Вестник Томского государственного университета. Право. 2024. № 54. С. 33–46
Tomsk State University Journal of Law. 2024. 54. pp. 33–46

Научная статья
УДК 343.97
doi: 10.17223/22253513/54/3

Латентность информационной преступности и пути противодействия ей

Александр Александрович Гребеньков[1]

[1] *Юго-Западный государственный университет, Курск, Россия, grebenkov@gmail.com*

Аннотация. Информационная преступность характеризуется гиперлатентностью: лишь крайне небольшая доля совершённых деяний находит отражение в уголовной статистике. Раскрываются основные наиболее актуальные угрозы, связанные с совершением информационных преступлений, характеризуются причины их латентности. Предлагаются меры, направленные на снижение латентности. Указывается на необходимость декриминализации малоопасных посягательств в информационной сфере.

Ключевые слова: уголовная статистика, вредоносные программы, кибервымогательство

Для цитирования: Гребеньков А.А. Латентность информационной преступности и пути противодействия ей // Вестник Томского государственного университета. Право. 2024. № 54. С. 33–46. doi: 10.17223/22253513/54/3

Original article
doi: 10.17223/22253513/54/3

Latency of information crime and ways to counter it

Alexander A. Grebenkov[1]

[1] *Southwestern State University (Kursk, Russian Federation, grebenkov@gmail.com*

Abstract. The article is devoted to the study of the problem of latency of information crimes, i.e. such acts, in the mechanism of which the use of information technologies and information and telecommunication networks plays a significant role. This type of crime is characterised by hyperlatency: only a very small proportion of committed acts are reflected in criminal statistics, and often the most 'convenient' for disclosure and investigation acts are registered, rather than the most dangerous ones.

The author considers the latency of information offences on the example of two types of offences: 'traditional' computer crimes (unlawful access to computer information, use and distribution of malware) and infringement of copyright and related rights. It summarises data on the scale of cybercrime, its cross-border nature and the amount of damage associated with it. The main threats associated with these types of offences are highlighted. These include, in particular, cyber espionage, cyber sabotage, disclosure of confidential data, attacks on critical information infrastructure, including process control systems, and cyber extortion. Such reasons for their latency are characterised as the use by criminals of the latest technologies to conceal their activities, the

abnormally large role of the non-governmental sector in countering crime, the conflicting interests of victims, and deficiencies in legal regulation. The existence of mass forms of criminal activity is noted, which may involve network communities with a number of members that precludes the possibility of bringing them all to criminal responsibility.

In connection with the above, measures aimed at reducing latency are proposed, in particular, increasing the competence of law enforcement agencies whose tasks include combating information crime. This could be achieved by establishing special investigative jurisdiction and jurisdiction over these offences. It may also be necessary to organise the activities of monitoring services that identify and analyse newly emerging threats to Russia's information security and transfer materials to law enforcement agencies for the initiation of criminal proceedings. It seems expedient to encourage responsible business behaviour in the field of countering common threats to information security, and to establish legal sanctions related to the concealment of information incidents. It is pointed out that it is necessary to decriminalise offences in the information sphere that do not pose a great public danger and to reorient law enforcement agencies to fight the most dangerous manifestations of information crime.

Keywords: criminal statistics, malware, cyber extortion

For citation: Grebenkov, A.A. (2024) Latency of information crime and ways to counter it. *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo – Tomsk State University Journal of Law.* 54. pp. 33–46. (In Russian). doi: 10.17223/22253513/54/3

Одной из важных характеристик преступности является её латентность. Латентная преступность – это фактически совершённые преступления, которые по тем или иным причинам остаются скрытыми от правоохранительных органов или незарегистрированными ими. Отдельными авторами в понятие латентной преступности включаются также преступления, зарегистрированные, но не раскрытые правоохранительными органами, т.е. такие, по которым не выявлено совершившее их лицо [1].

Как отмечает С.М. Иншаков, изучение латентной преступности – ключевая, системообразующая проблема, решение которой может вывести криминологические исследования на новый уровень [2]. Это суждение вполне обоснованно, так как без изучения этой «тёмной стороны» преступности наше представление о данном явлении будет неполным, а применяемые меры борьбы будут рассчитаны лишь на его поверхностные проявления, в то время как «подводная» часть айсберга преступности окажется вне сферы криминологического воздействия. Кроме того, латентными часто оказываются преступления, совершённые наиболее опасными категориями преступников, такими как криминальные профессионалы, а также преступления, совершение которых готовилось наиболее тщательно, в которые вложен максимальный объем интеллектуальных и иных усилий [3]. Латентизация преступности за счёт развития организованных и профессиональных её проявлений, а также её следствия в виде развития правового нигилизма, снижения доверия к правоохранительным органам и падения уровня профессионального правосознания их сотрудников играет существенную роль в механизме самодетерминации преступности [4]. Не имея сведений о действительной структуре преступности, правоохранительные органы не могут

определить действительно приоритетные направления борьбы с ней [5], а уголовная политика государства не может быть сориентирована правильным образом [6].

