УДК 343.521
ББК Х408.16
DOI: 10.14529/law210303

ВИКТИМОЛОГИЯ И КИБЕРПРЕСТУПНОСТЬ В РОССИИ

Н. В. Ткачева, Е. Н. Серова
Южно-Уральский государственный университет, г. Челябинск

В статье отмечается, что причиной большинства из совершенных преступлений становилось халатное отношение пользователя к своим личным данным в сети. Роль потерпевшего при совершении киберпреступлений трудно переоценить. Проводится анализ причин, по которым определенные лица становятся жертвами киберпреступленпй, с целью предотвращения их совершения. Анализируется учение о жертве преступления с точки зрения поведения разного рода лиц, пострадавших от преступлений. Уделяется внимание анализу поведения лица, которое совершает действия в информационном пространстве посредством компьютерных систем. Вопрос о соотношении виктимологии с другими науками является дискуссионным. Авторы останавливаются на этой дискуссии и высказывают свою точку зрения. В рамках исследования и с целью выяснения изменений, которые произошли за десять лет, и причин, по которым лица становятся жертвами преступлений, авторы провели опрос 100 студентов Южно-Уральского государственного университета, средний возраст которых – от 17 до 24 лет.

Ключевые слова: информационная среда, киберпреступность, виктимология, личность преступника, жертва преступления, компьютерная сеть.

С помощью компьютерных сетей, а также в рамках или против компьютерной системы или сети могут совершаться ряд преступлений. Эти преступления исторически получили название киберпреступления. События, связанные с COVID-19, показали, что многие сферы жизни человека, начиная от межличностного общения и до управления финансами, могут осуществляться посредством информационных технологий. Так как мировое сообщество увеличивает использование, накапливание, передачу информации через электронные ресурсы, количество преступлений, совершаемых в сфере информационных технологий, возрастает как в России, так и в мире. Статистика за январь–октябрь 2020 года свидетельствует о том, что зарегистрировано на 75,1 % больше противоправных деяний, совершенных с использованием информационных технологий, чем за 2019 год (URL: https://xnb1aew.xnp1ai/reports/item/). Причиной большинства совершенных преступлений становилось халатное отношение пользователя к своим личным данным в сети. Таким образом, роль потерпевшего при совершении киберпреступлений трудно переоценить. Проводили анализ причин, по которым определенные лица становятся жертвами киберпреступлений, с целью предотвращения их совершения.

Учение о жертве преступления исследует поведение разного рода лиц, пострадавших от преступлений. Интересным, на наш взгляд, представляется анализ поведения лица, которое совершает действия в информационном пространстве посредством компьютерных систем. Вопрос о соотношении виктимологии с другими науками является дискуссионным. Одни авторы называют виктимологию отраслью криминологии, другие – относят ее к частной криминалистической теории [1, с. 14], третьи – считают ее вспомогательной наукой уголовного и уголовно-процессуального права, четвертые – считают, что виктимология – самостоятельная наука, которая частично принадлежит к юридическим наукам, а частично относится к безопасности жизнедеятельности человека [4, с. 8]. На наш взгляд, последняя точка зрения является наиболее верной, так как виктимология развивается уже давно, и она вышла за рамки криминологии. Виктимология имеет очень мало общего с криминалистикой, а относить виктимологию к уголовному или уголовно-процессуальному праву можно только условно, так как понятие «жертва преступления» не равно понятию потерпевший; виктимология изучает как поведение потерпевших, так и лиц, которые не обращались в правоохранительные органы с заявлением о преступлении.

Основная цель виктимологии – изучение поведения жертвы преступления во взаимо-

связи с преступником для предотвращения будущих преступлений. Виктимное поведение означает такое поведение, которое отражает повышенную способность человека в силу его социальной роли и ряда физических и духовных качеств при определенных обстоятельствах становиться жертвой преступления.

Существует четыре вида виктимности: индивидуальная, видовая, групповая, массовая [3, с. 10]. Индивидуальная виктимность отражает свойства отдельного индивида, она сложнее всего поддается изучению, так как изучить каждого человека не представляется возможным. Видовая виктимность отражает предрасположенность отдельных людей становиться, в силу ряда обстоятельств, жертвами определенных видов преступлений. Групповая виктимность отражает поведение определенных категорий людей, обладающих сходными социальными, демографическими, психологическими, биофизическими и иными качествами. Массовая виктимность показывает поведение определенной части людей, в которой лица не связаны друг с другом какими-либо признаками.

