www.volsu.ru

DOI: https://doi.org/10.15688/lc.jvolsu.2020.1.22

UDC 343.985
LBC 67.52

Submitted: 08.01.2020
Accepted: 31.01.2020

CYBERCRIME AS ONE OF THE KEY PROBLEMS OF THE PRESENT TIME

Natalia I. Dolzhenko

Belgorod State National Research University, Belgorod, Russian Federation

Inna A. Yaroshchuk

Belgorod State National Research University, Belgorod, Russian Federation

Introduction: in the modern conditions, information technologies are widely used in all spheres of human activity, whose main purpose is to optimize social, communication, and economic processes. However, the information technologies often act as a platform for committing crimes, in particular, cybercrimes. In this regard, the authors of the paper set the **goal** of analyzing the data on cybercrimes and the problems arising during their investigation. **Methods:** the methodological framework for the study is based on the laws of scientific knowledge and the provisions of dialectical materialism using the system of general scientific methods, including statistical data analysis, synthesis, induction, deduction, and comparison. **Results:** as a result of the statistical data analysis, it is possible to state the growing amount of crimes that are committed through the information technologies and that, overcoming the limits of the domestic level, acquire the features of a global, world problem. The comparative approach considers the technologies for detecting cybercriminals and investigating cybercrimes in Russia, the United States, and European countries. Special attention is paid to the specifics of cybercrimes in Russia, which make them the most complex categories of crimes, which, in turn, determines the emergence of a number of problems in the investigation of these acts. The research focuses on the problems that arise in practice due to the large number and complex nature of cybercrimes, namely, the lack of special knowledge in the field of information technology among the law enforcement officers, a set of problems related to the effectiveness of investigating cybercrimes and bringing them to court, the lack of a unified investigative and judicial practice in criminal cases of the analyzed category, a number of procedural difficulties, etc. **Conclusions:** as a result of the study, the main problems that arise during the investigation of cybercrime are systematized, as well as the recommendations that allow effective organization of the work of the law enforcement agencies, which, in turn, will help reduce the number of cybercrimes and prevent their commission.

Key words: information technologies, cybercrime, law enforcement, crime investigation, digital forensics, criminally significant traces.

Citation. Dolzhenko N.I., Yaroshchuk I.A. Cybercrime as One of the Key Problems of the Present Time. *Legal Concept*, 2020, vol. 19, no. 1, pp. 151-157. (in Russian). DOI: https://doi.org/10.15688/lc.jvolsu.2020.1.22

УДК 343.985
ББК 67.52

Дата поступления статьи: 08.01.2020
Дата принятия статьи: 31.01.2020

КИБЕРПРЕСТУПНОСТЬ КАК ОДНА ИЗ КЛЮЧЕВЫХ ПРОБЛЕМ СОВРЕМЕННОСТИ

Наталья Игоревна Долженко

Белгородский государственный национальный исследовательский университет,
г. Белгород, Российская Федерация

Инна Александровна Ярощук

Белгородский государственный национальный исследовательский университет,
г. Белгород, Российская Федерация

