Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. Т. 24, № 2. С. 85–98.
Pacific Rim: Economics, Politics, Law. 2022. Vol. 24, no. 2. P. 85–98.

ПРАВО

Научная статья
УДК 343.988:343.713-027.44
https://doi.org/10.24866/1813-3274/2022-2/85-98

КИБЕРВИКТИМОЛОГИЯ ВЫМОГАТЕЛЬСТВ В ЦИФРОВОМ ПРОСТРАНСТВЕ*

Дмитрий Витальевич Жмуров
Байкальский государственный университет экономики и права, 664003, Россия, г. Иркутск, ул. Ленина, д. 11, zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X, ABH-8471-2020

Аннотация. В статье рассмотрен вопрос о вымогательстве в сети Интернет. Предложена дефиниция вымогательства как требования о передаче активов, совершении каких-либо действий под угрозой причинения ущерба, предъявляемого в виртуальной среде. В ходе анализа отечественной и зарубежной литературы автором рассматривается современное состояние проблемы, изучаются распространенность и специфика подобных деяний, а также личность потерпевшего от вымогательств. Описаны виктимологические характеристики потерпевшего, такие как криминальная эксцитативность (привлекательность для вымогателя), уязвимость (неспособность оказать эффективное сопротивление), высокие показатели интернет-активности, информационная сопряжённость (связь с информацией, используемой для шантажа). Предложена авторская классификация потерпевших от правонарушений изучаемой категории. В неё входят: 1) контентные жертвы, пострадавшие от реализуемого ими информационного поведения; 2) функциональные жертвы, утратившие контроль над важными техническими процессами или устройствами и желающие его восстановить; 3) жертвы личной безопасности, пострадавшие от шантажа вредоносными действиями и насилием в реальной жизни. Сделан вывод о том, что жертвы цифрового вымогательства – второй по распространенности тип потерпевших после интернет-мошенничества и для них характерен высокий уровень двойной виктимизации (от преступника и от социума).

Ключевые слова: кибервиктимность, кибервиктимология, интернет-потерпевший, жертвы цифровых преступлений, кибержертва, субъект кибервиктимизации, цифровая криминология, пострадавший в интернет-среде, кибервиктимизация, факторы кибервиктимизации, криминология цифрового мира.

Для цитирования: Жмуров Д. В. Кибервиктимология вымогательств в цифровом пространстве // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. Т. 24, №. 2. С. 85–98. https://doi.org/10.24866/1813-3274/2022-2/85-98

.

LAW

Original article

CYBER-VICTIMOLOGY OF EXTORTION IN THE DIGITAL SPACE

Dmitriy V. Zhmurov, Baikal State University, 664003, Russia, Irkutsk, st. Lenina, 11, zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X, ABH-8471-2020

Abstract. This article discusses the issue of extortion on the Internet. It is defined as a requirement of the transfer of assets, the commission of any actions under the threat of causing damage, presented in a virtual environment. During the analysis of domestic and foreign literature, the author examines the current state of the problem, studies the prevalence and specificity of such acts; in addition, the identity of the victim of extortion is studied. Its victimological characteristics are de-scribed, such as criminal excitability (attractiveness to extortionists), vulnerability (inability to provide effective resistance), high rates of Internet activity, information conjugacy (connection with information used for blackmail). The author suggests his own classification of victims of offenses of this category. It includes: 1) content victims affected by the information behavior they implement; 2) functional victims who have lost control over important technical processes and wants to restore it; 3) victims of personal security who have suffered from blackmail by malicious actions and violence in real life. It is concluded that victims of digital extortion are the second most common type of victims after Inter-net fraud and that they are characterized by a high level of double victimization (and from the criminal, and from society).

Keywords: cyber-victimhood, cyber-victimology, internet victim, victims of digital crimes, cyber-victim, subject of cyber-victimization, digital criminology, victim in the internet environment, cyber-victimization, factors of cyber-victimization, criminology of the digital world.