В теории криминологии традиционно латентность делится на искусственную и естественную. Первая обусловлена неправомерными действиями правоохранительных органов, которые уклоняются от регистрации и расследования преступлений по тем или иным причинам, начиная с ложно понимаемых интересов службы в связи с необходимостью достижения определённых статистических показателей и заканчивая корыстными мотивами коррупционного характера. Вторую обычно связывают с действиями преступников, стремящимися скрыть факт совершения преступления, либо потерпевших, не сообщающих в правоохранительные органы о данном факте (из-за страха мести со стороны преступников, неверия в возможности правоохранительных органов или в силу иных причин).

Информационная преступность (под которой мы понимаем систему преступных деяний, в механизме которых существенную роль играет использование информационных технологий и информационно-телекоммуникационных сетей) является видом преступности, показатели латентности которого являются одними из самых высоких, причем речь идёт как о естественной, так и о искусственной латентности. По оценкам С.М. Иншакова, скрытая часть общей преступности составляет 5/6, т.е. на одно зарегистрированное преступление приходится пять незарегистрированных [7]. В случае с информационными преступлениями эта часть намного выше. Ещё в 2001 г., по данным ФБР, жертвы сообщали в правоохранительные органы лишь об 1% компьютерных преступлений [8]. И это данные, относящиеся ещё к «классическому» этапу развития киберпреступности, когда она ещё не стала явлением, с которым приходится сталкиваться во всех сферах общественной жизни. Для отдельных категорий информационных преступлений в современный период показатели латентности могут быть значительно выше. Так, по нашим данным, основанным на анализе открытой статистики скачиваний на «пиратских» Bittorrent-трекерах, число фактов незаконного использования такого объекта авторских прав, как программное обеспечение стоимостью более 100 тысяч рублей, на несколько порядков (в 1 000–10 000 раз) превышает число зарегистрированных преступлений, ответственность за которые предусмотрена ч. 2 и 3 ст. 146 УК РФ [9].

Как отмечает В.В. Лунеев, латентизация преступности является проблемой не только для отдельно взятых государств, но и всего мирового сообщества [10. С. 280]. Это особенно верно для информационных преступлений, которые из-за использования глобальных компьютерных сетей практически всегда носят транснациональный характер и затрагивают интересы сразу нескольких государств. Кроме того, именно информационные преступления вытесняют традиционные общеуголовные преступления в рамках общей тенденции «переформатирования» преступности, в результате чего снижается общая эффективность работы правоохранительных органов, десятилетиями разрабатывавшими методики работы с насильственными и

корыстными преступлениями [11]. В результате основная тяжесть борьбы с киберпреступлениями перекладывается на плечи их жертв, которые вынуждены тратить значительные суммы на мероприятия по кибербезопасности. Отмечается, что повышение эффективности деятельности правоохранительных органов по борьбе с киберпреступностью могло бы сэкономить суммы, исчисляющиеся в глобальном масштабе миллиардами долларов [12].

Основной особенностью современной характеристики преступлений, связанных с неправомерным доступом к компьютерной информации, использованием и распространением вредоносных компьютерных программ («традиционной» компьютерной преступности), является её организованный и профессиональный характер. Если в исследованиях компьютерной преступности конца 1990-х – начала 2000-х гг. типичным было изображение лица, совершающего компьютерные преступления, как «хакера-одиночки», использующего свои обширные знания в области информационных технологий в исследовательских или хулиганских целях, то в настоящее время такая характеристика во многом утратила свою актуальность. Наибольшая угроза в настоящее время исходит от законспирированных организованных групп и преступных сообществ, совершающих компьютерные преступления в массовых масштабах и практически исключительно в корыстных целях, что определяет особенности их латентности [13].

Посягательства на компьютерную информацию отличаются исключительно масштабным характером. От деятельности преступника страдает не 1–2 потерпевших, а сотни тысяч и даже миллионы пользователей компьютеров во всём мире [14]. Ущерб от киберпреступлений в глобальном масштабе достиг сумм в несколько триллионов долларов [15]. Организованные группы, совершающие такие преступления, часто общаются между собой только посредством глобальных информационно-телекоммуникационных сетей, при этом члены группы могут находиться в разных странах. Сами преступления при этом могут совершаться на значительном расстоянии, в том числе с выходом за пределы национальных границ государств [16].