Введение: в условиях современной действительности информационные технологии имеют массовое использование и широкое применение во всех сферах человеческой деятельности, главной целью которых является оптимизация социальных, коммуникационных, экономических процессов. Однако информационные технологии зачастую выступают в качестве платформы для совершения преступлений, в частности, киберпреступлений. В связи с этим авторами статьи поставлена **цель** анализа данных относительно киберпреступлений и проблем, возникающих при их расследовании. **Методы:** методологическую основу данного исследования составили законы научного познания и положения диалектического материализма с применением системы общенаучных методов, среди которых анализ статистических данных, синтез, индукция, дедукция, сравнение. **Результаты:** в результате анализа статистических данных представляется возможным констатировать растущий уровень преступлений, которые совершаются посредством информационных технологий и которые, преодолевая рамки внутригосударственного уровня, приобретают черты глобальной, мировой проблемы. В рамках сравнительного подхода рассматриваются технологии обнаружения киберпреступников и расследования киберпреступлений в России, США и европейских странах. Особое внимание уделяется особенностям киберпреступлений в России, обусловливающих их в качестве наиболее сложных категорий преступлений, что, в свою очередь, определяет возникновение целого ряда проблем при осуществлении расследования указанных деяний. Исследовательский акцент делается на проблемах, возникающих на практике в силу большого числа и сложного характера киберпреступлений, а именно – отсутствие у сотрудников правоохранительных органов специальных знаний в сфере информационных технологий, комплекс проблем, связанный с эффективностью расследования киберпреступлений и доведения их до суда, отсутствие единой следственной и судебной практики по уголовным делам анализируемой категории, ряд сложностей процессуального характера и др. **Выводы:** в результате исследования систематизированы основные проблемы, возникающие при осуществлении расследования киберпреступлений, а также в качестве обобщающего вывода приводятся рекомендации, позволяющие эффективно организовывать работу правоохранительных органов, что, в свою очередь, будет способствовать снижению числа киберпреступлений и предупреждению их совершения.

Ключевые слова: информационные технологии, киберпреступность, киберпреступление, правоохранительная деятельность, расследование преступлений, компьютерно-техническая экспертиза, криминалистически значимые следы.

Цитирование. Долженко Н. И., Ярощук И. А. Киберпреступность как одна из ключевых проблем современности // Legal Concept = Правовая парадигма. – 2020. – Т. 19, № 1. – С. 151–157. – DOI: https://doi.org/10.15688/lc.jvolsu.2020.1.22

Введение

Стремительное развитие информационных технологий не только позволило оптимизировать деятельность человека в различных сферах, но и привело к возникновению такого негативного явления, как киберпреступность.

Согласно статистическим данным, за январь – ноябрь 2019 г. правоохранительными органами Российской Федерации зарегистрировано 261 208 киберпреступлений, что почти на 70 % больше, чем за аналогичный период предыдущего года [11]. По состоянию на сентябрь 2019 г. ущерб от киберпреступлений в нашей стране составлял более десяти миллиардов рублей [5].

Помимо этого, по данным немецкой страховой компании Allianz Global Corporate &Specialty, ущерб мировой экономике от киберпреступлений в 2016 г. составил не менее 575 млрд долл. США [1], в то время как уже в 2018 г. эта цифра достигла 1,5 триллионов [10].

Указанные цифры свидетельствуют о стремительно растущем уровне преступлений, совершаемых с помощью информационных технологий не только в нашем государстве, но и в глобальных условиях.

Проблемы, возникающие при осуществлении расследования киберпреступлений

Отметим, что сами по себе киберпреступления являются одной из наиболее сложных категорий преступлений в силу ряда особенностей.

К ним можно причислить повышенную латентность; интеллектуальный и трансграничный характер преступной деятельности; возможность совершения преступного деяния одновременно в нескольких местах в автома-

тизированном режиме; дистанционный способ совершения преступления; многоэпизодность в совокупности с множественностью потерпевших, их неосведомленность о том, что они подверглись преступному деянию, а также невозможность предотвращения и пресечения указанных преступлений традиционными средствами [8, с. 109–110].

Значительное число совершаемых киберпреступлений и их сложный характер на практике обусловливают возникновение ряда проблем при осуществлении расследования рассматриваемых деяний.

Так, особую значимость ввиду особой специфики киберпреступлений имеет наличие у сотрудников правоохранительных органов специальных знаний в сфере информационных технологий, так как одного юридического образования недостаточно для продуктивной работы в данном направлении правоохранительной деятельности.

Однако, согласно проведенным исследованиям, несмотря на функционирование Управления «К» МВД России и отделов «К», в наши дни только у 4,5 % следователей имеются более или менее удовлетворительные знания по специальности «Информатика и вычислительная техника» [12, с. 29–30], что формирует один из ключевых проблемных моментов в области расследования киберпреступлений.