For citation: Zhmurov D. V. Cyber-victimology of extortion in the digital space // Pacific RIM: Economics, Politics, Law. 2022. Vol 24, no 2. P. 85–98. https://doi.org/10.24866/1813-3274/2022-2/85-98

2020-й стал годом локдаунов и тотального карантина из-за коронавируса. А в киберпреступной среде это был год вымогательств. По данным компании Chainalysis, число транзакций жертв кибервымогателей в 2020 г. увеличилось на 311% – до 350 млн долларов (см. рис. 1). Но это лишь верхушка айсберга, а именно переводы людей, согласившихся платить. Ещё больше тех, кто игнорировал вымогателей, терял данные, пытался уладить проблему без выкупа, не обращался в полицию и проч. Если учитывать, что состав вымогательства – формальный, т.е. считается оконченным с момента предъявления незаконных требований, то число подобных преступлений несопоставимо больше, чем зафиксировано.

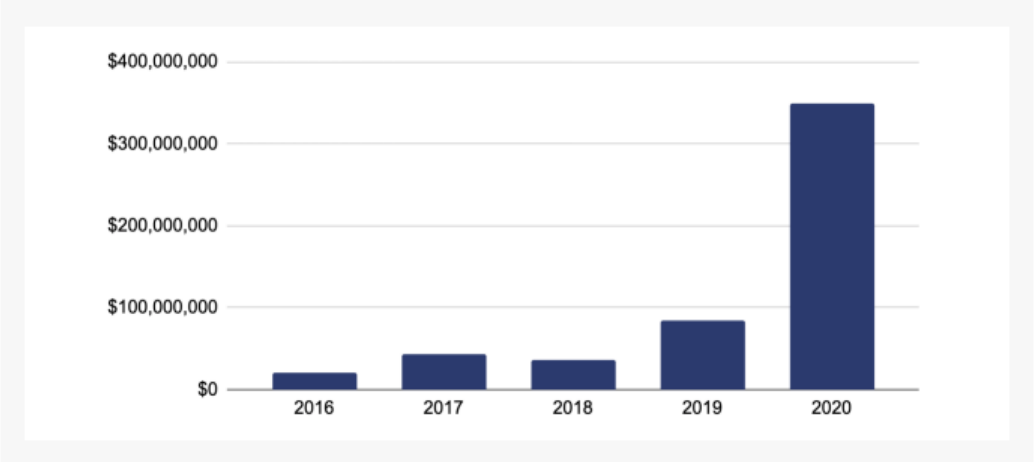

Рис. 1. Число платежей от жертв вымогателей, по данным Chainalysis (в BCH, BTC, ETH, USDT)

В России также происходил рост кибервымогательств: если в 2016 г. официально зарегистрирован 1621 инцидент, то в 2020 г. – уже 2425 (+49,5%) [1].

История вопроса началась в 1989 г. со СПИДа, точнее одноименной вредоносной программы AIDS, которую создал доктор биологических наук Джозефф Попп. Это был первый случай кибервымогательства. Он разослал учёным примерно 20 тыс. дискет с якобы важной информацией о СПИДе. На носителе была программа, которая отсчитывала 90 перезагрузок компьютера, а затем блокировала систему и выводила на печать листок с инструкциями об оплате выкупа в 189 либо 378 долларов на один из панамских почтовых ящиков. Дж. Попп был задержан, од-

нако избежал наказания, поскольку был признан невменяемым. У него была особая идея – выкуп предназначался на финансирование исследований ВИЧ.

После этого случая стали появляться блокировщики экрана, поддельные «антивирусы-попрошайки», но по-настоящему индустрия вымогательств заработала после 2000-х годов, ознаменовавших появление биткоина и популяризацию шифровальных методов. Наивные программы-блокировщики переросли в монстров, способных парализовать целые отрасли экономики, государственного управления и науки [2].

Сегодня *интернет-вымогательство* (кибершантаж, условно-цифровое вымогательство, киберэстракция) – это *предъявляемое в виртуальной среде требование о передаче активов, совершении каких-либо действий под угрозой причинения ущерба*. В России оно не всегда признается преступлением, поскольку ответственность за вымогательство наступает лишь в случае, если противоправные требования предъявляются под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких [3]. Указанные условия, бесспорно, реализуются не всегда.

Кибершантаж превратился в доходный бизнес. Структура рынка вымогательств разнообразна: от серьёзных теневых и серых игроков до случайных преступников-шантажистов, требующих выкуп за неосторожные репосты. Высказывается мнение о том, что вымогательская деятельность, наряду с отмыванием денег, криминальным наркотизмом, организацией проституции и проч., является одним из маркеров распространения организованной преступности [4].