«Компьютерные преступления» могут преследовать такую цель, как кибершпионаж, кибердиверсии, а также получение доступа к электронной переписке должностных лиц государства и её публикации с целью дискредитации их лично и политики государства в целом (примером может служить взлом электронного почтового ящика заместителя председателя Правительства РФ А.В. Дворковича в июле 2014 г. [17], а также многочисленные «утечки» непубличной информации государственных органов в 2022–2023 гг. в связи с действиями враждебных государств).

Одной из желанных целей атаки киберпреступников являются системы автоматизированного управления технологическими процессами (АСУ ТП) и иные компьютерные системы, используемые для управления индустриальными машинами и механизмами. В современных условиях никакое производство не обходится без таких систем. Более того, электронные системы управления распространяются повсеместно и используются, например, в автомобилях и бытовой технике. Нетрудно представить, насколько опасной

может быть утрата водителем контроля над автомобилем, движущемся на большой скорости, вследствие атаки на его компьютерную систему, однако возможный вред от этого меркнет по сравнению с возможными последствиями атаки на АСУ ТП, контролирующую атомную электростанцию, трубопроводную систему, горнодобывающее оборудование, медицинское оборудование или военные системы. Естественно, что подобные системы являются желанными целями для атаки кибертеррористов и прочих враждебных субъектов, включая спецслужбы иностранных государств.

Разумеется, случайное попадание вредоносного программного обеспечения в такие системы вряд ли возможно, так как они достаточно хорошо защищены, прежде всего, тем, что не подключены к глобальным сетям, используют специализированное программное обеспечение для предотвращения атак и обслуживаются квалифицированным персоналом. Однако угроза направленных атак на такие системы является вполне реальной и давно перестала быть лишь теоретической. Так, в 2010 г. программное обеспечение Stuxnet было использовано для нанесения вреда ядерной программе Ирана [18, 19]. В декабре 2015 г. программа BlackEnergy3 была использована для атаки на энергогенерирующую систему Ивано-Франковска (Украина) [20]. В мае 2021 г. из-за кибератаки прекратил работу трубопровод Colonial Pipeline, из-за чего нарушилось снабжение нефтью Восточного побережья США.

Общее мнение специалистов сходится в том, что данные атаки не были действиями преступников-одиночек или даже каких-то относительно маломасштабных преступных групп. Сложность данных программ говорит о том, что они были созданы большими коллективами хорошо подготовленных и финансируемых разработчиков. Так, в отношении Stuxnet считается, что заказчиками его разработки выступили спецслужбы США и Израиля [21].

Одной из получивших распространение в последние годы угроз, связанных с использованием вредоносного программного обеспечения, является кибервымогательство с использованием криптографических средств. Преступники применяютпрограммы, блокирующие информацию на атакуемом компьютере, с использованием «сильных» алгоритмов шифрования, и требуют от жертвы перечисления определённой суммы (как правило, криптовалюты, такой как Bitcoin) за предоставление ключа расшифровки. Такие атаки являются чрезвычайно прибыльными и представляют угрозу прежде всего для коммерческих организаций всех уровней [22].

В частности, в мае 2017 г. масштабная атака такого типа с использованием вредоносной программы, получившей известность под названием WannaCry, затронула значительное количество компьютеров в 150 странах мира, в том числе в России, причём подвержены заражению оказались сети банковских структур, операторов связи, правоохранительных органов [23]. В этом случае предполагаемыми «авторами» атаки стали преступники из Юго-Восточной Азии, возможно, пользующиеся поддержкой государствен-

ных структур [24], а для проникновения на целевые компьютеры были использованы уязвимости, раскрытые в ходе утечки конфиденциальной информации разведывательных спецслужб США [25].

Основной причиной латентности данного типа информационной преступности является то, что преступники используют в своей деятельности новейшие технические средства, такие как нераскрытые уязвимости программного обеспечения, анонимизирующие компьютерные сети (Tor, I2P и прочие), проводят операции с денежными средствами в криптовалютах, что затрудняет их отслеживание. Также основными «игроками» здесь являются хорошо организованные и законспирированные преступные сообщества, связь между членами которых осуществляется практически исключительно с использованием защищённых средств коммуникации, использующих методы криптографии и стеганографии. Всё это позволяет преступникам в течение длительного времени осуществлять свою деятельность фактически вне поля зрения правоохранительных органов.