Для решения указанной проблемы, на наш взгляд, целесообразно ввести специальный курс для повышения уровня знаний сотрудников в сфере IT-технологий, а также совершенствовать работу уже существующих структур (отделы «К»).

Отметим, что в связи с ростом числа киберпреступлений в последнее время в декабре 2019 г. Председатель Следственного комитета Российской Федерации подписал приказ о создании в составе Главного следственного управления нового подразделения – отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий [9].

Еще одной проблемой, сопровождающей процесс расследования киберпреступлений, является установление факта совершения преступления [6, с. 47]. Это вызвано тем, что киберпреступления обладают высокой степенью латентности. Так, незаконное копирование информации зачастую остается незамеченным, а введение в компьютер вируса обычно объясняется непреднамеренной ошибкой пользователя. Помимо этого сами пострадавшие (особенно если это какие-либо коммерческие организации, банки и т. д.) не спешат сообщать правоохранительным органам о факте совершения преступления, опасаясь подрыва деловой репутации.

Более чем в половине случаев с момента совершения киберпреступления до поступления информации о совершении преступления в правоохранительные органы проходит более 10 дней [2]. Такая несвоевременность ведет к тому, что расследование начинается с запозданием, когда многие доказательства уже утеряны.

Другая проблема заключается в существовании субъективного мнения, согласно которому киберпреступления не представляют большой общественной опасности. На практике возникают ситуации, когда киберпреступники получают довольно легкое наказание вплоть до условного осуждения, что предопределяет правовой нигилизм, с одной стороны, потерпевших, которые не обращаются в правоохранительные органы, так как считают, что преступники не понесут справедливого наказания, а с другой – преступников, которые чувствуют себя безнаказанно.

Целый комплекс проблем связан с эффективностью расследования киберпреступлений и доведения их до суда.

Очевидно, что при совершении киберпреступления следователь имеет дело со следовой информацией особого характера. Следы киберпреступлений возникают в процессе воздействия на информацию в результате внешнего доступа к ней и представляют собой любые ее изменения, связанные с событием преступления – следы копирования информации, ее уничтожения, модификации и т. д. Указанные следы, как правило, остаются на носителях информации, однако их выявление представляет собой довольно сложный и трудоемкий процесс, качественно реализовать который могут лишь квалифицированные эксперты.

Отметим, что как в процессе назначения, так и в процессе проведения компьютерно-технических экспертиз сегодня возникает ряд проблемных моментов.

Так, зачастую сотрудники правоохранительных органов неграмотно опечатывают и изымают различные компьютерно-технические средства. На практике широко распространена ошибка, когда, изымая какие-либо элементы компьютерной техники, следователь или иное лицо (специалист, оперативный сотрудник) опечатывает их таким образом, что не предотвращается возможность их подключения к иному устройству либо электрической сети [4, с. 295].

В результате возникает ситуация, не позволяющая с достоверностью утверждать о неизменности информации, хранящейся в памяти компьютерно-технического средства, так как даже при простом включении системного блока с загрузкой операционной системы создаются новые служебные файлы. Сама по себе загрузка операционной системы приводит к созданию резервных копий файлов реестра и специального файла подкачки, расширяющего виртуальную память, а также к иным изменениям. В свою очередь, запуск различных программ, открытие электронных документов, навигация по сайту в сети «Интернет» вызывают модификации служебных файлов и оставляют различные следы в истории работы, в папках, которые содержат временные и log-файлы и т. д.; а создание (копирование) новых файлов на носителях внешней памяти приводит к изменениям в кластерах, которые отмечены операционной системой как свободные (неиспользуемые) и могут содержать удаленные файлы.

В ходе указанных процессов новая информация записывается «поверх» удаленных, существовавших ранее электронных документов, приводя к невозможности их восстановления и, соответственно, к уничтожению криминалистически значимых следов [3, с. 22–26].

Таким образом, правильность процедуры изъятия объектов компьютерно-технической экспертизы имеет определяющее значение для достоверности и полноты их последующего исследования.