Крупные группировки вымогателей, вероятно, скомпонованы по принципу пирамиды, когда участники (сборщики информации, программисты, шантажисты, «обнальщики») не знают друг о друге. В 2020 г. в интернете было представлено более 10 таких проектов (рис. 2). Известно, что некоторые из них имеют колл-центры, сотрудники которых помогают жертвам разобраться в сложном процессе покупки криптовалюты для выкупа. Другие продают что-то вроде франшизы (RaaS – ransomware as a service) – программы для взлома в обмен на часть выкупа, а также предоставляют услуги на аутсорсе, такие как ведение переговоров с жертвами [5]. Вымогатели средней руки осуществляют свою деятельность на профессиональной основе, но зачастую в региональном масштабе. Они собирают компрометирующую информацию (интимный контент, факты правонарушений жертвы) или создают поводы сами (например, телеканал «*рынок шкур*» шантажирует потенциальных потерпевших публикациями с разоблачением якобы их прошлой жизни [6]; тенденциозные сайты могут представить правопослушных граждан как преступников и коррупционеров). Мелкие вымогатели работают по случайным, единичным целям, как правило не применяют программные методы и не

располагают серьезной медийной поддержкой. Они довольствуются примитивным шантажом в социальных сетях, закрытых чатах, сексуальных стримах и т.п.

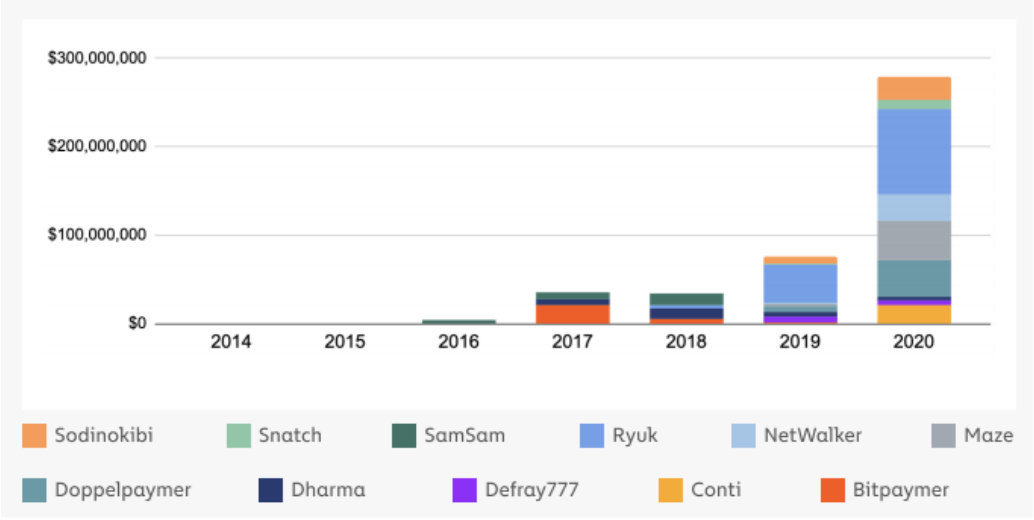

Рис. 2. Доля наиболее успешных программ-вымогателей в сети Интернет

В любом случае *жертва вымогательства – это физическое или юридическое лицо, которому под угрозой предъявлено некое требование*. Известно, что 85% из них предпочитают не обращаться по этому поводу в правоохранительные органы [7].

Основными характеристиками потерпевшего являются:

- *криминальная эксцитативность*, т.е. обладание нужными характеристиками (чаще всего – это платежеспособность, обладание высокой репутацией, а для случаев сексуального вымогательства – половые и гендерные спецификации);

- *уязвимость* – как предполагаемая физическая или моральная слабость [8], невозможность противопоставить вымогателю эффективные стратегии совладания (многие инциденты анонимны, жертве даётся мало времени, имеются признаки трансграничности, т.е. преступники находятся на значительном удалении от пострадавшего или правоохранительных органов его юрисдикции).

- *высокие показатели интернет-активности*;

- *информационная сопряжённость*, которая предполагает генерирование или обладание любой значимой информацией, распространение которой может дискредитировать социальный профиль потерпевшего, его репутацию, осуществляемые бизнес-процессы и т.п.

Чаще всего от жертвы требуется заплатить; значительно реже – произвести сексуальные манипуляции или выполнить иные притязания преступника.

