DOI 10.17150/2411-6262.2020.11(1).18 http://brj-bguep.ru

УДК 330.35

Д.В. Жмуров
Байкальский государственный университет,
г. Иркутск, Российская Федерация
Р.Н. Ключко
Гродненский государственный университет им. Янки Купалы,
г. Гродно, Республика Беларусь

КИБЕРВИКТИМОЛОГИЯ КАК НОВАЯ РЕАЛЬНОСТЬ ТЕХНОТРОННОГО ОБЩЕСТВА (ГЕНДЕРНОЕ ИССЛЕДОВАНИЕ)

АННОТАЦИЯ. В статье изучены некоторые вопросы развития кибервиктимологии. Это учение о жертве преступления, совершенного при помощи компьютерных технологий. Цель исследования — выявить реальное положение дел, касающихся виктимизации в сети Интернет лиц разного пола (в региональном аспекте). Для этой цели был проведен опрос 584 студентов всех крупных ВУЗов Иркутской области. Респондентов просили оценить опасности использования сети Интернет и указать случаи индивидуальной виктимизации в этой среде. Для получения сведений касающихся гендерных различий кибервиктимизации опрошенных разделили по полу (221 мужчина и 363 женщины). Проведенное исследование показало, что, как и в обычной жизни, в виртуальном пространстве мужчины чаще демонстрируют рискованное поведение, пренебрежение правилами безопасности и легкомысленное отношение к возможным угрозам. Жертвами в сети Интернет нередко становятся те, кто уже ранее был жертвой в реальной жизни. Вместе с тем, женщины чаще подвергаются виктимизирующему воздействию (на одного пользователя женского пола приходится почти 4 типа дискриминирующих акта, тогда как на мужчину — в среднем 3). Виды виктимизирующих воздействий также имеют гендерную специфику. Наибольшее расхождение в структуре виктимизации было зафиксировано для взлома аккаунта в социальных сетях (6 % у мужчин против 49 % у женщин); установки на компьютер вредоносных программ (14 % против 8 %); оскорблений (20 % против 10 %), непристойных предложений (10 % против 25 %), а также хищений конфиденциальной информации (3 % против 1 %). Таким образом, мужчины чаще становятся жертвами хищений данных паспорта (платежных карт), подвергаются атакам программ-вымогателей, вербальной агрессии или страдают от недобросовестных продавцов товаров. Женщины с более высокой частотой становятся потерпевшими от взлома аккаунтов в социальных сетях и сексуально окрашенного киберпреследования. Значительный ущерб, несмотря на малое количество подобных случаев, почти в два раза чаще причинялся мужчинам. Результаты исследования свидетельствуют о том, что более 90 % опрошенной возрастной группы становились жертвами киберпреступлений, как правило, нескольких. По данным отчетов респондентов было выявлено около 15 различных форм виктимизирующих воздействий в сети Интернет. Среди них: взлом почтового ящика или аккаунта, распространение ложной информации от имени пользователя, непристойные предложения, сексуальные домогательства, оформление платных интернет-подписок, ложное погашение штрафа и пр.

КЛЮЧЕВЫЕ СЛОВА. Кибервиктимология, жертвы киберпреступлений, потерпевшие в сети Интернет.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 1 декабря 2019 г.; дата принятия к печати 2 марта 2020 г.; дата онлайн-размещения 31 марта 2020 г.

D.V. Zhmurov
Baikal State University,
Irkutsk, Russian Federation
R.N. Klyuchko
Yanka Kupala Grodno State University,
Grodno, Belorussia

CYBER-VICTIMOLOGY AS A NEW REALITY OF THE TECHNOTRONIC SOCIETY (GENDER RESEARCH)

ABSTRACT. The article studies some issues of cyber-victimology development. This is a doctrine of the crime victim committed with the help of computer technology. The purpose of the study is to identify the real situation of epy cases regarding the victimization of different sexes on the Internet (in the regional aspect). For this purpose, a poll of 584 students of all major universities of Irkutsk Oblast was conducted. The respondents were asked to assess the dangers of using the Internet and indicate instances of individual victimization in this environment. To obtain information on gender differences of cyber-victimization, the respondents were divided in term of genders (221 men and 363 women). The study showed that, like in ordinary life, in the virtual space, men more often demonstrate risky behavior, neglect of safety rules and frivolous attitude to possible threats. Victims on the Internet are often those who have already been a victim in real life. At the same time, women are more often exposed to victimization effects (there are almost four ypes of discriminatory acts per one female user, while there are three acts per a man on the average). Types of victimization effects are also gender-specific. The largest discrepancy in the structure of victimization was recorded for hacking into an account on social networks (6 % for men against 49 % for women); installation of malicious programs on the computer (14 % against 8 %); insults (20 % against 10 %) and indecent proposals (10 % against 25 %), as well as embezzlement of confidential information (3 % against 1 %). Thus, men are more likely to become victims of the theft of passport data (payment cards), are subjected to attacks by extortionists, verbal aggression, or suffer from dishonest sellers of goods. Women with a higher frequency become victims of hacking into accounts in social networks and sexually colored cyber-stalking. Significant damage, despite a small number of such cases, was almost twice as often caused to men. The results of the study indicate that more than 90 % of the surveyed age group were victims of cybercrimes, as a rule, of several ones. According to the respondents' reports, about 15 various forms of victimization effects on the Internet were identified. Among them there is hacking of a mailbox or an account, dissemination of false information on behalf of the user's name, indecent offers, sexual harassment, registration of paid Internet subscriptions, false repayment of the fine, and so on.