Кроме того, в наши дни следователи зачастую испытывают сложности в грамотной постановке вопросов перед экспертом, что вызвано отсутствием опыта и знаний в предметной области.

Также многими следователями сегодня отмечается высокая загруженность государственных судебно-экспертных учреждений, что опосредует несвоевременность выполнения экспертиз. Причем, по мнению исследователей, в 58 % случаев проведение экспертизы по данной категории дел поручается именно государственно-экспертным учреждениям [6, с. 48].

Рекомендации по организации работы правоохранительных органов по расследованию киберпреступлений

Для решения выявленных проблем представляется разумным повысить уровень мониторинга киберпреступлений; внедрить специальные программы для повышения знаний сотрудников правоохранительных органов в области IT-технологий; улучшить технические возможности подразделений, специализирующихся на расследовании киберпреступлений, а также разработать единую автоматизированную систему для поиска и учета киберпреступлений, способную коррелировать преступные события, связанные с IT-технологиями, совершенные во всех субъектах Российской Федерации.

Выводы

Подводя итоги, отметим, что сегодня в силу огромного влияния информационных технологий на жизнь человека киберпреступность можно считать одной из самых серьезных глобальных проблем. При этом регистрируемые показатели киберпреступности на современном этапе в большей степени зависят от уровня развития государства и специализированных возможностей правоохранительных органов. Так, по данным исследователей, сегодня официальные статистические данные включают в себя лишь 10–20 % от реальной совокупности совершенных киберпреступлений [7, с. 51]: уровень латентности киберпреступности в нашей стране превышает 90 %, а в европейских странах и Соединенных Штатах Америки держится на уровне 75–85 % [13].

Указанные данные в очередной раз доказывают, что в наши дни киберпреступность представляет собой серьезную угрозу, по-

скольку одни только выявленные правоохранительными органами киберпреступления, которые составляют лишь небольшой процент от всех совершенных киберпреступлений, уже сами по себе свидетельствуют о значительном ущербе.

Быстро растущий уровень киберпреступности как в мире, так и в рамках конкретного государства, а также значительные суммы ущерба, причиненного в результате совершения киберпреступлений, опосредуют острую необходимость в выработке эффективных методических рекомендаций, оптимизирующих расследование и раскрытие киберпреступлений, и в подготовке квалифицированных кадров в составе правоохранительных органов.

Отметим, что в Соединенных Штатах Америки и во многих европейских странах на практике успешно применяется технология обнаружения киберпреступников, согласно которой средняя стоимость розыска одного из них равняется тремстам долларам [13]. Борьба с киберпреступлениями российских правоохранительных органов менее эффективна, что обусловлено рядом обстоятельств.

Во-первых, в России отсутствует единая следственная и судебная практика по уголовным делам анализируемой категории, а также наблюдается дефицит высококвалифицированных специалистов, специализирующихся на расследовании преступлений в сфере IT-технологий.

Во-вторых, российскими правоохранительными органами не выработано единых стандартов реагирования на киберпреступления, а также методик их расследования. При этом методики, разработанные другими государствами мирового сообщества, практически не применяются в нашей стране.

В-третьих, существует ряд сложностей процессуального характера, к примеру, проблемным моментом считается назначение и проведение компьютерно-технической экспертизы, которая требует не только особенно грамотной постановки вопросов в совокупности с правильным изъятием объекта, но и значительного количества времени и материальных затрат.

В заключение подчеркнем, что эффективно организованная на практике работа правоохранительных органов, осуществляющих расследование киберпреступлений, в значительной степени влияет на формирование условий, обеспечивающих снижение общего количества киберпреступлений и предупреждение их совершения.

СПИСОК ЛИТЕРАТУРЫ

1. Глобальные киберугрозы: возможно ли безопасное развитие цифровой инфраструктуры? – Электрон. текстовые дан. – Режим доступа: https://tass.ru/pmef-2017/articles/4271384 (дата обращения: 06.01.2020). – Загл. с экрана.

