Advances in Law Studies (2020). Vol. 8. Special issue: 86–93
DOI 10.29039/2409-5087-2020-8-5-86-93

ЦИФРОВЫЕ ТЕХНОЛОГИИ
И ЮРИДИЧЕСКАЯ ПРАКТИКА

Организованная киберпреступность в современных условиях цифровой трансформации социальных отношений

УДК 34(340)

Лобач Дмитрий Владимирович
Кандидат юридических наук, доцент кафедры теории и истории российского и зарубежного права,
Владивостокский государственный университет экономики и сервиса, Институт права; E-mail: dimaved85@mail.ru.

Смирнова Евгения Александровна
Кандидат юридических наук, старший преподаватель кафедры трудового и экологического права,
Дальневосточный федеральный университет, Юридическая школа; E-mail: smirnova.ea@dvfu.ru.

Статья получена: 17.03.2020. Рассмотрена: 14.04.2020. Одобрена: 19.05.2020. Опубликована онлайн: 04.06.2020.

Работа выполнена при финансовой поддержке Гранта Президента РФ № НШ-2668-2020.6 «Национально-культурные и цифровые тренды социально-экономического и политико-правового развития Российской Федерации в XXI веке».

Аннотация. В статье исследуется феномен организованной киберпреступности в современных условиях цифровой трансформации социальных отношений. Авторы отмечают, что несмотря на отсутствие в правовой науке и в практической сфере единообразного понимания организованной киберпреступности (organised cybercrime), что, соответственно, предопределяет проблему концептуализации организованной преступности в киберпространстве, все-таки представляется возможным выделить и проанализировать характерные особенности данного явления в условиях цифровой трансформации социальных отношений.

Ключевые слова: социальная трансформация социальных отношений, цифровизация, киберпреступность, киберугрозы, преступность, организованная преступность, цифровые риски, информационно-коммуникационные технологии

В условиях интенсивного развития сквозных (дизруптивных) информационно-коммуникативных технологий (ИКТ) и их широкой интеграции в различных сферах жизни общества происходит качественное изменение социальных отношений, которое выражается в появлении новых институциональных форм взаимодействия, цифровизации целых сегментов социальной организации и публичной власти, трансформации ценностных ориентиров, что в конечном счете приводит к амбивалентным последствиям. С одной стороны, интегративное использование ИКТ повышает эффективность

ORGANIZED CYBERCRIME IN MODERN CONDITIONS OF DIGITAL TRANSFORMATION OF SOCIAL RELATIONS

Lobach Dmitry Vladimirovich
PhD in Law, Associate Professor of the Department of Theory and History of Russian and Foreign Law, Vladivostok State University of Economics and Service, Institute of Law; E-mail: dimaved85@mail.ru.
Smirnova Evgeniya Aleksandrovna
PhD in Law, Senior Lecturer at the Department of Labor and Environmental Law, Far Eastern Federal University, Law School; E-mail: smirnova.ea@dvfu.ru.
Manuscript received: 17.03.2020. Revised: 14.04.2020. Accepted: 19.05.2020. Published online: 04.06.2020.
This work was financially supported by the Russian Federation Presidential Grant No. НШ-2668-2020.6 "National-Cultural and Digital Trends in the Socio-Economic, Political and Legal Development of the Russian Federation in the 21st Century".
Abstract. The article examines the phenomenon of organized cybercrime in modern conditions of digital transformation of social relations. The authors note that despite the lack of a uniform understanding of organized cybercrime in legal science and in practice, which, accordingly, determines the problem of conceptualization of organized crime in cyberspace, it is still possible to identify and analyze the characteristic features of this phenomenon in the context of digital transformation of social relations.
Keywords: social transformation of social relations, digitalization, cybercrime, cyber threats, crime, organized crime, digital risks, information and communication technologies

управления, снижает риски наступления неблагоприятных последствий, уменьшает трансакционные издержки и способствует консолидации социальных структур в информационном пространстве в решении актуальных проблем. В этом аспекте справедливо отмечается, что в современных условиях создается цифровое общество, сопровождаемое глубокими и качественными преобразованиями, которые захватывают все отрасли экономики (промышленность, сельское хозяйство, торговлю, сферу услуг), также разные сферы жизни человека (личную, семейную, общественную) [5, с. 25]. Кроме того, наблюдается рост интеллектуально-волевых возможностей (познавательный потенциал) относительно переработки информации посредством использования ИКТ в различных сферах деятельности, что порождает изменение структуры мыслительной деятельности [4, с. 17–33]. С другой стороны, быстрое развитие и широкое распространение ИКТ также предопределяет новые и нарождающиеся угрозы в отношении собственности, жизни и здоровья человека, публичных интересов общества и государства. Одной из таких угроз, актуализированных в условиях так называемой четвертой промышленной революции, выступает киберпреступность. О высокой общественной опасности данной угрозы свидетельствует следующая репрезентативная картина киберпреступности по состоянию на 2019 г., составленная на основании открытых информационных источников.