KEYWORDS. Cyber-victimology, victims of cybercrimes, victims on the Internet.

ARTICLE INFO. Received December 1, 2019; accepted March 2, 2020; available online March 31, 2020.

Реальность меняется и преступность меняется вместе с ней. Всего полтора века назад самым массовым преступлением было ограбление поезда. Мог ли Джесси Джеймс, отбиравший у ошеломленных пассажиров золото и кошельки, представить, что через 145 лет все настолько изменится? 77 млн потерпевших лишь от одного преступления, связанного с хищением персональных данных игрового сервиса Sony PSN [1]; вымогательства и кражи, совершаемые ботами без классического взаимодействия «жертва-преступник»; возможность похищения у человека его цифровой личности [2], налоговой идентичности [3] и много чего еще. По данным последних исследований только в США число инцидентов, связанных с кражей личности перевалило за 60 млн случаев[1].

В 2017 г. по данным Norton Cyber Security Insights почти каждый 7 житель Земли стал жертвой киберпреступлений. От хищений пострадали 978 млн чел. в 20 странах мира [4]. И это еще без учета сексуальных деликтов, эпизодов виртуального преследования, травли и много другого.

Такого стремительного роста преступности человечество еще не знало, как не знает, что с этим делать. Попытки применения наднациональной юрисдик-

[1] Protecting Children from Identity Theft Act : Report / Committee on Ways and Mean. Texas, 2018. 636 p. URL: https://www.govinfo.gov/content/pkg/CRPT-115hrpt636/pdf/CRPT-115hrpt636.pdf.

ции к интернет-преступникам, создания эффективной системы приема заявлений граждан или специализированных органов профилактики, пока не увенчались успехом. Сложности возникают на уровне квалификации преступных деяний [5]. Правоохранительная система развитых стран не готова к решению возникшей проблемы. Не говоря уже о развивающихся государствах и России, в частности. По мнению ряда it-экспертов, современная реакция общества на кибепреступность напоминает кавалерийские атаки 1941 г. на укрепленные пулеметные точки немецкой армии [6]. Бесполезно, трагично и неэффективно.

В свете сказанного, фундаментальной задачей научного сообщества является не только изучение киберпреступности, но и корпуса ее жертв. Как никогда актуальна разработка концептуальных основ кибервиктимологии, т.е. **учения о жертве преступления, совершенного при помощи компьютерных технологий.** В ближайшие десятилетия число таких лиц будет только расти. Исследования в области кибервиктимологии позволят: объективно оценить масштабы и цену киберпреступности, дополнить научную концепцию жертвы преступления новыми знаниями, создать инструменты прогнозирования виктимного поведения в мировой сети, разработать комплексную систему виктимологической профилактики киберпреступности.

Проблема изучения жертв киберпреступности является фундаментальной для современной науки и актуальна по ряду причин:

Во-первых, мы очень мало знаем об этой категории лиц. В докладе ООН о всестороннем исследовании проблем киберпреступности (2013) указано, что около 80 % таких пострадавших в полицию не обращаются [7, с. 25]. В России, вероятно, эта цифра выше. Следовательно, имеющиеся представления о жертвах киберпреступности фрагментарны, получены на основе изучения меньшинства потерпевших. Дефицит знаний о них влечет неполноценность виктимологической профилактики, а значит, в косвенном смысле, позволяет киберпреступности расти и процветать. Многие авторы сегодня отмечают, что для выявления истинных масштабов распространения киберпреступности требуется использование новых источников получения информации [8], которым вполне могут стать жертвы этой преступности.

Во-вторых, развитие технологий и рост их популярности среди населения существенно повышает число жертв этих технологий. Повсеместное распространение электронных устройств и высокие темпы технических инноваций, готовность многих людей к рискованному поведению в Интернет, анонимность и транснациональность сетевых коммуникаций: все это делает пользователей менее защищенными от действий злоумышленников. Нельзя забывать о правовой безграмотности и инертности пострадавших, вносящей свой вклад в латентность киберпреступности [9]. Виктимология будущего сосредоточится именно на этом типе жертв. Вероятно, он станет доминирующим в ближайшие десятилетия, если уже не стал таковым.

В-третьих, нельзя не отметить, что изучение жертв киберпреступности помогает лучше понять это явление, оценить его масштабы и разработать методы профилактики. Исследование и профилирование жертв является одним из способов контроля над киберпреступностью, формой предупреждения и минимизации наносимого ею ущерба. Во многом это связано с выявлением виктимогенных личностных характеристик и созданием программ девиктимизации указанных категорий лиц.