Среди потерпевших от цифрового вымогательства можно выделить следующие группы:

1) *контентные жертвы* (угроза потери репутации, социального статуса, прерывания экономической деятельности), пострадавшие от реализуемого ими информационного поведения, т.е. действий, связанных с производством, получением, передачей и хранением данных. Это лица, шантажируемые содержанием их интернет-активности (мемы, репосты, лайки, переписка, фото- и видеоизображения); пострадавшие из-за утечки информации, не подлежащей разглашению; компании-агрегаторы личных данных и проч.;

2) *функциональные жертвы* (угроза нормальной работе оборудования), утратившие контроль над важными техническими процессами. Они стремятся сохранить работоспособность девайсов и компьютерных систем, обеспечить защиту информации на накопителях. Это и представители крупного бизнеса, и владельцы мобильных телефонов, заблокированных преступниками;

3) *жертвы личной безопасности,* страдающие от шантажа вредоносными действиями и насилием в реальной жизни (угроза сохранению здоровья, имущества, неприкосновенности жилища).

По характеру применяемых вымогателями методов потерпевших можно подразделить на жертв программного (при помощи специализированного ПО) или коммуникативного вымогательства (посредством личного взаимодействия с преступником).

1. Контентные жертвы – это активные субъекты информационного поведения. Самостоятельно или не своей воле они производят некий контент (инфопродукт), который становится интересен вымогателям. Потерпевшие уверены, что в их интересах – не допустить разглашения или максимально быстро удалить эти материалы, желательно без привлечения общественного внимания.

Если говорить о юридических лицах, то вымогателям интересны базы данных (клиенты, транзакции, поставки), коммерческие сведения и ноу-хау, а также всё, что может навредить бизнесу в случае огласки. Компания, которая не сможет выполнить их требования, рискует потерять корпоративные данные. Вдобавок, если нарушение связано с данными клиентов, то организация может быть привлечена к юридической ответственности (например, по законодательству США).

У физических лиц преступники стремятся заполучить самогенерируемые откровенные материалы (SGEM); самогенерируемые непристойные материалы (SGIM); материалы, связанные с педофилией или сексуальным насилием над детьми (CSAM); цифровые следы, свидетельствующие об аморальном или правонарушающем поведении (дискредитирующие жертву). Благо, недостатка в этом не отмечается. Согласно отчёту NetClean, 90% сотрудников, расследующих сексуальное насилие над детьми в интернете, заявили, что самостоятельно созданный ими сексуальный контент можно найти часто или очень часто [9]. Разумеется, это касается не только несовершеннолетних.

Далее жертве сообщается: если она не желает утечки или заявления в полицию, требуется оплата. На практике «предметом» вымогательства могут быть не только денежные средства, но и приобретение товаров, предоставление данных, включая логины и пароли, а также иные требования: расстаться с сексуальным партнёром, вновь стать парой с бывшим возлюбленным [10], не прерывать интимные отношения, осуществить на камеру сексуальные манипуляции [11] и проч.

Частным примером подобного вымогательства является сексторция (сексторшн), когда интимный контент угрожают распространить онлайн, если жертва не выполнит требования. Иногда сексторцией называют мошеннические действия в форме спам-рассылки, убеждающей пользователя, что у недоброжелателей есть компрометирующие его съемки во время посещения порносайтов. Согласно отчёту компании ESET, 11% пользователей сети были объектами таких «сексуальных вымогательств» [12].

Потенциальными жертвами сексторции являются люди, обменивающиеся интимными изображениями (нюдсами, дикпиками), либо фиксирующие половые акты с партнером на видео. Для них характерна повышенная значимость сексуальных стимулов, стремление разнообразить половое поведение (с помощью онлайн знакомств, виртуального секса). В основе их деятельности лежат разные стремления: сделать личную жизнь интереснее, сексуальное новаторство, чувство одиночества или подростковый интерес, а иногда и сексуальные проблемы (комплексы неполноценности, нарциссизм, виртуальный промискуитет). Потенциальные потерпевшие – это молодые люди в возрасте от 15 до 44 лет. По данным паблика VK «Интернет-полиция», возраст реальных жертв составляет от 13 до 25 лет – это наиболее активные и наивные пользователи социальных сетей [13]. Зачастую отправители таких сообщений – женщины и девушки, а мужчины выступают их потребителями [14]. Но с заявлениями в полицию чаще обращаются лица мужского пола [15].