Прежде всего необходимо отметить, что за период 2009–2018 гг. наблюдается экспоненциальный рост количества заражений вредоносным программным обеспечением. Так, если в 2009 г. было зарегистрировано 12,4 млн инцидентов, то уже в 2010 г. — 29,97 млн, в 2011 г. — 48,17 млн, в 2012 г. — 82,62 млн, в 2013 г. — 165,81 млн, в 2014 г. — 308,96 млн, в 2015 г. — 452,93 млн, в 2016 г. — 580,40 млн, в 2017 г. — 702,06 млн и в 2018 г. было зарегистрировано 812,67 млн соответствующих фактов заражения [24]. В целом темпы прироста за указанный десятилетний период составили около 6553%.

В соответствии с экспертными оценками, представленными разными организациями, осуществляющими мониторинг кибербезопасности в мире, по состоянию на 2020 г. 59% компаний в США и Великобритании сообщили о нарушениях компьютерной безопасности со стороны третьих лиц, при этом в 35% случаев было отмечено, что управление рисками со стороны третьих лиц были высокоэффективными. Нарушения конфиденциальности данных увеличились с 2006 по 2019 г. на 160%. Наблюдается тенденция совершения хакерских атак на малый бизнес (43% кибератак направлены на учреждения малого бизнеса). Ежедневно производится 230 000 новых образцов вредоносного программного обеспечения, и в ближайшей перспективе их количество будет увеличиваться [14]. Хакерские атаки становятся всё более сложными и опасными, из-за чего компаниям часто требуется более шести месяцев для обнаружения утечки данных [23]. По данным Федерального бюро расследований более 4000 кибератак, связанных с вымогательством, происходят каждый день, а общая оценка ущерба, связанного с этими атаками, составляет 11,5 млрд долларов по состоянию на 2019 г. [19]. Экономические подсчеты, связанные с ущербом и издержками, которые, возможно, возникнут в результате совершения кибератак на объекты критической инфраструктуры, показывают, что в ближайшее время кибератаки могут привести к убыткам до 3 трлн долларов, в то время как восстановительные работы, проводимые после совершения киберпреступлений, оцениваются от 375 до 575 млрд долларов в год. По оценкам Центра исследования риска им. Ллойда и Кембриджского университета, отключение электроэнергии из-за кибератаки на электрические сети США обойдется государству в сумму от 243 млрд до 1 трлн долларов США, а также окажет значительное влияние на смертность, а Центр стратегических и международных исследований оценил вероятные ежегодные затраты по восстановлению и ремонту поврежденных от кибертерроризма систем и убытки от экономического шпионажа в масштабах мировой экономики в размере более 445 млрд долларов [15, с. 265–266].

Сложившаяся ситуация в области кибербезопасности, характеризуемая количественными (в части увеличения общего количества атак)

[20] и качественными факторами (в части эволюционирующего хакерского инструментария), угрожающими состоянию безопасности информационных систем, предполагает постановку вопроса о возможном организационном усложнении киберпреступности до уровня организованной криминальной кооперации в киберпространстве, что, соответственно, предполагает выработку оптимального концепта «организованная киберпреступность» (organised cybercrime), так как понятийная характеристика данного явления поможет представить масштабы угрозы (правда, в релевантном фокусе), которую несет это явление, пути и тенденции развития этого явления, а также детерминистский комплекс, обусловливающий возникновение и существование организованной киберпреступности как специфического проявления более широкого феномена, каким выступает транснациональная организованная преступность.