Целью настоящей статьи было проведение одного из первых в отечественной науке исследований по кибервиктимологии (в региональном аспекте). Для реализации этой цели был разработан опросник виктимного поведения в сети Интернет, призванный оценить риски использования этой технологии, а так-

же выявить реальное положение дел с частотой дискриминации пользователей. Для получения репрезентативных результатов было опрошено 584 студента всех крупных ВУЗов Иркутской области (ИГУ, БГУ, ИГАУ, ИРНИТУ, ИРГУПС) в возрасте от 19 до 24 лет.

Помимо этого, в рамках подготовки настоящей статьи было проведено аналитическое исследование научных материалов по проблеме кибервиктимологии. Для первичного анализа были использованы ключевые слова «интернет-потерпевший», «жертва в Интернет», «жертва киберпреступления», «кибервиктимология», «Интернет-виктимность», «пострадавший в Интернет». Поиск осуществлялся на базе портала E-library с учетом морфологии с последующей ручной обработкой результатов. Проведенный анализ позволил сделать несколько выводов относительно современного состояния исследований в этой области. Озвучим их:

1. Научное сообщество не уделяет достаточного внимания этой проблеме даже несмотря на десятикратный рост киберпреступности и ее жертв в 2013–18 гг. (с 11 тыс. зарегистрированных случаев в 2013 г. до 121 тыс. в октябре 2018)[2]. В ходе анализа было выявлено 143 работы по теме. Из них: 82 статьи, 57 тезисов выступлений, 1 учебное пособие, 3 главы в книге. Подавляющее большинство датированы 2016 г. (16 %) и 2017 г. (33 %), 2018 (27 %) годами. То есть научная проблема еще только конкретизируется.

2. Значительная доля исследований охватывает частные вопросы кибервиктимологии. Немало публикаций на тему суицидальных интернет-групп (20 %). Это связано со своеобразной «модой» на подобный контент, культивируемой средствами массовой информации. 14 % работ посвящены особенностям виктимизации от интернет-мошенничества, еще 21 % — кибербулингу, киберсталкингу и сходным формам агрессии в виртуальном пространстве. Существенно меньше исследований затрагивают вопросы сексуальной эксплуатации несовершеннолетних (6 %) и пропаганды терроризма (4 %) во всемирной паутине. Предметом 31 % изысканий являются различные виктимологические аспекты преступности в Интернет. Таким образом, публикационный пул разрознен частными проблемами без фундаментального и системного осмысления ситуации. Всего 4 % исследований изучают предметные и методологические вопросы кибервиктимологии (О.Б. Бовть, М.А. Данилова, А.С. Горелова, Ю.А. Иванова, А.В. Попова). Об актуальности кибервиктимологии упоминают в своих работах П.А. Кабанов, В.А. Плешаков, А.А. Мишин и другие авторы.

3. Проведенный анализ показал, что изучение проблемы кибервиктимологии находится в зачаточном состоянии. Это серьезное отставание науки от объективной реальности, которое нуждается в скорейшем преодолении.

В зарубежной научной среде эта проблема обсуждается значительно более активно и вынесена на повестку дня. К примеру, за последние годы опубликованы фундаментальные исследования «Киберпреступность и виктимизация женщин: законы, права и положения» (2012), «Кибер-виктимология: виктимологическая расшифровка киберпреступности» (2019) профессора К. Джайшанкара, университет Ракша Шакти (университет полиции внутренней безопасности) [10]. Проведены серьезные изыскания по профилированию жертв киберпреступности [11]. В сети Интернет функционируют ресурсы, посвященные отдельным формам кибервиктимизации, в частности «Центр исследования кибербулинга», который ежегодно публикует научные материалы и информационный бюллетень «Киберзапугивание: идентификация, профилактика и ответ» [12]. В США в рамках национального обзора киберпреступности (NCSS) был проведен виктимологический

[2] Генпрокуратура сообщила почти о двукратном росте числа киберпреступлений в РФ в 2018 г. // ТАСС. URL: https://tass.ru/proisshestviya/5733551.

опрос 7 818 юридических лиц на предмет виктимизации в интернет-среде. 67 % опрошенных представителей предприятий назвали как минимум одно киберпреступление, совершенное в отношении их организации[3]. Также вопросы кибервиктимологии изучаются в рамках психиатрии и социальной психологии. В 2017 г. по данным опроса Eurobarometer было проведено аналитическое исследование фобий и страхов перед преступностью в Интернет у лиц с предшествующим опытом виртуальной виктимизации [13]. Все эти и многие другие проблемы весьма актуальны и для отечественной науки.

В рамках описанных вопросов и руководствуясь необходимостью их решения, было проведено эмпирическое исследование по обозначенной теме. Оно проводилось в форме анкетирования. Респондентам было задано 11 вопросов, касающихся опыта использования сети интернет и случаев индивидуальной виктимизации в этой среде. Интернет, как потенциально опасная медиасреда, был выбран неслучайно, поскольку абсолютное большинство подобных случаев происходит именно в глобальной сети и лишь около 3–4 % преступлений — в региональных и локальных (на основе изучения материалов по кибермошенничествам) [14].