Столь виктимные формы сексуальной коммуникации практикуют многие пользователи интернета. По данным Pew Research Center, среди 25–44-летних американцев 56% практикуют секстинг. В альтернативных исследованиях эта цифра превышает 80% [16]. В России 63% молодых мужчин и женщин хотя бы раз отправляли свои интимные фотографии [17].

Захват контента происходит по-разному: при его добровольной передаче, записи без ведома жертвы, взломе файлового хранилища или почты. Были случаи, когда потерпевшие забывали выйти из почтового аккаунта или сдавали телефон в ремонт [18], а злоумышленники этим пользовались. Д. Тхаккар в монографии «Предотвращение цифрового вымогательства» сообщает, что средняя сумма выкупа за сексторцию составляет приблизительно 500 долларов, хотя бывали случаи, когда суммы достигали десятков миллионов долларов [19].

Как уже упоминалось, контентные жертвы не исчерпываются приведённым выше примером. Ими могут стать любые лица, пострадавшие от нарушения при-

ватности или конфиденциальности хранения данных. Иногда они сами характеризуются негативным поведением: ведут себя аморально, нарушают закон, становятся участниками неоднозначных и одиозных ситуаций.

Укажем несколько вариантов контентного шантажа:

- интимными фотографиями или видео с личным участием;
- перепиской, репостами, мемами;
- принадлежностью к какой-либо группе или сообществу[1];
- обвинением в растлении малолетних или сексуальных домогательствах;
- инкриминированием какого-либо преступления и правонарушения;
- распространением данных коммерческого или иного характера[2].

2. Функциональные жертвы становятся объектами вымогательства по другим причинам. Платя выкуп, они стремятся обезопасить себя от взломов, DDOS-атак, нарушения работы сетевого оборудования, шифрования рабочей информации и т.п. В одном показательном случае преступник угрожал «взорвать» компьютер 13-летней девочки, которая действительно верила, что он может это сделать, и выполняла его эротические прихоти по скайпу [20].

Традиционно функциональные жертвы страдают от «корпоративных вымогательств». Нападкам подвергаются юридические лица – коммерческие, неправительственные и правительственные организации. Чаще это – небольшие компании, но и крупные не застрахованы от этого. 91% малых и средних предприятий в России становятся объектами IT-атак [21]. Большие компании эффективней защищают себя, имеют службы безопасности, а государственный, муниципальный сектор и мелкий бизнес не уделяют этому достаточного внимания. Подобные цели выглядят предпочтительнее: они не могут быстро отреагировать на угрозы, неустойчивы к перебоям в работе, для их взлома не нужно писать оригинальные программы и т.п.

Наиболее популярными отраслями у киберпреступников в 2020 г. были профессиональные услуги – юристов, бухгалтеров, агентств недвижимости и т.д. (34,45%); государственные услуги (17,79%), производство (14,72%). В меньшей степени пострадали здравоохранение (12,13%), технологии (8,89%), финансы (6,89%) [22]. Так, к примеру, в 2019 г. в США жертвами программ-вымогателей стали более 170 муниципальных служб, а суммы запрашиваемого выкупа доходили до нескольких миллионов долларов [2]. Если верить статистике Emsisoft, в 2020 г. хакерам удалось остановить работу 560 медицинских центров, 1 681 школ и колледжей, а также более чем 1 300 иных организаций [23]. Средний чек таких вымогательства отличается по отраслям экономики: в здравоохранении он составляет

[1] Хакерская группа Black Shadow, взломавшая сайт знакомств израильских ЛГБТ «Атраф», требует выплатить выкуп в миллион долларов. В противном случае угрожает опубликовать личные данные пользователей сайта, около миллиона человек, переписку в чатах и проч.

[2] Публикация базы клиентов британского ювелирного дома Graff Diamonds

140 тыс. долл., в финансовой сфере – более 200 тыс. долл., а в секторе технологий, инжиниринга и телекоммуникаций может превысить 1 млн долл. [13]. Порой суммы выкупа доходят до значительных размеров, например, Colonial Pipeline (США) заплатила хакерам 5 млн долл. за восстановление транзита топлива в трубопроводной системе компании [24].

В основном жертвы страдают от нескольких форм вымогательства:

- угрозы атаки «отказ в обслуживании» (DDOS, DOS), предполагающей имитацию большого количества обращений к серверу, которые делают его на какое-то время неработоспособным;

- блокирование рабочих устройств (с ограничением доступа к функционалу компьютера, смартфона или другого оборудования) и платой за восстановление доступа;

- шифрование данных, когда информация на носителе кодируется, а ключ расшифровки находится у вымогателя (утрачивается целостность и идентифицируемость данных).