Для эффективного противодействия данной категории информационной преступности необходим крайне высокий уровень подготовки, характерный для специалистов в области информационных технологий, специализирующихся в области информационной безопасности, а не для правоохранителей, имеющих в первую очередь юридическую подготовку. Неудивительно, что значительную роль в борьбе с данными преступными проявлениями стали играть частные игроки, такие как подразделения безопасности наиболее крупных IT-корпораций, в частности Microsoft. Государственные правоохранительные органы здесь оказываются на вторых ролях, что вызывает у специалистов определённую обеспокоенность [26]. В частности, борьба с подобными преступными проявлениями практически невозможна без использования технических средств и методов, аналогичных используемых преступниками, а также осуществления мероприятий, сходных по своему содержанию с оперативно-розыскными. Такая деятельность в сфере информационной безопасности практически не урегулирована нормами права, не контролируется государственными органами. Её субъекты осуществляют сотрудничество с правоохранительными органами, но его нельзя назвать полноценным. Так, разработчики антивирусного и иного программного обеспечения, обеспечивающего информационную безопасность, накапливают огромные массивы данных о случаях кибератак и используемом преступниками вредоносном программном обеспечении, однако отсутствуют какие-либо правовые нормы, обязывающие их передавать данные сведения государственным правоохранительным органам. В результате последние вынуждены действовать в условиях неполноты информации о текущем состоянии преступности в сфере информационных технологий.

Здесь следует отметить, что не следует перекладывать всю вину за такое положение вещей на частные компании, осуществляющие деятельность в сфере информационной безопасности. Первично здесь всё же то, что правоохранительные органы оказались не готовы к взрывному росту преступных проявлений в информационной сфере, у них отсутствовало (и продолжает в

значительной мере отсутствовать) правовое, материально-техническое и кадровое обеспечение для такой борьбы. Именно это позволило частным игрокам занять такое положение в сфере обеспечения информационной безопасности. Однако эта ситуация является ненормальной, и следует предпринимать меры для того, чтобы негосударственные субъекты в сфере борьбы с информационной преступностью выступали в роли помощников правоохранительных органов, а не их заместителей.

Существенным фактором латентности здесь также является то, что потерпевшие от информационных атак далеко не всегда обращаются в правоохранительные органы с заявлениями о совершённых в их отношении преступлении. С одной стороны, это связано с неверием в то, что правоохранительные органы способны выявить виновных и привлечь их к ответственности. Однако немаловажное значение имеет также убеждённость многих потерпевших в том, что расследование инцидента повлечёт репутационные и иные издержки, так как вскроет недостатки в обеспечении информационной безопасности. Кроме того, необходимо будет предоставить следственным и экспертным органам доступ к информационным системам, что может повлечь «попутное» выявление нарушений уже со стороны самих потерпевших (например, использования нелицензионного программного обеспечения или финансовых махинаций). В итоге информация о совершённом преступлении направляется в негосударственные организации, оказывающие услуги в области информационной безопасности, иногда даже становится достоянием СМИ, но не правоохранительных органов, которые, казалось бы, должны играть главную роль в деле борьбы с информационной преступностью. Возбуждение уголовного дела и, соответственно, учёт преступления в уголовной статистике в такой ситуации возможны только при условии явно выраженной инициативы со стороны прокурора или руководителя следственного органа, которые полномочны в соответствии со ст. 144 УПК РФ инициировать проверку сообщения о преступлении, опубликованного в СМИ.

Немного иная ситуация складывается в сфере борьбы с нарушением авторских и смежных прав на цифровые объекты, в том числе программное обеспечение. Как показывает изучение судебной практики, большинство уголовных дел возбуждается в отношении системных администраторов (как являющихся штатными сотрудниками организаций, так и работающими в так называемых службах компьютерной помощи), осуществивших установку на компьютер некоторых видов программного обеспечения, авторские права на которое принадлежат определённому небольшому числу компаний (Adobe, Autodesk, Microsoft, 1С). В то же время совершенно очевидно, что данные нарушения составляют крайне небольшую долю от общей массы случаев незаконного использования цифровых объектов авторских и смежных прав.

В отличие от хорошо законспирированных преступников, совершающих преступления, связанные с неправомерным доступом к компьютерной информации и использованием и распространением вредоносных компьютерных программ в качестве постоянного источника дохода, большинство

нарушителей авторских прав действуют практически не скрываясь, осуществляя распространение соответствующих произведений через открытые для всеобщего доступа интернет-сайты, такие как файлообменники и торрент-трекеры. При этом практически не применяются технические средства, затрудняющие выявление и изобличение правонарушителей: для распространения объектов авторских прав используются домашние и рабочие компьютеры и обычное подключение к Интернету, что позволяет легко установить нарушителя, установив его IP-адрес и зафиксировав время подключения. В результате в ряде государств сложилась практика борьбы с подобными нарушителями в порядке их самостоятельного выявления правообладателями и их представителями с последующим урегулированием данного вопроса в досудебном порядке или в ходе судебного разбирательства по гражданско-правовому иску.