Прежде всего необходимо отметить, что концептуально-правовое раскрытие данного феномена немыслимо без определения киберпреступности как родового понятия. Несмотря на то, что в системе международного уголовного права всё еще не принята единая (универсальная) конвенция о киберпреступности, хотя необходимость в таковой уже давно назрела, понятие киберпреступности становится возможным вывести из анализа трех региональных конвенций, составляющих конвенционный механизм противодействия компьютерным преступлениям.

В первую очередь необходимо отметить Конвенцию Совета Европы «О преступности в сфере компьютерной информации» (ETS № 185) от 23 ноября 2001 г. [8]. В рамках данного документа все компьютерные преступления подразделяются на четыре группы: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (в частности, противозаконный доступ; неправомерный перехват; воздействие на данные; воздействие на функционирование системы; противозаконное использование устройств); преступления, связанные с использованием компьютерных средств (в частности, подлог с использованием компьютерных технологий; мошенничество с использованием компьютерных технологий); преступления, связанные с содержанием данных, в частности, противоправные деяния, связанные с детской порнографией; правонарушения, связанные с нарушением авторского права и смежных прав.

В более широком диапазоне преступления против компьютерной информации находят свое отражение в Конвенции Африканского Союза «О кибербезопасности и защите персональных данных» от 27 июня 2014 г. [7]. По смыслу данной конвенции к киберпреступлениям были отнесены атаки на компьютерные системы (шесть составов преступлений); атаки на компьютерную информацию (шесть составов преступлений); преступления, связанные с содержанием компьютерной информации (восемь составов преступлений, связанных главным образом с детской порнографией и экстремизмом); преступления, связанные с электронными сообщениями; имущественные преступления, совершаемые через использование информационно-коммуникационных технологий (четыре состава преступлений).

В крайне усеченном варианте представлены компьютерные преступления в Соглашении о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 2001 г. В соответствии со ст. 3 соглашения к компьютерным преступлениям относятся совершенные умышленно следующие деяния: а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; б) создание, использование или распространение вредоносных программ; в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия; г) незаконное использование программ для ЭВМ и баз данных,

являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

В срезе традиционного криминологического понимания преступности и с учетом положений вышеуказанных конвенций киберпреступность можно определить как исторически изменчивое социальное и уголовно-правовое негативное явление, представляющее собой всю совокупность преступлений в сфере информационных технологий, посягающих на безопасность информационных систем и угрожающих конфиденциальности, целостности и доступности компьютерных данных и систем, здоровью населения и общественной нравственности, а также общественным отношениям, возникающим в связи с осуществлением правомочий собственника и в сфере реализации авторских и смежных прав, совершенных в информационно-коммуникационном пространстве в определенный период времени. В свою очередь обобщение доктринальных позиций относительно выработки определения организованной преступности [3, с. 25; 10, с. 37–41; 11, с. 61–90; 1, с. 24–31; 21; 18, с. 63–83] в контекстуальной привязке к предложенному выше понятию киберпреступности позволяет сформулировать концептуальное определение организованной киберпреступности как негативное социальное явление, представляющее собой организованную преступную деятельность в киберпространстве, которая проявляется в совершении множества преступлений в сфере информационных технологий (киберпреступлений) на криминально-профессиональной основе в целях получения прямых или косвенных финансовых или материальных выгод лицами, объединенным в организованные, законспирированные преступные формирования сетевого характера . Справедливости ради также следует признать, что данное определение никоим образом не может претендовать на универсальность, так как в правовой науке и практической сфере отсутствует единообразное понимание организованной киберпреступности (organised cybercrime), а различные дискурсивные аспекты повествования о данном явлении предопределяют проблему концептуализации организованной преступности в киберпространстве [22, с. 289]. Поэтому, отказываясь в целом от механической экстраполяции признаков релевантного определения организованной преступности на криминальную деятельность, осуществляемую в киберпространстве, представляется возможным и целесообразным охарактеризовать особенности организованной киберпреступности в современных условиях с учетом специфики криминальной кооперации в интернет-пространстве.