Для получения сведений касающихся гендерных различий кибервиктимизации опрошенных разделили по признаку пола. В опросе приняли участие 221 мужчина и 363 женщины.

На вопрос «насколько часто Вы пользуйтесь сетью Интернет?» обе группы дали приблизительно одинаковые ответы. Ежедневно к виртуальной сети подключались 98 % мужчин и 99 % женщин. О случаях передачи персональных данных (реквизитов паспорта или СНИЛС, домашнего адреса, номера телефона и проч.) упомянули 88 % утвердительно ответивших лиц мужского пола и 90 % женского. Анализ предоставления конфиденциальной информации свидетельствует о том, что женщины чаще сообщают ее в он-лайн магазины, при записи в медучреждения, а мужчины — в банки, государственные и иные тематические порталы (см. табл. 1.).

Таблица 1

Структура предоставления конфиденциальной информации в сети Интернет

Ресурс	Мужчины	Женщины
Государственные услуги	72 %	66 %
Банки	6 %	59 %
Он-лайн магазины	43 %	50 %
Запись в медицинские учреждения	29 %	48 %
Бронирование отелей и покупка туристических путевок	14 %	13 %
Сайты перевозчиков	8 %	9 %
Регистрация на различных тематических порталах	20 %	14 %
На сайтах объявлений (Авито, Дром)	45 %	44 %
Свой вариант (ставки на спорт, Али-экспресс, социальные сети)	5 %	4 %

По поводу внимательности и осмотрительности при использовании сетевых ресурсов пользователи высказались следующим образом. На вопрос «Всегда ли Вы следуете предупреждению на экране о том, что сайт небезопасный и его не стоит посещать?» 21 % мужчин и 12 % женщин ответили отрицательно, указав, что игнорируют подобные сообщения. Неукоснительно следуют им лишь каждый пятый мужчина (20 %) и каждая третья женщина (33 %). Более подробно см. рис. 1.

[3] Cybercrime // Bureau of Justise Statistics. URL: https://www.bjs.gov/index.cfm?ty=tp&tid=41.

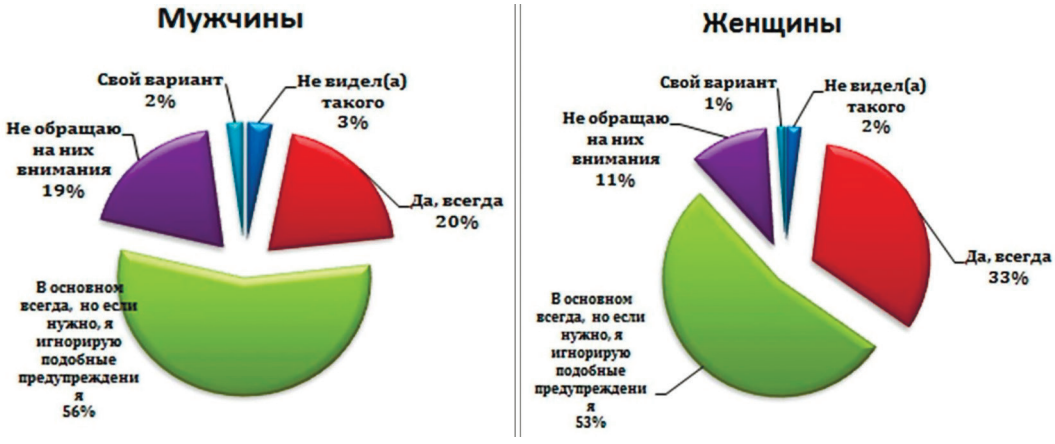

Рис. 1. Посещение небезопасных сайтов мужчинами и женщинами

Исходя из полученных ответов, женщины демонстрируют более высокую дисциплину, чем представители мужского пола и стремление следовать формальным предупреждениям о сетевых угрозах. Несмотря на это, в обеих группах почти половина респондентов (более 54,5 %) указали, что «если нужно перейти на сайт, я игнорирую подобные предупреждения». Более того, оказалось, что женщины менее внимательны к деталям безопасного интернет-серфинга (или не всегда придают им значение). Так, в меньшей степени, они обращают внимание на сертификат подлинности сайта (надпись «https...» или «Защищено» в адресной строке). Если мужчины обычно это делают больше чем в половине случаев (54 %), то женщины — лишь в трети (33 %).