Большинство подобных нарушений не являются значительными по своему объёму и совершаются не с целью прямого извлечения материальной выгоды, однако достаточно существенной, как упоминалось выше, является доля посягательств, которые формально являются уголовно-противоправными. Сюда можно отнести, в частности, распространение программного обеспечения, стоимость лицензии на которое превышает 100 тысяч рублей: распространение медиапродукции, экземпляры которой недоступны для приобретения потребителями (например, фильмы до их выхода в прокат), а также распространение инструментов для преодоления технических средств защиты авторских прав, которые многими специалистами рассматриваются как вредоносные программы. Практически все такие посягательства можно отнести к латентным, поскольку они не зарегистрированы и не учтены в статистических данных. Однако речь идёт о таком количестве деяний, в которых формально имеются признаки состава преступления, что вряд ли можно говорить о полноценной возможности их полной регистрации, не говоря уже об осуществлении уголовного преследования и привлечения к уголовной ответственности виновных.

Здесь можно говорить о том, что основными причинами латентности выступают недоработки законодательно-правового и доктринального характера. Во-первых, многие составы информационных преступлений с высокой латентностью не имеют своим признаком последствия в виде причинения какого-либо существенного вреда либо иные обстоятельства, определяющие их общественную опасность. В результате подлежащими учёту оказываются даже незначительные инциденты, не причинившие какого-либо выраженного ущерба общественным отношениям. Кроме того, правоохранительные органы оказываются ориентированы на борьбу не с наиболее опасными проявлениями информационной преступности, а с теми, которые легче раскрыть, что приводит к искажению статистики за счёт искусственного повышения в ней доли малоопасных посягательств. Как верно указывает А.Л. Осипенко, крайне нежелательна криминализация деяний, которые не несут реальной повышенной опасности [27].

Во-вторых, ни в законодательстве, ни в доктрине уголовного права не предусмотрено эффективных средств противодействия преступным деяниям массового характера, в которых используются сетевые средства координации преступной деятельности большого числа участников. Впервые данное обстоятельство заявило о себе ещё в 1990-е гг., когда возникла необходимость противостоять деятельности финансовых пирамид. Правоохранительная система оказалась не в состоянии эффективно расследовать дела с огромным количеством потерпевших и эпизодов преступной деятельности, что привело к тому, что очень многие организаторы такой деятельности остались безнаказанными, а те из них, которых удалось привлечь к ответственности, получили относительно небольшие наказания. Ещё более актуальной является разработка данной проблематики в настоящее время, когда Интернет и социальные сети позволяют организовать деятельность значительного числа лиц, каждое из которых вносит относительно небольшой вклад в общий результат, который суммарно оказывается весьма опасен для общества.

Обобщая изложенное, среди причин латентности информационных преступлений, помимо общих, характерных для всех категорий преступных деяний, можно выделить следующее:

1) использование преступниками новейших информационных технологий для конспирирования своих действий;

2) перехват инициативы в борьбе с преступными проявлениями, связанными с использованием информационных технологий, частными компаниями, осуществляющими деятельность в сфере информационной безопасности;

3) склонность потерпевших скрывать инциденты в области информационной безопасности вследствие неверия в эффективность действий государственных правоохранительных органов, а также в связи с репутационными издержками и стремлением избежать внимания правоохранительных органов к собственной деятельности;

4) недостатки правового регулирования, затрудняющие борьбу с рядом проявлений киберпреступности.

На этой основе можно выдвинуть следующие предложения, направленные на снижение уровня латентности информационных преступлений и, как результат, повышение эффективности борьбы с ними:

1. Связанные с повышением значимости правоохранительных органов в сфере борьбы с посягательствами в информационной сфере и увеличением уровня их компетентности.

В этой части необходимым, в первую очередь, является повышение уровня компетентности правоохранительных органов, осуществляющих раскрытие и расследование информационных преступлений, улучшение показателей работы судебной системы. В настоящее время предварительное расследование по большинству таких преступлений осуществляют подразделения, относящиеся к ведению МВД РФ, а рассмотрение дел происходит

в районных судах. Обеспечить должный уровень компетентности их должностных лиц, особенно если речь идёт о регионах, крайне затруднительно. Ввиду этого представляется желательным передать расследование информационных преступлений Следственному комитету РФ, а судебное рассмотрение соответствующих дел – в подсудность областным судам как наиболее компетентным. Кроме этого, необходимо обеспечить их комплектование сотрудниками, имеющими спецподготовку в области информационной безопасности.