Во-первых, проявление организованной преступности в киберпространстве связано с возникновением новых криминальных рынков. В специальной литературе и ведомственных отчетах неоднократно отмечалось, что разработки в области информационных технологий, а именно использование криптовалют, программного обеспечения для шифрования и защитных браузеров (например, The Onion Router), способствуют развитию так называемых теневых веб-рынков в сокрытой части Интернета (даркнет) [26, с. 347]. Организованную криминальную деятельность в даркнете, связанную с расширением теневых веб-рынков, можно проиллюстрировать на примере двух таких торговых площадок, как AlphaBay и Silk Road, которые осуществляли торговые операции относительно незаконных товаров и услуг (например, наркотики, краденные банковские карты, поддельные документы, средства хакерских атак, оружие и др.). Торговую площадку AlphaBay использовали в различных целях более 400 000 подписчиков [17], а ежедневный оборот от торговых операций оценивался от 600 000 до 800 000 долларов [16]. Анализ деятельности площадки Silk Road за два с половиной года ее существования позволил американским правоохранительным органам оценить оборот денежных средств в зависимости от курса биткоина на общую сумму от 200 млн до 1,2 млрд долларов [12, с. 180–181]. Общий доход от этих продаж составил 9 519 664 биткоинов, и общая комиссия, собранная Silk Road от продаж, составила 614 305 биткоинов. За указанный период было совершено около 1 229 465 транзакций на сайте с участием 146 946 счетов покупателей и 3877 учетных записей поставщиков [25].

Во-вторых, организованная киберпреступность представляет собой сложную многоэтапную деятельность, ориентированную на обогащение. Осуществление современных кибератак предполагает длительный, поэтапный процесс достижения преступной цели, что обусловливает необходимость распределения функциональных ролей и согласования общей стратегии преступной кооперации. В сущности, кибератака (целевая атака) представляет собой непрерывный процесс несанкционированной активности в инфраструктуре атакуемой системы, удаленно управляемый в реальном времени вручную и ориентированный на преодоление конкретных механизмов безопасности [2].

В этом плане необходимо отличать спонтанно создаваемые небольшие законспирированные группы пользователей Интернета (сообщества педофилов, самоубийц, экстремистов), занимающиеся противоправной деятельностью без ориентации на извлечение прибыли, от устойчивых, сложных сетевых форм криминальной кооперации, которые стремятся к получению прямых или косвенных материальных или финансовых выгод.

Сложный характер организованной криминальной деятельности выражается в поэтапном совершении операциональных действий в модели общего алгоритма при ролевой и функциональной дифференциации прилагаемых усилий. Проиллюстрировать сказанное можно на примере анализа современных кибератак, совершаемых в условиях сетевого сговора в целях обогащения.

В первую очередь кибератака начинается с разведывательной деятельности (стадия разведки). Данная стадия предполагает выбор компании-жертвы, оценку ее системы информационной безопасности, поиск неизвестных уязвимостей в системе организации, применение методов социальной инженерии в целях составления «троянского» письма.

На втором этапе происходит разработка и выбор оптимального с позиции оценки поставленной задачи и прогнозируемых мер противодействия инструментариям предстоящей кибератаки. Современные средства проведения кибератак охватывают внушительный диапазон различных зловредных программных средств, среди которых прежде всего следует отметить фишинг (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя), троян (тип вредоносных программ, основной целью которых является вредоносное воздействие по отношению к компьютерной системе), DDoS-атака (поток ложных запросов, который пытается блокировать выбранный ресурс либо путем атаки на канал связи, который забивается огромной массой бесполезных данных, либо атакой непосредственно на сервер, обслуживающий данный ресурс), ботнет (сам компьютер с вредоносным программным обеспечением, дающим возможность злоумышленнику выполнять некие действия с использованием ресурсов зараженного ПК), бэкдор (программа или набор программ, которые устанавливает взломщик (хакер) на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе), червь (тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных систем, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, осуществлению иного вредоносного воздействия), вирус-вымогатель (программы-вымогатели представляют проблему для предприятий, образовательных учреждений и системы здравоохранения), вредоносная программа (компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы), руткин (программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы) [6].

Третий этап кибератаки охватывает проникновение зловредных программных средств в сеть организации. Эта стадия во многом коррелирует с первым этапом, так как в большинстве случаев проникновение происходит посредством распространения «троянского» письма через со-

трудника организации, который ранее на стадии разведки был предельно подробно изучен (используя методы социальной инженерии выявляются его функциональные задачи, информационные предпочтения и досуговые увлечения). Троянские письма, как правило, содержат вложения (документы, архивы, списки) или же ссылки к скрытой вредоносной программе.

Четвертый этап предполагает взлом системы посредством активирования вредоносной программы и установления последующего контроля над нею. Вредоносная программа начинает собирать информацию о системных характеристиках и программном обеспечении зараженного компьютера. При этом несанкционированное присутствие может продолжаться длительное время.