На вопросы касающиеся кибервиктимизации, 94 % опрошенных обоего пола положительно ответили на вопрос, случались ли с ними какие-либо противоправные инциденты в сети. По данным отчетов было выявлено около 15 различных форм виктимизирующих действий (см. ниже табл. 2). При этом особое внимание обращает на себя поливиктимная природа интернет-дискриминации, т.е. каждый пользователь подвергался нескольким видам противоправных воздействий. В среднем мужчины испытывали на себе 3,1 виктимизирующее действие, а женщины — 3,8. Среди видов виктимизирующих действий были названы следующие:

Наибольшее расхождение в гендерной структуре виктимизации было зафиксировано для взлома аккаунта в социальных сетях (6 % у мужчин против 49 % у женщин); установки на компьютер вредоносных программ (14 % против 8 %); оскорблений (20 % против 10 %), непристойных предложений (10 % против 25 %), а также хищений конфиденциальной информации (3 % против 1 %). Таким образом, мужчины чаще становились жертвами хищений паспортных данных (платежных карт), атак программ-вымогателей, вербальной агрессии или обмана недобросовестными продавцами. Женщины с более высокой частотой оказывались потерпевшими от взлома аккаунтов в социальных сетях и сексуально окрашенного киберпреследования.

При этом 62 % мужчин и 64 % женщин отметили, что данные инциденты нанесли им вред. На вопрос «Как Вы оцениваете причиненный ущерб?» были получены следующие ответы (см. рис. 2)

Лица женского пола чаще сообщали о незначительном ущербе до 1 000 р. (43 %) и моральных издержках (30 %). Мужчины о незначительном материальном (28 %), моральном (34 %) вреде, косвенных затратах на восстановление

Таблица 2

Структура виктимизации в сети Интернет

Виктимизирующее действие	Мужчины	Женщины
Взлом почтового ящика или аккаунта в социальных сетях	6 %	49 %
Распространение от моего имени ложной информации	19 %	18 %
Обращение ко мне с просьбами о сборе денег на лечение якобы «больных» детей, похороны родственников и т.п.	42 %	41 %
Просьбы со стороны друзей и одноклассников помочь материально, занять им денег после взлома их аккаунта	59 %	70 %
Просьбы под различными предлогами перейти на зараженные или сомнительные сайты	46 %	57 %
Установка на моем компьютере программы-вымогателя, блокирующего его работу и требующего денег	14 %	8 %
Угрозы распространения в сети Интернет конфиденциальной информации обо мне	4 %	3 %
Услуги явно мошеннического характера, когда товар или услуга не соответствовали заявленным в договоре или отсутствовали	18 %	11 %
Оскорбления, попытки меня унизить	20 %	10 %
Непристойные предложения, сексуальные домогательства и навязчивость, отправка собеседником фотографий в обнаженном виде	10 %	25 %
Хищение конфиденциальной информации (данных платежных карт, паспортные данные и т.п.)	3 %	1 %
Списание со счета телефона средств при смс-подтверждении регистрации на сайте или при скачивании файла	8 %	13 %
Оформление без моего явного согласия платных интернет-подписок или услуг	21 %	24 %
Получение сообщений о выигрыше с просьбой оплатить накладные расходы	47 %	52 %
Свой вариант (предложения работать курьером наркотиков, кражи фото и выдача их за свои, ложное погашение штрафа)	1 %	–

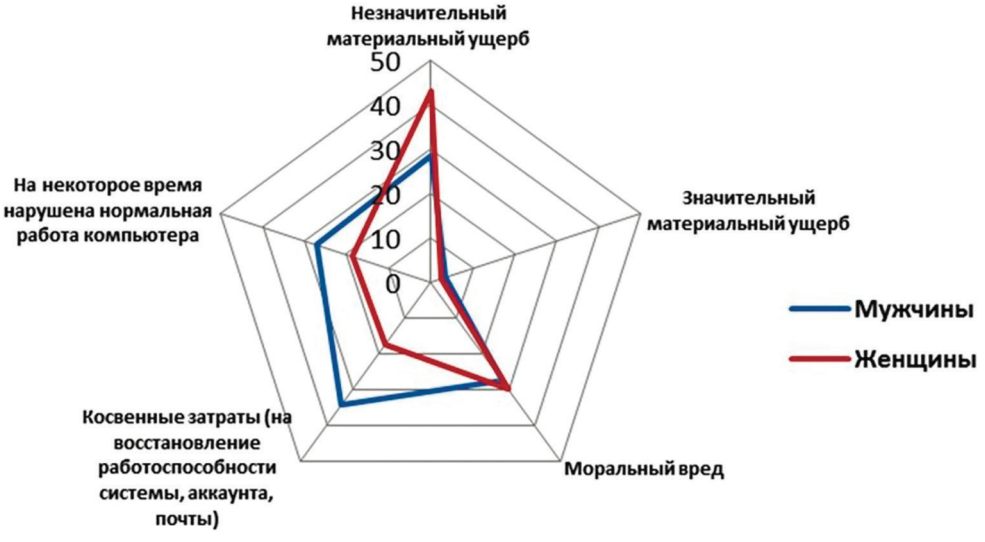

Рис. 2. Оценка ущерба пользователями, нанесенного неправомерными действиями третьих лиц.

компьютера (34 %), а также потерях времени вследствие остановленной работы (27 %). Значительный ущерб, несмотря на малое количество подобных случаев, **почти в два раза чаще причинялся мужчинам.**

По поводу формальных мер, которыми реагировала жертва, заметной гендерной разницы отмечено не было. Представители обоих полов в равной степени предпочитали не обращаться в полицию (заявивших было менее 1 %), разобраться в ситуации самостоятельно (около 70 %) или игнорировать подозрительные письма, ссылки и просьбы (приблизительно 30 %). Правоохранительная практика между тем чаще фиксирует обращения от юридических, нежели физических лиц [15].