2. Киберпреступления: основные проблемы расследования. – Электрон. текстовые дан. – Режим доступа: https://ceur.ru/library/articles/obshhie_stati/item196792/ (дата обращения: 06.01.2020). – Загл. с экрана.

3. Костин, П. В. Исследование машинных носителей информации при расследовании преступлений в сфере экономики / П. В. Костин. – Н. Новгород, 2009. – 108 с.

4. Кувычков, С. И. О современных проблемах проведения судебно-компьютерных экспертиз в ходе предварительного расследования / С. И. Кувычков // Юридическая наука и практика. Вестник Нижегородской академии МВД России. – 2016. – № 2 (34). – С. 293–298.

5. МВД: Ущерб от киберпреступлений превысил 10 миллиардов рублей. – Электрон. текстовые дан. – Режим доступа: https://rg.ru/2019/12/10/mvd-ushcherb-ot-kiberprestuplenij-prevysil-10-milliardov-rublej.html (дата обращения: 03.01.2020). – Загл. с экрана.

6. Нестерович, С. А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов / С. А. Нестерович // Вестник науки и образования. – 2018. – № 8 (44). – С. 46–49.

7. Номоконов, В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 1. – С. 45–55.

8. Осипенко, А. Л. Сетевая компьютерная преступность: теория и практика борьбы / А. Л. Осипенко. – Омск : Изд-во Омск. акад. МВД России, 2009. – 479 с.

9. Расследованием киберпреступлений в СКР займется спецотдел. – Электрон. текстовые дан. – Режим доступа: https://www.interfax.ru/russia/688619 (дата обращения: 03.01.2020). – Загл. с экрана.

10. Сбербанк дал прогноз по ущербу мировой экономике от кибератак в 2019 году. – Электрон. текстовые дан. – Режим доступа: https://www.rbc.ru/

finances/26/04/2019/5cc2d4fb9a7947c25f7a521a (дата обращения: 03.01.2020). – Загл. с экрана.

11. Состояние преступности в России за январь – ноябрь 2019 г. – Электрон. текстовые дан. – Режим доступа: https://genproc.gov.ru/upload/iblock/c8f/sbornik_11_2019.pdf (дата обращения: 07.01.2020). – Загл. с экрана.

12. Шевченко, Е. С. Актуальные проблемы расследования киберпреступлений / Е. С. Шевченко // Эксперт-криминалист. – 2015. – № 3. – С. 29–30.

13. 80 % пользователей не верят, что интернет-преступников можно наказать. – Электрон. текстовые дан. – Режим доступа: http://itua.info/software/28662.html (дата обращения: 06.01.2020). – Загл. с экрана.

REFERENCES

1. *Globalnyye kiberugrozy: vozmozhno li bezopasnoye razvitiye tsifrovoy infrastruktury?* [Global Cyber Threats: is it Possible to Safely Develop a Digital Infrastructure?]. URL: https://tass.ru/pmef-2017/articles/4271384 (accessed 6 January 2020).

2. *Kiberprestupleniya: osnovnyye problemy rassledovaniya* [Cybercrimes: The Main Problems of the Investigation]. URL: https://ceur.ru/library/articles/obshhie_stati/item196792/ (accessed 6 January 2020).

3. Kostin P.V. *Issledovaniye mashinnykh nositeley informatsii pri rassledovanii prestupleniy v sfere ekonomiki* [The Study of Computer Storage Media in the Investigation of Economic Crimes]. Nizhny Novgorod, 2009. 108 p.

4. Kuvychkov S.I. O sovremennykh problemakh provedeniya sudebno-kompyuternykh ekspertiz v khode predvaritelnogo rassledovaniya [On Current Issues of Forensic Computer Examinations During the Preliminary Investigation]. *Yuridicheskaya nauka i praktika. Vestnik Nizhegorodskoy akademii MVD Rossii* [Jurisprudence and Practice], 2016, no. 2 (34), pp. 293-298.