Для противодействия наиболее опасным угрозам в сфере информационной безопасности следует организовать деятельность мониторинговых служб в рамках правоохранительных органов, в чьи задачи будет входить анализ текущих угроз (в том числе по материалам, публикуемым в средствах массовой информации и Интернете) и координация деятельности правоохранительных органов по борьбе с ними, в том числе путём предоставления информации, необходимой для возбуждения уголовных дел и осуществления их расследования.

Следует также обеспечить ответственное поведение бизнеса в области противодействия общим угрозам информационной безопасности. Это касается как частных компаний, осуществляющих деятельность в данной сфере, которым следует в обязательном порядке осуществлять сотрудничество с правоохранительными органами, так и иных компаний, скрывающих информацию о факте информационного преступления. В частности, могло бы оказаться полезным введение административной ответственности юридических лиц в виде крупных штрафов или административного приостановления деятельности (для компаний, занимающихся обеспечением информационной безопасности) за несообщение ставшей им известной достоверной информации о преступлениях в информационной сфере, а также лицах, их совершивших.

2. Направленные на коррекцию подхода к криминализации деяний в информационной сфере и переориентацию на борьбу с наиболее опасными их проявлениями.

В первую очередь, следует признать необходимой декриминализацию наименее опасных посягательств в информационной сфере. В качестве ориентира можно принять, что в криминализации нуждаются деяния, последствием которых выступило причинение существенного материального ущерба, либо наступление иных тяжких последствий, в том числе разглашение информации, образующей охраняемую законом тайну, персональных данных или иных сведений конфиденциального характера, либо совершённые в целях извлечения дохода в значительном размере. Это позволит ориентировать правоохранительную систему на использование средств уголовной репрессии в отношении наиболее опасных преступных посягательств в информационной сфере, а также исключит из состава латентной преступности значительное число не столь опасных правонарушений, что обеспечит более адекватное отражение информационной преступности в уголовной

статистике и, как следствие, повысит научную обоснованность и эффективность мер борьбы с ней.

Необходимы также разработки теоретического характера, направленные на развитие научных представлений о преступных действиях массового характера, в которые вовлечено значительное число участвующих лиц.

Делатентизация информационной преступности должна стать важной составляющей мер, направленных на борьбу с ней, эффективное ведение которой немыслимо в условиях, когда государственные правоохранительные структуры не обладают всей полнотой информации и вынуждены полагаться больше на экспертные оценки, чем на объективные данные.

Список источников

1. Клейменов М.П. Нераскрытая и латентная преступность: различия и сходство // Правоприменение. 2017. № 1. С. 106–113.

2. Иншаков С.М. Латентная преступность как объект исследования // Криминология: вчера, сегодня, завтра. 2009. № 16. С. 107–130.

3. Иванова Е.О. Латентная преступность: понятие и критерии классификации // Современное право. 2015. № 5. С. 119–123.

4. Легостаев С.В. Прогнозирование и предупреждение латентной преступности // Человек: преступление и наказание. 2016. № 3. С. 110–114.

5. Иншаков С.М. Гносеологические проблемы исследования латентной преступности // Russian Journal of Economics and Law. 2010. № 1 (13). С. 136–142.

6. Jewkes Y., Yar M. Policing cybercrime: emerging trends and future challenges // Handbook of Policing / ed. by T. Newborn. London ; New York : Routledge, 2008. P. 580–606.

7. Иншаков С.М. Латентная преступность как показатель эффективности уголовной политики // Российский следователь. 2008. № 14. С. 20–21.

8. Goodman M. Making computer crime count // FBI Law Enforcement Bulletin. 2001. Vol. 70, № 8. P. 10–17.

9. Гребеньков А.А. Нарушения авторского права с использованием технологии BitTorrent: проблемы уголовной ответственности // Уголовное право: стратегия развития в XXI веке : материалы Восьмой Междуна. науч.-практ. конф., 27–28 января 2011 г. М. : Проспект, 2011. С. 376–380.

10. Лунеев В.В. Преступность XX века: мировые, региональные и российские тенденции. М. : Волтерс Клувер, 2005. 912 с.

11. Квашис В.Е. Сравнительный анализ латентной преступности в России и зарубежных странах: проблемы и перспективы // Журнал законодательства и сравнительного правоведения. 2016. № 5. С. 89–93.

12. Hyman P. Cybercrime: it's serious, but exactly how serious? // Communications of the ACM. 2013. Vol. 56, Is. 3. P. 18–20.

13. Осипенко А.Л., Соловьев В.С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. № 6. С. 681–691.

14. Гребеньков А.А. Преступность в сфере высоких технологий в России: приоритеты борьбы // Известия Юго-Западного государственного университета. 2014. № 3. С. 72–77.