В последнюю очередь респондентов попросили составить рейтинг рисков, которые, по их мнению, повышают шанс человека стать жертвой компьютерных преступников. Каждый вид риска было предложено оценить от 1 до 5 баллов в зависимости от степени опасности (где 1 — почти не опасно, а 5 — чрезвычайно опасно). Полученные результаты были сведены в табл. 3.

Таблица 3

Оценка рисков виктимизации в сети Интернет по мнению пользователей

Риски в сети Интернет	Индекс опасности	
	Мужчины	Женщины
Отсутствие необходимых средств защиты (антивирус, файервол и т.п.)	2,8	3,3
В случае собственных неправомерных действий (скачивание пиратского контента, взломанных компьютерных программ и пр.)	2,9	3,3
Использование браузера Tor и посещение Даркнета (темного интернета)	2,2	3,1
Посещение сайтов для взрослых	2,6	3,2
Посещение незнакомых сайтов и переходы по сомнительным ссылкам	3,0	3,4
Некритичное отношение к различного рода рассылкам, письмам с незнакомых адресов	2,8	3,0
В случае осуществления покупок через Интернет	2,0	2,4
Свой вариант (напр., отсутствие двойной аутентификации)	–	–

Представители обеих групп опрошенных согласились, что наиболее виктимной формой поведения является посещение незнакомых сайтов и переходы по сомнительным ссылкам, а наименее виктимной — покупки через Интернет. При этом женщины с большей готовностью оценивали различные риски как опасные и присваивали им более высокие баллы. Мужчины придавали данным рискам меньшее значение и не усматривали в них особой опасности.

Таким образом, проведенное исследование показало, что, как и в обычной жизни, в виртуальном пространстве мужчины чаще демонстрируют рискованное поведение, пренебрежение правилами безопасности и легкомысленное отношение к возможным угрозам. Жертвами в сети Интернет нередко становятся те, кто уже ранее был жертвой в реальной жизни. Вместе с тем, женщины чаще подвергаются виктимизирующему воздействию (на одного пользователя женского пола приходится почти 4 типа дискриминирующих акта, тогда как на индивида мужского пола — в среднем 3). Типы виктимизирующих воздействий также имеют гендерную специфику, к примеру, женщины чаще становятся жертвами домогательств и взлома аккаунтов, а мужчины — потерпевшими от оскорблений и хищения конфиденциальной платежной информации (по данным нашего исследования).

В зарубежной литературе также подчеркивается гендерный аспект кибервиктимности. Так, в «Национальной стратегии кибербезопасности Великобритании» (2016) выделяют 2 вида киберпреступлений: кибер-зависимые (cyber-dependent crimes), совершенные с использованием информационных технологий (распространение вредоносного ПО, кражи персональных данных) и кибер-включенные (cyber-enabled crimes), т.е. общеуголовные преступления, осуществляемые при поддержке новейших коммуникационных достижений[4]. Согласно виктимологическому обзору киберпреступности Лондонской полиции (2016) наиболее серьезный материальный ущерб от кибер-зависимых преступлений наносится именно мужчинам и составляет в среднем 2 355 фунтов стерлингов, что в 3 раза больше, чем ущерб наносимый женщинам[5]. Отчасти эти данные согласуются с полученными нами сведениями.

Результаты исследования свидетельствуют о том, что более 90 % опрошенных становились жертвами киберпреступлений, как правило, нескольких. Если исходить из официальной статистики проникновения Интернет и 74 млн россиян, ежедневно пользующихся сетью[6], цифры пострадавших от киберпреступлений, вероятно, значительно выше, чем их оценивают официально. Данные генеральной прокуратуры (121 тыс. зарегистрированных преступлений на октябрь 2018 г.) занижены в десятки раз. И не исключено, что это оптимистическая оценка. Государство в настоящий момент не имеет представления о действительном положении дел.

В связи с этим, сегодня особо ощущается потребность в детальной разработке важнейших вопросов кибервиктимологии, включающих следующие важные моменты:

– определение ее предметных границ, конкретизация теоретико-методологического поля и ключевых парадигмальных подходов;

– наработка теоретических знаний и эмпирического материала о потерпевших от киберпреступлений (составление профиля личности жертвы; типизация потерпевших для оптимизации следственных действий [16], разработка методики «Шкала виктимного поведения», позволяющей оценить степень кибервиктимности; проведение национального обзора виктимизации населения в сети Интернет);

– разработка комплексной программы профилактики виктимного поведения в киберпространстве.

Кибервиктимология, как теория и метод, вышедший за рамки традиционной виктимологии и криминологии, без сомнения, полемична, но именно она является недостающим звеном дискурса кибердевиантности [17].