В конечном счёте, проводимые атаки делают оборудование бесполезным и нефункциональным. Для восстановления его работы, физического доступа или сохранения данных потребуется выкуп. Его сумма в среднем составляет около 170 тыс. долл., тогда как средняя цена самостоятельного восстановления колеблется от 761 тыс. долл. в 2020 г. до 1,8 млн долл. в 2021 г. [22]. Эксперты полагают, что большинство подобных происшествий вызвано халатностью или излишней самоуверенностью сотрудников, отвечающих за информационную безопасность компаний [23].

3. Жертвы личной безопасности подвергаются вымогательству, связанному с угрозой жизни и здоровью, распространению адреса проживания (иных данных), порчи имущества через телекоммуникационную сеть.

Интернет здесь выступает средством связи между сторонами преступления. В судебной практике фиксируются случаи, когда вымогатели обращаются к потерпевшему через социальные сети или почту, отправляя текстовые сообщения с требованием передать денежные средства под угрозой применения насилия [25]. Не исключено, что популярность систем «умный дом» создаст новый повод для вымогателей, которые будут требовать деньги под угрозой вывода из строя Iot-приборов. Ещё одним заметным методом вымогательства является доксинг, т.е. «практика раскрытия идентифицирующей человека информации» (например, его домашнего адреса) в Интернете, чтобы получить от него выкуп [20].

Итак, жертвы цифрового вымогательства – это второй по распространённости тип потерпевших после интернет-мошенничества. Чаще всего – это платёжеспособные субъекты (юридические и физические лица), стеснённые в средствах реагирования и не способные оказать вымогателям адекватное противодействие (техни-

ческое, юридическое и т.п.). Для них характерен высокий уровень двойной виктимизации. С одной стороны, дискриминация и давление, исходящее от преступника, с другой – прессинг общественности с вытекающей ретравматизацией и социальными последствиями шантажа. Ведь риск быть опороченным и потерять репутацию высок чрезвычайно. Таким образом, жертва интернет-вымогательства нередко терпит многократный ущерб, к примеру, оплачивая выкуп, так и не восстанавливает информацию на жёстком диске (если речь о программах-вайперах); выполняя требования вымогателей, не пресекает публикацию интимного видео; может подвергаться штрафным санкциям со стороны государства, если выясняется, что выкуп был заплачен, или в дополнение ко всему компенсирует ущерб третьим лицам (например, клиентам), чьи персональные данные были утрачены от действий вымогателей. В ряде случаев жертвы, поддающиеся вымогательским угрозам, будут страдать от постоянных, повторяющихся требований со стороны преступников – своеобразной психологической ситуации, которая может перерасти в отношения доминирования и подчинения [20].

Список источников

1. Кириленко В. П., Алексеев Г. В. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. Т. 14, № 6. С. 898–913. DOI: 10.17150/2500-4255.2020.14(6).898-913.

2. Grustniy L. Cara о программах-вымогателях. URL: https://www.kaspersky.ru/blog/history-of-ransomware/30373/.

3. Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. Т. 14, № 5. С. 699–709. DOI: 10.17150/2500-4255.2020.14(5).699-709.

4. Номоконов В. А. Борьба с преступными организациями: американский опыт и российские реалии // Криминологический журнал Байкальского государственного университета экономики и права. 2014. № 4. С. 46–53. DOI: 10.17150/1996-7756.2014.8(4).46-53.

5. Monroe R. How to negotiate with Ransomware Hackers. URL: https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.

6. «Рынок шкур»: блогеры жалуются на вымогательство в обмен на репутацию. URL: https://ren.tv/news/v-rossii/453525-rynok-shkur-blogery-zhaluiutsia-na-vymogatelstvo-v-obmen-na-reputatsiiu.

7. Internet Crime Report by Internet crime complaint center IC3, 2016. URL: https://pdf.ic3.gov/2016_IC3Report.pdf.

8. Вымогательство // Википедия. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Вымогательство.

9. Thorn Research: Understanding sexually explicit images, self-produced by children. URL: https://www.thorn.org/blog/thorn-research-understanding-sexually-explicit-images-self-produced-by-children/.