На заключительном этапе происходит непосредственное причинение вреда и сокрытие следов противоправной деятельности. Причинение вреда, как правило, выражается в материальном (например, хищение денежных средств или криптовалюты, вывод из строя объектов инфраструктуры, упущенная выгода), информационном (копирование конфиденциальных данных) или репутационном ущербе (снижение рейтинга компании, вызванное недоверием со стороны потребителей). В отдельных случаях несанкционированное проникновение в систему может и не сопровождаться наступлением какого-либо ущерба. Данные ситуации становятся возможными, когда такое проникновение осуществляется ради праздного любопытства, в целях проверки надежности взламываемой системы или чтобы прославиться.

В-третьих, организованная киберпреступность представляет собой сложный анонимный конгломерат социальных связей при широкой ролевой и функциональной дифференциации. При этом ролевая и функциональная дифференциация при общей координации в преступной деятельности заключается в распределении обязанностей и полномочий среди участников преступного сговора в зависимости от определенного этапа (стадии) криминальной деятельности. Вместе с тем усложнение функционального содержания современных кибератак предполагает объединение различных лиц, обладающих необходимыми знаниями и навыками в области программирования, на основании их специализации, что предполагает подразделение хакеров по видам специализации. Например, выделяют кракеров (лица, занимающиеся взломом прикладного программного обеспечения в целях дальнейшей его эксплуатации), вирусописателей (лица, занимающиеся созданием вредоносных программ и кодов), спамеров (лица, которые занимаются рассылкой бесполезных электронных писем), кардеров (лица, занимающиеся нелегальным получением номеров кредитных карт и сведений об их владельцах), фрикеров (лица, осуществляющие взлом телефонной сети для того, чтобы в дальнейшем осуществлять бесплатные телефонные звонки).

В дальнейшем, если кибератака возымела успех, то возникает потребность в обналичивании денежных средств, в связи с чем в преступную деятельность вовлекаются посредники (так называемые мулы), которые за определенное вознаграждение берут на себя риски перемещения этих средств до обозначенного места. В случае, если полученные средства не используются в дальнейшей криминальной деятельности, то актуализируется потребность в их легализации, а как следствие — привлекаются специалисты в этой сфере.

В-четвертых, учитывая тот факт, что противоправная деятельность осуществляется в интернет-пространстве, которое априори является коммуникационной средой, где происходят перманентные процессы трансграничного оборота информации, закономерно сделать допущение о транснациональном характере рассматриваемого явления.

Транснациональный характер преступной деятельности нормативно определен в Конвенции Организации Объединенных Наций против транснациональной организованной преступности от 15 ноября 2000 г. [9]. Ч. 2 ст. 3 этого документа закрепляет, что транснациональный характер преступления определяется через одну из следующих ситуаций: преступление совершено в более чем одном государстве; преступление совершено в одном государстве, но существенная часть его подготовки, планирования, руководства или контроля имеет место в другом государстве; преступление совершено в одном го-

сударстве, но при участии организованной преступной группы, которая осуществляет преступную деятельность в более чем одном государстве; преступление совершено в одном государстве, но его существенные последствия имеют место в другом государстве.

В-пятых, обязательным условием для идентификации организованной киберпреступности является ее сетевой характер. Киберпреступления представляют собой криминальные акты, которые совершаются посредством компьютерных систем или сетей, а также в самих системах или сетях либо в отношении этих объектов. Кроме того, сетевой характер киберпреступности означает особую модель сетевой организации хакеров, функциональное взаимодействие между которыми осуществляется на горизонтальной основе при общей координации.

В заключение следует отметить, что интенсификация киберпреступности, а также ее организационно-функциональное усложнение во многом обусловлены появлением и опережающим развитием информационно-коммуникационных технологий, активным их внедрением в системы публичного управления и социального взаимодействия [13]. Киберпреступность перестает быть экзотической девиацией со стороны энтузиастов, обладающих особыми знаниями и необходимыми навыками в области программирования, как это было ранее, напротив, преступления в сфере информационных технологий теперь совершаются как организованное предприятие по извлечению сверхприбылей в интернет-пространстве. Если первоначально хакерство, как девиантное поведение в информационном пространстве, осуществлялось людьми, которые направляли свои усилия не только на достижение противоправных целей, но также и на освоение чего-то нового (например, выявление в системе мест уязвимостей, проба своих сил, изучение алгоритмов безопасности), то в современных условиях за преступными действиями стоит организованный криминальный бизнес.