[4] Cybercrime — Prosecution Guidance // The Crown Prosecution Service. 2019. 26 Sept. URL: https://www.cps.gov.uk/ legal-guidance/cybercrime-prosecution-guidance.

[5] Cyber Crime — Victimology Analysis // City of London Police. 2016, February. URL: https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology% 20Analysis-latest.pdf.

[6] Интернет в России: динамика проникновения. Зима 2017–2018 гг. // ФОМ. URL: https://fom.ru/posts/13999.

Список использованной литературы

1. Crecente B. Sony Comes Clean: PlayStation Network Hackers Have Stolen Personal Data / B. Crecente // Kotaku. — URL: http://kotaku.com/#!psn/5795913.

2. Hoofnagle Ch.J. Identity Theft: Making the Known Unknowns Known / Ch.J. Hoofnagle // Harvard Journal of Law and Technology. — 2007. — Vol. 21. — P. 97–122.

3. Grimaldi J. Tax and Financial Consideration : Identity Theft / J. Grimaldi. — 2017. — No. 2. — URL: https://www.citrincooperman.com/infocus/identity-theft-tax-and-financial-consideration.

4. Иванов О.Б. Глобальные риски современного мира. Кризис глобализации / О.Б. Иванов // ЭТАП: экономическая теория, анализ, практика. — 2018. — № 1. — С. 7–29.

5. Бархатова Е.Н. Особенности квалификации преступлений, связанных с мошенничеством в сфере высоких технологий : учеб. пособие / Е.Н. Бархатова, В.С. Ишигеев, О.В. Радченко — Иркутск : Изд-во ВСИ МВД России, 2018. — 80 с.

6. Сачков И. Почему IT-преступления остаются безнаказанными / И. Сачков // Секрет фирмы. — 2015. — 7 июля. — URL: https://secretmag.ru/opinions/sachkov.htm.

7. Всестороннее исследование проблемы киберпреступности : проект / С. Малби, Р. Мейс, А. Холтерхоф [и др.]. — Вена, 2013. —360 с.

8. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А. Протасевич, Л.П. Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. — 2011. — № 3. — С. 28–33.

9. Суходолов А.П. Проблемы противодействия преступности в сфере цифровой экономики / А.П. Суходолов, Л.А. Колпакова, Б.А. Спасенников. — DOI: 10.17150/2500-4255.2017.11(2).258-267 // Всероссийский криминологический журнал. — 2017. — Т. 11, № 2. — С. 258–267.

10. Jaishankar K. Cyber Victimology: Decoding Cyber Crime Victimization / K. Jaishankar. — Boca Raton : CRC Press, 2017. — 275 p.

11. Miry-Llinares F. That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime / F. Miry-Llinares // Cybercrime Risks and Responses / ed. R.G. Smith, R.Ch. Cheung, L.Y. Lau. — London : Palgrave Macmillan, 2015. — P. 47–63.

12. Hinduja S. Cyberbullying Identification, Prevention, and Response / S. Hinduja, J.W. Patchin // Cyberbullying Research Center. — 2018. — URL: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2018.pdf.

13. Virtanen S.M. Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities / S.M. Virtanen // Psychiatry, Psychology and Law. — 2017. — Vol. 24, no. 3. — P. 1–16.

14. Коломинов В.В. Мошенничество в сфере компьютерной информации: криминалистический аспект / В.В. Коломинов. — DOI: 10.17150/2072-0904.2015.6(1).26 // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 1. — URL: http://eizvestia.isea.ru/reader/article.aspx?id=19976.

15. Егерева О.А. Некоторые вопросы методики расследования киберпреступлений / О.А. Егерева, В.В. Коломинов, М.С. Сизова // Сибирские уголовно-процессуальные и криминалистические чтения. — 2018. — № 4. — С. 24–32.

16. Смирнова И.Г. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации / И.Г. Смирнова, В.В. Коломинов. — DOI : 10.17150/2072-0904.2015.6(3).27 // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 3. — URL: http://brj-bguep.ru/reader/article.aspx?id=20140.

17. Arntfield M. Towards a Cybervictimology: Cyberbullying, Routine Activities Theory, and the Anti-Sociality of Social Media / M. Arntfield // Canadian Journal of Communication. — 2015. — Vol. 40, no. 3. — P. 371–388.

References

1. Crecente B. Sony Comes Clean: PlayStation Network Hackers Have Stolen Personal Data. *Kotaku*. Available at: http://kotaku.com/#!psn/5795913.

2. Hoofnagle Ch.J. Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law and Technology*, 2007, vol. 21, pp. 97–122.

3. Grimaldi J. *Tax and Financial Consideration : Identity Theft*, 2017, no. 2. Available at: https://www.citrincooperman. com/infocus/identity-theft-tax-and-financial-consideration.

4. Ivanov O.B. Global Risks of the Modern World. The Crisis of Globalization. *ETAP: ekonomicheskaya teoriya, analiz, praktika = ETAP: Economic Theory, Analysis, and Practice*, 2018, no. 1, pp. 7–29. (In Russian).