10. Третьяк И. В. Новые виды вымогательства в сети Интернет // Вестник науки. 2018. № 7. С. 95–100.

11. The extortion economy: Inside the shadowy world of Ransomware payouts. URL: https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html.

12. Каждый десятый пользователь в России стал жертвой шантажа во время самоизоляции. URL: https://xakep.ru/2020/06/01/covid-19-sextortion/.

13. Лютых С. Этот жестокий, опасный и безжалостный интернет или как легко стать жертвой вымогателей, орудующих в соцсетях. URL: https://lenta.ru/articles/2015/03/01/shantaz/.

14. Секстинг: зачем люди отправляют друг другу интимные фотографии. URL: https://daily.afisha.ru/relationship/5505-seksting-zachem-lyudi-otpravlyayut-drug-drugu-intimnye-fotografii/.

15. Жертвы «клубничного» шантажа. В Витебской области участились случаи вымогательства в соцсетях. URL: https://vitvesti.by/crime/zhertvy-klubnichnogo-shantazha-v-vitebskoi-oblasti-uchastilis-sluchai-vymogatelstva-v-sotcsetiakh.html.

16. How common is sexting? Over 80 percent of survey respondents report sexting within past year. URL: https://www.sciencedaily.com/releases/2015/08/150808172217.htm.

17. Меня шантажируют интимными фото и видео. Что делать? URL: https://meduza.io/cards/menya-shantazhiruyut-intimnymi-foto-i-video-chto-delat.

18. Обмен приблудностями: как правильно реагировать на шантаж в интернете. URL: https://iz.ru/1238402/mariia-nemtceva/obmen-pribludnostiami-kak-pravilno-reagirovat-na-shantazh-v-internete.

19. Thakkar D. Preventing digital extortion. URL: https://www.packtpub.com/product/preventing-digital-extortion/9781787120365.

20. Vasiu I., Vasiu L. Forms and consequences of the cyber threats and extortion phenomenon // European Journal of Sustainable Development. 2020. Vol. 9 (4). P. 295–302. DOI:10.14207/ejsd.2020.v9n4p295.

21. Practical security guide to prevent cyber extortion. Shopper Software Security in SMBs. Nielsen, April 2015. URL: http://cdvnas04.myqnapcloud.com/media/fileman ager/Cyberextortion_Guide-DE-WEB.pdf.

22. Understanding cyber extortion and how to protect your business. URL: https://www.embroker.com/blog/cyber-extortion/.

23. Банальная халатность: почему вирусы-вымогатели невозможно победить? URL: https://www.gazeta.ru/tech/2021/04/05/13547660/ransomware_strikes.shtml.

24. Оператор крупнейшего трубопровода США заплатил хакерам почти $5 млн выкупа. URL: https://www.forbes.ru/newsroom/biznes/429299-operator-krupneyshego-truboprovoda-ssha-zaplatil-hakeram-pochti-5-mln-vykupa.

25. Овсюков Д. А. Использование информационно-телекоммуникационных сетей при совершении вымогательства // Актуальные проблемы российского права. 2021. № 2 (123). С. 140–145.

References

1. Kirilenko V. P., Alekseev G. V. Harmonization of the Russian criminal legislation on combating cybercrime with the legal standards of the Council of Europe. *Vserossiiskii kriminologicheskii zhurnal*, 2020, vol. 14, no. 6, pp. 898–913. DOI: 10.17150/2500-4255.2020.14(6).898-913. (In Russ.).

2. Grustniy L. Ransomware saga. URL: https://www.kaspersky.ru/blog/history-of-ransomware/30373/. (In Russ.).

3. Rossinskaya E. R., Ryadovsky I. A. The concept of malware as a means of committing computer crimes: classifications and technologies of illegal use. *Vserossiiskii kriminologicheskii zhurnal*, 2020, vol. 14, no. 5, pp. 699–709. DOI: 10.17150/2500-4255.2020.14(5).699-709. (In Russ.).

4. Nomokonov V. A. Fighting criminal organizations: American experience and Russian realities. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava*, 2014, no. 4, pp. 46–53. DOI: 10.17150/1996-7756.2014.8(4).46-53. (In Russ.).

5. Monroe R. How to negotiate with Ransomware Hackers. URL: https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.

6. "Market of skins": bloggers complain about extortion in exchange for reputation. URL: https://ren.tv/news/v-rossii/453525-rynok-shkur-blogery-zhaluiutsia-na-vymogatelstvo-v-obmen-na-reputatsiiu. (In Russ.).