Исследуя термин «киберпреступления», обратимся к Конвенции Совета Европы, где типы компьютерных преступлений связаны с нарушением конфиденциальности, а также целостности и доступности компьютерных данных и систем. Анализ научной литературы и законодательства показывает, что авторы и законодатель используют термины «компьютерные преступления», «электронные средства связи», «информационные технологии» или «преступления в сфере высоких технологий». В Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) не используется термин «киберпреступность», а дается определение преступления в сфере компьютерной информации как уголовно наказуемого деяния, предметом посягательства которого является компьютерная информация. Это определение присутствует только в доктрине. Например, существует точка зрения о том, что киберпреступления – преступления, связанные как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. По мнению Е. П. Ищенко, к киберпреступлениям относятся такие деяния, которые совершаются в виртуальной реальности с помощью или посредством компьютерных систем или сетей, а также иных средств удаленного доступа [2, с. 16]. Необходимо отметить, что по данным на октябрь 2020 года на деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходится одно из четырех регистрируемых в текущем году преступлений, то есть это 420,7 тыс. (Ежемесячный сборник о состоянии преступности в России за январь–октябрь 2020 года. URL: http://www.crimestat.ru/analytics).

К понятию «киберпреступления» относят следующие составы преступлений: мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

Однако большой интерес с точки зрения виктимологии представляют только ст. 159.3 УК РФ и ст. 272 УК РФ, потому что при создании вредоносных программ возможны случаи, когда жертв нет. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей является практически «мертвым» составом, за 2015 год было зарегистрировано 12 преступлений, и это максимум с 2011 года. А при неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации жертвой становится Российская Федерация, государство не поддается виктимологическому изучению.

Представляется, что имеет смысл исследовать мошенничество с использованием электронных средств платежа и неправомерный доступ к компьютерной информации. Самым распространенным составом в сфере компьютерных преступлений остается мошенничество с использованием электронных средств платежа (далее – мошенничество), на втором месте находится неправомерный доступ к компьютерной информации (далее – не-

правомерный доступ). Неправомерный доступ обладает средним уровнем латентности, потому что о факте неправомерного доступа к компьютерной информации жертва узнает не всегда, а только тогда, когда данные потерпевшего преступник передает третьим лицам. Интерес, на наш взгляд, представляет изучение причин, по которым лица становятся жертвами преступлений в сфере компьютерной информации.

В теории выделяют следующие причины виктимности. Основной причиной является неграмотность пользователя, так как пользователи неразумно предоставляют пароли от своих компьютеров третьим лицам. Например, жертвы предоставляют свои данные, когда кто-либо звонит и представляется служащим банка или администратором, при этом не проверяя их личность. Это распространенный случай в таком составе преступления, как мошенничество. Второй причиной является доверчивость лиц, которые используют свои данные на непроверенных сайтах. Третьей причиной является страх, так как преступники используют методы морального давления на жертв, угрожая им тем, что их денежные средства могут быть списаны третьими лицами. Четвертой причиной является нежелание устанавливать защитные программы на свои персональные устройства, так как пользователи либо не верят в их эффективность, либо не желают нести затраты на оплату этих программ. В 2011 году был проведен опрос среди жертв киберпреступлений: было выявлено, что мужчины становились жертвами преступлений в 54,8 % случаев, а женщины – в 45,2 %. В 78,6 % случаев пострадавшие от незаконного доступа посредством сети «Интернет» не защищали свои данные, и преступники беспрепятственно с помощью общераспространенных программ получили доступ к вычислительным машинам жертв. В 2018 году был проведен новый опрос, в котором опрошено 17 000 респондентов: 200 человек, или около 1,1 %, стали жертвами удаленного мошенничества за последний год, то есть их имуществом (в том числе деньгами), по их мнению, завладели обманом при помощи телефона или интернета. При этом респондентами были лица разных возрастов и социального положения.