15. Ефремова И.А., Смушкин А.Б., Донченко А.Г., Матушкин П.А. Киберпространство как новая среда преступности // Вестник Томского государственного университета. 2021. № 472. С. 248–256.

16. Клишков В.Б., Стебенева Е.В., Яковлева М.А. Киберпреступность: понятие, признаки, основные направления противодействия // Вестник ННГУ. 2022. № 4. С. 106–114.

17. Карпюк И. Взлом Дворковича // Полит.Ру. 22.07.2014. URL: http://polit.ru/article/2014/07/22/dvorkovich (дата обращения: 14.02.2023).

18. Bencsáth B. et al. The Cousins of Stuxnet: Duqu, Flame, and Gauss // Future Internet. 2012. Vol. 4, Is. 4. P. 971–1003.

19. Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon // IEEE Security & Privacy. 2011. Vol. 9, № 3. P. 49–51.

20. Piggin R. Cyber security trends: What should keep CEOs awake at night // International Journal of Critical Infrastructure Protection. 2016. Vol. 13. P. 36–38.

21. Chen T. M., Abu-Nimeh S. Lessons from Stuxnet // Computer. 2011. Vol. 44, Is. 4. P. 91–93.

22. Simmonds M. How businesses can navigate the growing tide of ransomware attacks // Computer Fraud & Security. 2017. Is. 3. P. 9–12.

23. Ehrenfeld J.M. WannaCry, Cybersecurity and Health Information Technology: A Time to Act // Journal of Medical Systems. 2017. Vol. 41, № 7. P. 104.

24. Condra J., Costello J., Chu S. Linguistic Analysis of WannaCry Ransomware Messages Suggests Chinese-Speaking Authors // Flashpoint. URL: https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/ (accessed: 14.02.2023).

25. Urquhart L., McAuley D. Cybersecurity Implications of the Industrial Internet of Things // TILTing Perspectives 2017: Regulating a Connected World. Tilburg, 2017.

26. Hiller J.S. Civil Cyberconflict: Microsoft, Cybercrime, and Botnets / J. S. Hiller // Santa Clara High Technology Law Journal. 2015. Vol. 31, Is. 2. P. 163–214.

27. Осипенко А.Л. Информационное пространство глобальных компьютерных сетей как объект криминологического изучения // Современное право. 2009. № 5. С. 110–114.

References

1. Kleymenov, M.P. (2017) Neraskrytaya i latentnaya prestupnost': razlichiya i skhodstvo [Unsolved and Latent Crime: Differences and Similarities]. *Pravoprimenenie*. 1. pp. 106–113.

2. Inshakov, S.M. (2009) Latentnaya prestupnost' kak ob"ekt issledovaniya [Latent Crime as an Object of Research]. *Kriminologiya: vchera, segodnya, zavtra*. 16. pp. 107–130.

3. Ivanova, E.O. (2015) Latentnaya prestupnost': ponyatie i kriterii klassifikatsii [Latent Crime: Concept and Classification Criteria]. *Sovremennoe pravo*. 5. pp. 119–123.

4. Legostaev, S.V. (2016) Prognozirovanie i preduprezhdenie latentnoy prestupnosti [Forecasting and Prevention of Latent Crime]. *Chelovek: prestuplenie i nakazanie*. 3. pp. 110–114.

5. Inshakov, S.M. (2010) Gnoseologicheskie problemy issledovaniya latentnoy prestupnosti [Gnoseological problems of studying latent crime]. *Russian Journal of Economics and Law*. 1(13). pp. 136–142.

6. Jewkes, Y. & Yar, M. (2008) Policing cybercrime: emerging trends and future challenges. In: Newborn, T. (ed.) *Handbook of Policing*. London; New York: Routledge. pp. 580–606.

7. Inshakov, S.M. (2008) Latentnaya prestupnost' kak pokazatel' effektivnosti ugolovnoy politiki [Latent crime as an indicator of the effectiveness of criminal policy]. *Rossiyskiy sledovatel'*. 14. pp. 20–21.

8. Goodman, M. (2001) Making computer crime count. *FBI Law Enforcement Bulletin*. 70(8). pp. 10–17.

9. Grebenkov, A.A. (2011) Narusheniya avtorskogo prava s ispol'zovaniem tekhnologii BitTorrent: problemy ugolovnoy otvetstvennosti [Copyright Infringement Using BitTorrent Technology: Issues of Criminal Liability]. *Ugolovnoe pravo: strategiya razvitiya v XXI veke* [Criminal Law: Development Strategy in the 21st Century]. Proc. of the Eighth International Conference. January 27–28, 2011. Moscow: Prospekt. pp. 376–380.