7. Internet Crime Report by Internet crime complaint center IC3, 2016. URL: https://pdf.ic3.gov/2016_IC3Report.pdf.

8. Extortion // Wikipedia. Free encyclopedia. URL: https://ru.wikipedia.org/wiki/Extortion. (In Russ.).

9. Thorn Research: Understanding sexually explicit images, self-produced by children. URL: https://www.thorn.org/blog/thorn-research-understanding-sexually-explicit-images-self-produced-by-children/.

10. Tretyak I. V. New types of extortion on the Internet. *Vestnik nauki*, 2018, no. 7, pp. 95–100. (In Russ.).

11. The extortion economy: Inside the shadowy world of ransomware payouts. URL: https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html.

12. Every tenth user in Russia became a victim of blackmail during self-isolation. URL: https://xakep.ru/2020/06/01/covid-19-sextortion/. (In Russ.).

13. Lyutykh S. This cruel, dangerous and ruthless Internet or how easy it is to become a victim of extortionists operating in social networks. URL: https://lenta.ru/articles/2015/03/01/shantaz/. (In Russ.).

14. Sexting: Why do people send each other intimate photos. URL: https://daily.afisha.ru/relationship/5505-seksting-zachem-lyudi-otpravlyayut-drug-drugu-intimnye-fotografii/. (In Russ.).

15. Victims of "strawberry" blackmail. Cases of extortion in social networks have become more frequent in the Vitebsk region. URL: https://vitvesti.by/crime/zhertvy-klubnichnogo-shantazha-v-vitebskoi-oblasti-uchastilis-sluchai-vymogatelstva-v-sotcsetiakh.html. (In Russ.).

16. How common is sexting? Over 80 percent of survey respondents report sexting within the past year. URL: https://www.sciencedaily.com/releases/2015/08/150808172217.htm.

17. I am being blackmailed with intimate photos and videos. What to do? URL: https://meduza.io/cards/menya-shantazhiruyut-intimnymi-foto-i-video-chto-delat. (In Russ.).

18. The exchange of stray: how to properly respond to blackmail on the Internet. URL: https://iz.ru/1238402/mariia-nemtceva/obmen-pribludnostiami-kak-pravilno-reagirovat-na-shantazh-v-internete. (In Russ.).

19. Thakkar D. Preventing digital extortion. URL: https://www.packtpub.com/product/preventing-digital-extortion/9781787120365.

20. Vasiu I., Vasiu L. Forms and consequences of the cyber threats and extortion phenomenon. *European Journal of Sustainable Development,* 2020, vol. 9 (4), pp. 295–302. DOI:10.14207/ejsd.2020.v9n4p295.

21. Practical security guide to prevent cyber extortion. Shopper Software Security in SMBs. Nielsen, April 2015. URL: http://cdvnas04.myqnapcloud.com/media/ filemanager/Cyberextortion_Guide-DE-WEB.pdf.

22. Understanding cyber extortion and how to protect your business. URL: https://www.embroker.com/blog/cyber-extortion/.

23. Banal negligence: why are ransomware viruses impossible to defeat? URL: https://www.gazeta.ru/tech/2021/04/05/13547660/ransomware_strikes.shtml. (In Russ.).

24. The operator of the largest US pipeline paid hackers almost $5 million in ransom. URL: https://www.forbes.ru/newsroom/biznes/429299-operator-krupneyshego-truboprovoda-ssha-zaplatil-hakeram-pochti-5-mln-vykupa. (In Russ.).

25. Ovsyukov D. A. The use of information and telecommunication networks in the commission of extortion. *Aktual'nye problemy rossiiskogo prava*, 2021, no. 2 (123), pp. 140–145. (In Russ.).

Информация об авторе

Дмитрий Витальевич Жмуров – кандидат юридических наук, доцент кафедры уголовного права и криминологии Байкальского государственного университета экономики и права, руководитель проекта «Национальная энциклопедическая служба России», г. Иркутск, Россия.

Information about the author

Dmitriy Vitalievich Zhmurov – Candidate of Sciences (Law), Associate Professor of the Department of Criminal Law and Criminology of the Baikal State University of Economics and Law; Coordinator of the Project «National Encyclopedic Service of Russia», Irkutsk, Russia.