С целью выяснения изменений, которые произошли за десять лет, и причин, по которым лица становятся жертвами преступлений, мы провели опрос среди студентов Южно-Уральского государственного университета. В опросе приняло участие 100 человек. Средний возраст опрошенных от 17 до 24 лет. В опросе участвовали студенты обоих полов. Студентам были заданы следующие вопросы:

1) совершались ли в отношении вас или ваших близких киберпреступления;

2) почему в отношении вас или ваших родственников совершилось киберпреступление?

На второй вопрос были предоставлены следующие варианты ответов:

1) злоумышленники были убедительны в своих предложениях;

2) я даже не предполагал, что мои данные похитят, всегда было все нормально;

3) я не могу назвать причины, со мной не взаимодействовали злоумышленники, узнал о преступлении после списания денежных средств;

4) я испытал психологическое давление в виде запугивания и т.д.

Результаты опроса показали следующее: 52 % не сталкивались с совершением киберпреступлений ни в отношении себя, ни в отношении своих родственников, 25 % опрошенных сталкивались с совершением киберпреступлений в отношении своих знакомых и родственников, а 23 %, среди которых 11 % женщин и 12 % мужчин, сталкивались с совершением киберпреступлений в отношении себя.

Относительно причин совершения преступлений опрошенные сообщили: 29 человек не знает причин, почему они стали жертвами преступлений, так как о них узнали только тогда, когда списали денежные средства. Среди них было 19 женщин и 10 мужчин. При этом 10 человек заявило, что всегда использовали пароли на одних и тех же сайтах, всегда было все нормально, а затем неожиданно узнали о том, что стали жертвами преступлений, среди них 5 женщин и 5 мужчин. На убедительность злоумышленников сослалось только 7 человек, среди которых 4 женщины и 3 мужчин. Испытали психологическое давление только 2 человека, среди которых были только женщины.

По результатам данного опроса можно сделать следующие выводы.

Во-первых, мужчины и женщины примерно в равном процентном соотношении становятся жертвами преступлений. Это явля-

ется еще одной особенностью преступлений, так как цель преступника – это, как правило, завладение чужими денежными средствами, поэтому здесь не важны личность и физические особенности жертвы, поскольку он с ней не имеет прямого контакта.

Во-вторых, из-за развития технологий злоумышленники почти перестали напрямую связываться с жертвой, а совершают преступления тайно. Большинство опрошенных узнали о преступлении только после того, как списали денежные средства с их карты.

В-третьих, такие методы, как убеждение и психологическое давление, больше воздействует на женщин, чем на мужчин.

В-четвертых, только 23 % среди молодежи являются жертвами преступлений. С одной стороны, это хороший показатель, так как большинство не становятся жертвами, но, с другой стороны, почти каждый четвертый студент является жертвой киберпреступления, при этом, молодежь – это та часть населения, которая относится к категории активных пользователей компьютерных технологий, в теории они должны понимать различные мошеннические интернет-схемы.

Как правило, результатом любого виктимологического исследования являются типичный портрет жертвы и советы по профилактике определенной категории преступлений. В случае киберпреступлений описать типичный портрет жертвы очень сложно. Как уже было сказано выше, преступнику не важен пол жертвы, так как он с ней не имеет прямого контакта, возраст тоже не является определяющим, так как молодежь является активно пользуется интернет-технологиями, но им известно много о мошеннических схемах. Обратная ситуация с гражданами, старше 50 лет. Дети являются активными пользователями интернета, но они зачастую не имеют собственных денежных средств или какой-либо важной информации, поэтому эта категория лиц не интересна преступникам. Киберпреступления не связаны с социальным положением лица, преступники могут завладеть как 5 000 000 руб., так и 5 000 руб. Типичная жертва должна иметь два признака: первый – использовать компьютерные технологии, а это почти 100 %, второй – неграмотно распространять свои персональные данные и сведения о паролях и лицевых счетах.