10. Luneev, V.V. (2005) *Prestupnost' XX veka: mirovye, regional'nye i rossiyskie tendentsii* [Crime in the 20th Century: Global, Regional, and Russian Trends]. Moscow: Wolters Kluwer.

11. Kvashis, V.E. (2016) Sravnitel'nyy analiz latentnoy prestupnosti v Rossii i zarubezhnykh stranakh: problemy i perspektivy [Comparative Analysis of Latent Crime in Russia and Foreign Countries: Problems and Prospects]. *Zhurnal zakonodatel'stva i sravnitel'nogo pravovedeniya*. 5. pp. 89–93.

12. Hyman, P. (2013) Cybercrime: it's serious, but exactly how serious? *Communications of the ACM.* 56(3). pp. 18–20.

13. Osipenko, A.L. & Soloviev, V.S. (2021) Osnovnye napravleniya razvitiya kriminologicheskoy nauki i praktiki preduprezhdeniya prestupleniy v usloviyakh tsifrovizatsii obshchestva [The main directions of development of criminological science and crime prevention practice in the context of digitalization of society]. *Vserossiyskiy kriminologicheskiy zhurnal*. 6. pp. 681–691.

14. Grebenkov, A.A. (2014) Prestupnost' v sfere vysokikh tekhnologiy v Rossii: prioritety bor'by [High-Tech Crime in Russia: Priorities of the Fight]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta*. 3. pp. 72–77.

15. Efremova, I.A., Smushkin, A.B., Donchenko, A.G. & Matushkin, P.A. (2021) Cyberspace as a New Crime Environment. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 472. pp. 248–256. (In Russian). DOI: 10.17223/15617793/472/29

16. Klishkov, V.B., Stebeneva, E.V. & Yakovleva, M.A. (2022) Kiberprestupnost': ponyatie, priznaki, osnovnye napravleniya protivodeystviya [Cybercrime: concept, features, main directions of counteraction]. *Vestnik NNGU*. 4. pp. 106–114.

17. Karpyuk, I. (2014) Vzlom Dvorkovicha [Hacking Dvorkovich]. *Polit.Ru*. 22nd July. [Online] Available from: http://polit.ru/article/2014/07/22/dvorkovich (Accessed: 14th February 2023).

18. Bencsáth, B. et al. (2012) The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Inter-net*. 4(4). pp. 971–1003.

19. Langner, R. (2011) Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Priva-cy*. 9(3). pp. 49–51.

20. Piggin, R. (2016) Cyber security trends: What should keep CEOs awake at night. *Interna-tional Journal of Critical Infrastructure Protection*. 13. pp. 36–38.

21. Chen, T.M. & Abu-Nimeh, S. (2011) Lessons from Stuxnet. *Computer*. 44(4). pp. 91–93.

22. Simmonds, M. (2017) How businesses can navigate the growing tide of ransomware attacks. *Computer Fraud & Security*. 3. pp. 9–12.

23. Ehrenfeld, J.M. (2017) WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems.* 41(7). p. 104.

24. Condra, J., Costello, J. & Chu, S. (n.d.) *Linguistic Analysis of WannaCry Ransomware Messages Suggests Chinese-Speaking Authors*. [Online] Available from: https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/ (Accessed: 14th February 2023).

25. Urquhart, L. & McAuley, D. (2017) Cybersecurity Implications of the Industrial Internet of Things. *TILTing Perspectives 2017: Regulating a Connected World*. Proc. of the Conference. Tilburg.

26. Hiller, J.S. (2015) Civil Cyberconflict: Microsoft, Cybercrime, and Botnets. *Santa Clara High Technology Law Journal*. 31(2). pp. 163–214.

27. Osipenko, A.L. (2009) Informatsionnoe prostranstvo global'nykh komp'yuternykh setey kak ob"ekt kriminologicheskogo izucheniya [Information space of global computer networks as an object of criminological study]. *Sovremennoe pravo*. 5. pp. 110–114.

Информация об авторе:
Гребеньков А.А. – кандидат юридических наук, доцент, доцент кафедры уголовного права Юго-Западного государственного университета (Курск, Россия). E-mail: grebenkov@gmail.com

Автор заявляет об отсутствии конфликта интересов.

Information about the author:
A.A. Grebenkov, Southwestern State University (Kursk, Russian Federation). E-mail: grebenkov@gmail.com

The author declares no conflicts of interests.

Статья поступила в редакцию 14.02.2023;
одобрена после рецензирования 17.05.2023; принята к публикации 16.12.2024.

The article was submitted 14.02.2023;
approved after reviewing 17.05.2023; accepted for publication 16.12.2024.