Литература

1. Абадинский Г. Организованная преступность. Пер. с англ. — СПб.: Издательство С-Петербургского университета, 2002. — 688 с.
2. Анатомия таргетированной атаки [Электронный ресурс]. — URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/.
3. Годунов И.В. Организованная преступность от расцвета до заката: Учебное пособие для вузов. —2-е изд., расш. — М.: Академический Проспект, 2008. — 613 с.
4. Гриншкун В.В. Развитие интегративных подходов к созданию средств информатизации образования: дисс. ... д-ра пед. наук: 13.00.02: защищена 18.02.2005. — М., 2004. — 554 с.
5. Катасонов В.Ю. Цифровые финансы. Криптовалюты и электронная экономика. Свобода или концлагерь? — М.: Книжный мир, 2017. — 320 с. — Серия «Финансовые хроники профессора Катасонова».
6. Кибератаки [Электронный ресурс]. — URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8.
7. Конвенция Африканского Союза «О кибербезопасности и защите персональных данных» (Малабо, 27 июня 2014 г.) [Электронный ресурс]. — URL: https://www.sbs.ox.ac.uk/cybersecurity capacity/system/files/African%20Union%20Convention%20on%20CyberSecurity%20%26%20Personal%20Data%20Protection_1.pdf.
8. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. — URL: https://base.garant.ru/4089723/.
9. Конвенция Организации Объединенных Наций против транснациональной организованной преступности от 15 ноября 2000 г. [Электронный ресурс]. — URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml.
10. Попов В.И. Противодействие организованной преступности, коррупции, терроризму в России и за рубежом. — М.: Изд-во СГУ, 2007. — 581 с.
11. Топильская Е.В. Организованная преступность. — СПб.: Издательство «Юридический центр Пресс», 1999. — 256 с.
12. Уэйнрайт Т. Narconomics: Преступный синдикат как успешная бизнес-модель / Пер. с англ. Г. Михайлова. — М.: Изд-во «Пальмира», 2018. — 271 с.
13. Цифровая безопасность личности, общества и государства в условиях глобализации: юридические механизмы обеспечения. Обзор сессии в рамках ПМЮФ 2019 г. / А.И. Овчинников, О.В. Ахрамеева, С.А. Воронцов и др. // Вестник юридического факультета Южного федерального университета. — 2019. — № 2. — С. 111–122.
14. 24 Cybersecurity statistics that matter in 2019. URL: https://preyproject.com/blog/en/24-cybersecurity-statistics-that-matter-in-2019/.
15. Akhgar B., Brewster B. Combatting Cybercrime and Cyberterrorism. *Challenges, Trends and Priorities. Springer International Publishing Switzerland*. 2016, 325 p.
16. AlphaBay, Biggest Online Drug Bazaar, Goes Dark, and Questions Swirl. URL: https://www.nytimes.com/2017/07/06/business/dealbook/alphabay-online-drug-bazaar-goes-dark.html.
17. Cimpanu C. *AlphaBay Dark Web Market Taken Down After Law Enforcement Raids*. URL: https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/.
18. Finckenauer J.O. Problems of definition: What is organized crime? *Trends in Organized Crime*. 2005, no. 8(3), pp. 63–83.
19. Global Ransomware Damage Costs Predicted To Exceed $8 Billion In 2018. URL: https://cybersecurityventures.com/

global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/.
20. Internet crime report, 2019. URL: https://pdf.ic3.gov/2019_IC3Report.pdf.
21. Lebeta S.G. Defining organized crime: a comparative analysis : diss... doctor of law, 2012.
22. Leukfeldt E.R., Lavorgna A., Kleemans E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *Eur J Crim Policy Res*. 2017, no. 23, pp. 287–300.
23. Most companies take over six months to detect data breaches. URL: https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/.
24. The Ultimate List Of Cyber Security Statistics For 2019. Looking for the latest cyber security stats and trends? We've got you covered. URL: https://purplesec.us/resources/cyber-security-statistics/.
25. The complaint published when Ulbricht. *The Internet Archive*. URL: https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf.
26. Weber J., Kruisbergen E.W. Criminal markets: the dark web, money laundering and counterstrategies — An overview of the 10th Research Conference on Organized Crime. *Trends in Organized Crime*. 2019, no. 22, pp. 346–356.