Самым эффективным методом профилактики является постоянное упоминание в СМИ о новых способах совершения киберпреступлений. Одной из причин того, что злоумышленники почти перестали звонить, писать сообщения и т.д. своей жертве, является информирование населения о распространенных способах обмана. Это подтверждает и опрос. Некоторые из наших респондентов поясняли, что они не являлись жертвами киберпреступлений, так как они слышали об определенных приемах мошенников. Например, при поступлении в социальных сетях предложения о вложении инвестиций в какой-либо проект преступники не сообщают практически никакой конкретной информации о проекте, либо отсутствуют данные о самом злоумышленнике. Вторым способом являются разработка и последующее распространение в СМИ определенных кратких схем, в которых была бы указана информация о безопасном поведении в сети «Интернет» и безопасном использовании мобильных устройств. Третий способ – разработка специальных компьютерных программ, которые либо блокировали бы неправомерный доступ к данным пользователя, либо уведомляли бы о нем. Однако этот способ является самым неэффективным, так как с помощью современных технологий можно обойти практически любую защитную программу.

Литература

1. Виницкий, Л. В. Криминалистическая виктимология: монография / Л. В. Виницкий, Н. Е. Шинкевич. – Челябинск, 2005. – 203 с.

2. Ищенко, Е. П. К вопросу об экспертном и криминалистическом обеспечении расследования киберпреступности / Е. П. Ищенко // Вестник Московского университета МВД России. – 2013. – № 3. – С. 15–17.

3. Полубинский, В. И. Криминальная виктимология / В. И. Полубинский. – М.: ВНИИ МВД России, 2008. – 210 с.

4. Ривман, Д. В. Криминальная виктимология: учебник / Д. В. Ривман. – СПб., 2002. – 304 с.

Ткачева Наталья Викторовна – кандидат юридических наук, доцент, доцент кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: tkachevanv@susu.ru.

Серова Евгения Николаевна – студент, Южно-Уральский государственный университет, г. Челябинск. E-mail: zhenya.serova@bk.ru.

Статья поступила в редакцию 17 мая 2021 г.

DOI: 10.14529/law210303

VICTIMOLOGY AND CYBERCRIME IN RUSSIA

N. V. Tkacheva, E. N. Serova
South Ural State University, Chelyabinsk, Russian Federation

The article notes that in most of the crimes committed, the reason was the user's negligent attitude to their personal data online. The role of the victim in cybercrime is difficult to overestimate. An analysis of the reasons why certain individuals become victims of cybercrime is conducted in order to prevent them from committing them. The doctrine of the victim of crime is analyzed in terms of the behavior of various kinds of persons affected by crime. Attention is paid to the analysis of the behavior of the person who commits acts in the information space through computer systems. The issue of correlation of victimology with other sciences is debatable. The authors dwell on this debate and express their point of view. As part of the research and in order to find out the changes that have occurred over a decade and to find out the reasons why individuals become victims of crime, we conducted a survey among students at South Ural State University. One hundred people took part in the survey. The average age of those surveyed ranged from 17 to 24 years old.

Keywords: information environment, cybercrime, victimology, identity of the offender, victim of a crime, computer network.

References

1. Vinickij L. V., Šinkevič N. E. *Kriminalističeskaâ viktimologiâ* [Forensic victimology]. Chelyabinsk, 2005, 203 p.

2. Išenko E. P. [On the issue of expert and forensic support for the investigation of cybercrime]. *Vestnik moskovskogo universiteta MVD Rossii [Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia]*, 2013, no. 3, pp. 15–17. (in Russ.)

3. Polubinskij V. I. *Kriminal'naâ viktimologiâ* [Criminal victimology]. Moscow, 2008, 210 p.

4. Rivman D. V. *Kriminal'naâ viktimologiâ* [Criminal victimology]. St. Petegsburg, 2002, 304 p.

Natalia Viktorovna Tkacheva – Candidate of Sciences (Law), Associate Professor of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: tkachevanv@susu.ru.

Evgenia Nikolaevna Serova – student, South Ural State University, Chelyabinsk, Russian Federation. E-mail: zhenya.serova@bk.ru.

Received 17 May 2021.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Ткачева, Н. В. Виктимология и киберпреступность в России / Н. В., Ткачева, Е. Н. Серова // Вестник ЮУрГУ. Серия «Право». – 2021. – Т. 21, № 3. – С. 19–23. DOI: 10.14529/law210303.

FOR CITATION

Tkacheva N. V., Serova E. N. Victimology and cybercrime in Russia. *Bulletin of the South Ural State University. Ser. Law*, 2021, vol. 21, no. 3, pp. 19–23. (in Russ.) DOI: 10.14529/law210303.