5. *MVD: Ushcherb ot kiberprestupleniy prevysil 10 milliardov rubley* [The Ministry of Internal Affairs: Damage From Cybercrime Exceeded 10 Billion Rubles]. URL: https://rg.ru/2019/12/10/mvd-ushcherb-ot-kiberprestuplenij-prevysil-10-milliardov-rublej.html (accessed 3 January 2020).

6. Nesterovich S.A. Problemy rassledovaniya kiberprestupleniy, kotoryye stoyat pered sotrudnikami sledstvennykh organov [Problems of Investigation of Cybercrimes that are Faced by Investigative Authorities]. *Vestnik nauki i obrazovaniya* [Bulletin of Science and Education], 2018, no. 8 (44), pp. 46-49.

7. Nomokonov V.A., Tropina T.L. Kiberprestupnost kak novaya kriminalnaya ugroza [Cybercrime as a New Criminal Threat]. *Kriminologiya: vchera, segodnya, zavtra* [Criminology: Yesterday, Today, Tomorrow], 2012, no. 1, pp. 45-55.

8. Osipenko A.L. *Setevaya kompyuternaya prestupnost: teoriya i praktika borby* [Network Computer Crime: Theory and Practice of Combat]. Omsk, Izd-vo Omsk. akad. MVD Rossii, 2009. 479 p.

9. *Rassledovaniyem kiberprestupleniy v SKR zaymetsya spetsotdel* [Investigation of Cybercrime in the TFR will be Carried Out by the Special Department]. URL: https://www.interfax.ru/russia/688619 (accessed 3 January 2020).

10. *Sberbank dal prognoz po ushcherbu mirovoy ekonomike ot kiberatak v 2019 godu* [Sberbank Gives a Forecast on the Damage to the Global Economy From Cyber Attacks in 2019]. URL: https://www.rbc.ru/finances/26/04/2019/5cc2d4fb9a7947c25f7a521a (accessed 3 January 2020).

11. *Sostoyaniye prestupnosti v Rossii za yanvar – noyabr 2019 g.* [The State of Crime in Russia for January – November 2019]. URL: https://genproc.gov.ru/upload/iblock/c8f/sbornik_11_2019.pdf (accessed 7 February 2020).

12. Shevchenko E.S. Aktualnyye problemy rassledovaniya kiberprestupleniy [Actual Problems of the Investigation of Cybercrime]. *Ekspert-kriminalist* [Expert Criminalist], 2015, no. 3, pp. 29-30.

13. *80 % polzovateley ne veryat, chto internet-prestupnikov mozhno nakazat* [80% of Users do not Believe that Internet Criminals can be Punished]. URL: http://itua.info/software/28662.html (accessed 6 January 2020).

Information About the Authors

Natalia I. Dolzhenko, Candidate of Sciences (Jurisprudence), Associate Professor, Department of Forensic Science and Criminology, Belgorod State National Research University, Pobedy St., 85, 308015 Belgorod, Russian Federation, dolzhenko@bsu.edu.ru, https://orcid.org/0000-0001-6382-1111

Inna A. Yaroshchuk, Candidate of Sciences (Philology), Associate Professor, Department of Forensic Science and Criminology, Belgorod State National Research University, Pobedy St., 85, 308015 Belgorod, Russian Federation, yaroshchuk@bsu.edu.ru, https://orcid.org/0000-0002-5604-549X

Информация об авторах

Наталья Игоревна Долженко, кандидат юридических наук, доцент кафедры судебной экспертизы и криминалистики, Белгородский государственный национальный исследовательский университет, ул. Победы, 85, 308015 г. Белгород, Российская Федерация, dolzhenko@bsu.edu.ru, https://orcid.org/0000-0001-6382-1111

Инна Александровна Ярощук, кандидат филологических наук, доцент кафедры судебной экспертизы и криминалистики, Белгородский государственный национальный исследовательский университет, ул. Победы, 85, 308015 г. Белгород, Российская Федерация, yaroshchuk@bsu.edu.ru, https://orcid.org/0000-0002-5604-549X