References

1. Abadinsky G. *Organized crime. Translation from English*. St. Petersburg: Publishing House of St. Petersburg University, 2002. 688 p.
2. Anatomy of a targeted attack. Kaspersky. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/.
3. Godunov I.V. *Organized crime from the heyday to the sunset*: a Textbook for universities. 2nd ed., extended. Moscow: Akademicheskiy Prospekt, 2008. 613 p.
4. Grynshkun V.V. *Development of integrative approaches to the creation of means of Informatization of education*: Diss. ... doctor of pedagogical Sciences: 13.00.02: protected 18 February 2005. Moscow, 2004. 554 p.
5. Katasonov V.Yu. *Digital Finance. Cryptocurrencies and the electronic economy. Freedom or concentration camp? Series "Financial Chronicles of Professor Katasonov"*. Moscow: Knizhny Mir, 2017. 320 p.
6. Cyberattacks. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8.
7. African Union Convention on cybersecurity and personal data protection (adopted Malabo, 27 June 2014). University of Oxford. URL: https://www.sbs.ox.ac.uk/cybersecurity capacity/system/files/African%20Union%20Convention%20on%20CyberSecurity%20%26%20Personal%20Data%20Protection_1.pdf.
8. Convention on crime in sphere of computer information. ETS, no. 185 (adopted Budapest, 23 November 2001). URL: https://base.garant.ru/4089723/.
9. United Nations Convention against transnational organized crime of 15 November 2000. *UN official web site*. URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml.
10. Popov V.I. *Counteraction to organized crime, corruption, and terrorism in Russia and abroad*. Moscow: SSU Publishing house, 2007. 581 p.
11. Topilskaya E.V. *Organized crime*. St. Petersburg: publishing house "Legal center Press", 1999. 256 p.
12. Wainwright T. *Narconomics: the Criminal syndicate as a successful business model*. Translated from the English by G. Mikhailov. Moscow: Palmyra Publishing house, 2018. 271 p.
13. Digital security of the individual, society and state in the context globalization: legal mechanisms of ensuring. Review of the session in the framework of SPIEF 2019. A.I. Ovchinnikov, O.V. Akhrameeva, S.A. Vorontsov et al. *Bulletin of the faculty of law of the southern Federal University*. 2019, no. 2, pp. 111–122.
14. 24 Cybersecurity statistics that matter in 2019. URL: https://preyproject.com/blog/en/24-cybersecurity-statistics-that-matter-in-2019/.
15. Akhgar B., Brewster B. Combatting Cybercrime and Cyberterrorism. *Challenges, Trends and Priorities. Springer International Publishing Switzerland*. 2016, 325 p.
16. AlphaBay, Biggest Online Drug Bazaar, Goes Dark, and Questions Swirl. URL: https://www.nytimes.com/2017/07/06/business/dealbook/alphabay-online-drug-bazaar-goes-dark.html.
17. Cimpanu C. *AlphaBay Dark Web Market Taken Down After Law Enforcement Raids*. URL: https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/.
18. Finckenauer J.O. Problems of definition: What is organized crime? *Trends in Organized Crime*. 2005, no. 8(3), pp. 63–83.
19. Global Ransomware Damage Costs Predicted To Exceed $8 Billion In 2018. URL: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/.
20. Internet crime report, 2019. URL: https://pdf.ic3.gov/2019_IC3Report.pdf.
21. Lebeta S.G. Defining organized crime: a comparative analysis : diss... doctor of law, 2012.
22. Leukfeldt E.R., Lavorgna A., Kleemans E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *Eur J Crim Policy Res*. 2017, no. 23, pp. 287–300.
23. Most companies take over six months to detect data breaches. URL: https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/.
24. The Ultimate List Of Cyber Security Statistics For 2019. Looking for the latest cyber security stats and trends? We've got you covered. URL: https://purplesec.us/resources/cyber-security-statistics/.
25. The complaint published when Ulbricht. *The Internet Archive*. URL: https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf.
26. Weber J., Kruisbergen E.W. Criminal markets: the dark web, money laundering and counterstrategies — An overview of the 10th Research Conference on Organized Crime. *Trends in Organized Crime*. 2019, no. 22, pp. 346–356.