5. Barkhatova E.N., Ishigeev V.S., Radchenko O.V. *Osobennosti kvalifikatsii prestuplenii, svyazannykh s moshennichestvom v sfere vysokikh tekhnologii* [Peculiarities of Qualification of Crimes Related to Fraud in the Sphere of High Technologies]. Irkutsk, East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation Publ., 2018. 80 p.

6. Sachkov I. Why IT Crimes go Unpunished. *Sekret firmy= Business secret*, 2015, July 7. Available at: https://secretmag.ru/opinions/sachkov.htm.

7. Malbi S., Mesa, R., Holterhoff A., Brown K., Caseros S., E. Ignatenko *Comprehensive Study of the Problem of Cybercrime: project*. Vienna, 2013. 360 p.

8. Protasyevich A.A., Zveryanskaya L.P. Fighting Cybercrimes as an Urgent Task for Contemporary Research. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2011, no. 3, pp. 28–33. (In Russian).

9. Sukhodolov A.P., Kolpakova L.A., Spasennikov B.A. Issues of Counteracting Crimes in the Sphere of Digital Economy. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2017, vol. 11, no. 2, pp. 258–267. DOI: 10.17150/2500-4255.2017.11(2).258-267. (In Russian).

10. Jaishankar K. *Cyber Victimology: Decoding Cyber Crime Victimization*. Boca Raton, CRC Press, 2017. 275 p.

11. Miry-Llinares F. That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime. In Smith R.G., Cheung R.Ch., Lau L.Y. (eds). *Cybercrime Risks and Responses*. London, Palgrave Macmillan, 2015, pp. 47–63.

12. Hinduja S., Patchin J.W. Cyberbullying Identification, Prevention, and Response. *Cyberbullying Research Center*, 2018. Available at: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2018.pdf.

13. Virtanen S.M. Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*, 2017, vol. 24, no. 3, pp. 1–16.

14. Kolominov V.V. Fraud in the field of computer information: criminalistic aspect. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii (Baykalskiy gosudarstvennyy universitet ekonomiki i prava) = Izvestiya of Irkutsk State Economics Academy (Baikal State University of Economics and Law)*, 2015, vol. 6, no. 1. DOI: 10.17150/2072-0904.2015.6(1).26. Available at: http://eizvestia.isea.ru/reader/article.aspx?id=19976. (In Russian).

15. Egereva O.A., Kolominov V.V., Sizova M.S. Some Questions of the Technique of the Investigation of Cyber Crimes. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2018, no. 4, pp. 24–32. (In Russian).

16. Smirnova I.G., Kolominov V.V. Tactical Features of Taking Statements of Criminal Cases in Computer Information Sphere. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii (Baykalskiy gosudarstvennyy universitet ekonomiki i prava) = Izvestiya of Irkutsk State Economics Academy (Baikal State University of Economics and Law)*, 2015, vol. 6, no. 3. DOI: 10.17150/2072-0904.2015.6(3).27. Available at: http://brj-bguep.ru/reader/article.aspx?id=20140. (In Russian).

17. Arntfield M. Towards a Cybervictimology: Cyberbullying, Routine Activities Theory, and the Anti-Sociality of Social Media. *Canadian Journal of Communication*, 2015, vol. 40, no. 3, pp. 371–388.

Информация об авторах

Жмуров Дмитрий Витальевич — кандидат юридических наук, доцент, кафедра уголовного права, криминологии и уголовного процесса, Институт государства и права, Байкальский государственный университет, координатор проекта «Национальная энциклопедическая служба России», Российская Федерация, г. Иркутск, e-mail: zdevraz@ya.ru.

Ключко Римма Николаевна — кандидат юридических наук, доцент, заведующий кафедрой уголовного права, уголовного процесса и криминалистики, Гродненский государственный университет им. Янки Купалы, Республика Беларусь, г. Гродно, e-mail: klrn.grodno@tut.by.

Authors

Dmitry V. Zhmurov — Ph.D. in Law, Associate Professor, Chair of Criminal Law, Criminology and Criminal Procedure, Institute of State and Law, Baikal State University, Coordinator of Project «National Encyclopedic Service of Russia», Irkutsk, Russian Federation, e-mail: zdevraz@ya.ru.

Rimma N. Klyuchko — Ph.D. in Law, Associate Professor, Head of Chair of Criminal Law, Criminal Procedure and Criminalistics, Yanka Kupala Grodno State University, Grodno, Belorussia, e-mail: klrn.grodno@tut.by.

Для цитирования

Жмуров Д.В. Кибервиктимология как новая реальность технотронного общества (гендерное исследование) / Д.В. Жмуров, Р.Н. Ключко. — DOI: 10.17150/2411-6262.2020.11(1).18 // Baikal Research Journal. — 2020. — Т. 11, № 1.

For Citation

Zhmurov D.V., Klyuchko R.N. Cyber-Victimology as a New Reality of the Technotronic Society (Gender Research). *Baikal Research Journal*, 2020, vol. 11, no. 1. DOI: 10.17150/2411-6262.2020.11(1).18. (In Russian).