагают в должной мере о том, какие опасности могут скрываться в сети Интернет.

Для решения этой задачи необходимо:

– массово предупреждать о данных проблемах при помощи средств массовой информации;

– в образовательных организациях включать в учебные занятия по дисциплинам направленности информационных технологий материал о мерах информационной безопасности;

– на уровне интернет-провайдеров и операторов связи вводить меры, позволяющие блокировать нежелательные для пользователя вторжения.

Также рост преступлений компьютерной направленности связан с некоторыми особенностями в нормативных правовых актах, недостаточным количеством экспертов-криминалистов в области ИКТ, недостаточной подготовкой «правоохранителей» по данному вопросу.

Решение данного вопроса должно быть последовательным и комплексным. Например, корректировка действующего законодательства с учетом современной криминогенной обстановки в информационном пространстве, полная и основательная

подготовка и переподготовка сотрудников правоохранительных органов с обязательной обратной связью между образовательной организацией и территориальными органами для того, чтобы обучение происходило с учетом того, что требуется современным «правоохранителям».

Список литературы

1. Федотов Н.Н. Форензика – компьютерная криминалистика [Текст] / Н.Н. Федотов. – М.: Юрид. мир, 2007. – 360 с.
2. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями [Текст] / Д. Айков, К. Сейгер, У. Фонсторх. – М.: Мир, 2014. – 351 с.
3. Спутник – международная новостная лента. URL: https://sputnik-georgia.ru/georgia/20191024/246837584/Georgia-peredala-Rossii-khakera-Yaroslava-Sumbaeva.html (дата обращения: 02.08.2021).
4. Газета «Деловой Петербург». URL: https://www.dp.ru/a/2017/02/08/MVD_likvidirovalo_krupnej (дата обращения: 02.08.2021).
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021) // СПС Кодекс (дата обращения: 02.08.2021).
6. Минаев С.В. Компьютерные преступления: сущность, особенности и возможности предотвращения // Научные ведомости БелГУ. Серия: Философия. Социология. Право. 2017. № 24 (273). URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya (дата обращения: 02.08.2021).
7. Маякова А.С., Шелепова С.А. Компьютерные преступления: отдельные вопросы квалификации // Проблемы экономики и юридической практики. 2017. № 6. URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-otdelnye-voprosy-kvalifikatsii (дата обращения: 02.08.2021).
8. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3 (148). URL: https://cyberleninka.ru/article/n/sovremennye-sposoby-kompyuternyh-prestupleniy-i-zakonomernosti-ih-realizatsii (дата обращения: 02.08.2021).

References

1. Fedotov N.N. Forenzika – computer forensics [Text] /N.N. Fedotov. – M.: Yuri. peace, 2007. – 360 p.
2. Ikov D. Computer crimes. Computer Crime Guide [Text] /D. Ikov, K. Seiger, W. Fonstorch. – M.: World, 2014. – 351 p.
3. Satellite is an international news feed. URL: https://sputnik-georgia.ru/georgia/20191024/246837584/Georgia-peredala-Rossii-khakera-Yaroslava-Sumbaeva.html (date of access: 02.08.2021).
4. Newspaper «Business Petersburg». URL: https://www.dp.ru/a/2017/02/08/MVD_likvidirovalo_krupnej (date of access: 02.08.2021).
5. Criminal Code of the Russian Federation of 13.06.1996 № 63-FZ (ed. from 01.07.2021) // SPS Code (date of access: 02.08.2021).
6. Minaev S.V. Computer crimes: essence, features and possibilities of prevention // Scientific statements of BelSU. Series: Philosophy. Sociology. Right. 2017. № 24 (273). URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya (date of access: 02.08.2021).

7. Mayakova A.S., Shelepova S.A. Computer crimes: individual questions of qualification // Problems of economics and legal practice. 2017. № 6. URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-otdelnye-voprosy-kvalifikatsii (date of access: 02.08.2021).
8. Rossinskaya E.R., Ryadovsky I.A. Modern methods of computer crimes and the patterns of their implementation // Lex Russica. 2019. № 3 (148). URL: https://cyberleninka.ru/article/n/sovremennye-sposoby-kompyuternyh-prestupleniy-i-zakonomernosti-ih-realizatsii (date of access: 02.08.2021).