ISSN 2500-1442

Научная статья
УДК 343.97
EDN CLXHHF
DOI 10.17150/2500-4255.2023.17(2).146-155

ЛАТЕНТНОСТЬ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ: ПОНЯТИЕ, СТРУКТУРА, МЕТОДЫ ОЦЕНКИ УРОВНЯ

В.В. Поляков
Алтайский государственный университет, г. Барнаул, Российская Федерация

Информация о статье

Дата поступления
14 января 2023 г.

Дата принятия в печать
1 мая 2023 г.

Дата онлайн-размещения
26 мая 2023 г.

Ключевые слова

Высокотехнологичные преступления; компьютерные преступления; выявление преступлений; сокрытие преступлений; фактическая преступность

Аннотация. Проблема низкой выявляемости и раскрываемости высокотехнологичных преступлений обусловливает недостаточность знаний о реальном масштабе высокотехнологичной преступности и препятствует организации противодействия ей. В статье приведены отличительные признаки и особенности высокотехнологичных преступлений, предложена трактовка понятия их латентности. Проанализированы главные причины, влияющие на латентность высокотехнологичных преступлений, выделены основные разновидности для естественной и искусственной латентности таких преступных деяний. Выявлены и рассмотрены факторы, приводящие к существенному повышению уровня латентности высокотехнологичных преступлений, включая специфические виктимогенные факторы. Для количественной оценки степени латентности преступлений данной группы предложено использовать коэффициент, отражающий реальный «вклад» скрытых и скрываемых преступлений в фактическую преступность. В работе описаны особенности методов и подходов к количественной оценке уровня латентности высокотехнологичных преступлений, в том числе методов аналогии, экспертных оценок, информационно-сравнительного метода. Изучены трудности применения традиционных методов анализа латентности, в частности методов анализа виктимизации. Приведены результаты применения метода экспертных оценок, полученные путем анкетирования различных групп респондентов. Обращается внимание на необходимость разработки новых методов, направленных на выявление высокотехнологичных преступлений и обеспечивающих более объективную оценку их латентности. В качестве примера приводится исследовательская система Honeypot. Сделан вывод, что высокотехнологичные преступления нужно отнести к группе высоколатентных преступлений, имеющих негативную тенденцию к дальнейшей латентизации. Отмечена специфика соотношения между латентностью и общественной опасностью преступлений данного вида. Проведенное исследование призвано способствовать организации противодействия современной высокотехнологичной преступности. Полученные результаты помогут повысить эффективность криминалистических методик и рекомендаций, предназначенных для использования на первоначальном этапе расследования высокотехнологичных преступлений, и улучшить их раскрываемость.

Original article

LATENCY OF HIGH-TECH CRIMES: CONCEPT, STRUCTURE AND METHODS OF ASSESSING ITS LEVEL

Vitaly V. Polyakov
Altai State University, Barnaul, the Russian Federation

Article info

Received
2023 January 14

Accepted
2023 May 1

Available online
2023 May 26

Abstract. The detection and solving rates for high-tech crimes result in our insufficient knowledge about the true scale of high-tech crimes and hinders the organization of fighting them. The author discusses specific features and characteristics of high-tech crimes and offers an interpretation of the concept of their latency. Key factors influencing the latency of high-tech crimes are analyzed and main types of natural and artificial latency of such offences are identified. The author reveals and examines the factors that lead to a considerable increase in high-tech crime latency, including specific victimogenic factors. It is suggested that a coefficient reflecting the real contribution of hidden and concealed crimes to the actual criminality should be used for the quantitative assessment of latency rate for this group of crimes. The ar-

ISSN 2500-1442

Keywords

High-tech crimes; computer crimes; detection of crimes; concealment of crimes; actual crime

ticle presents a description of the specific features of methods and approaches used for the quantitative assessment of high-tech crime latency rate, including the methods of analogy, expert evaluation, and the information-comparison method. The difficulties of applying traditional methods of analyzing latency, specifically, methods of analyzing victimization, have been researched. The author presents the results of the expert evaluation method obtained by conducting a questionnaire for various groups of respondents. Special attention is paid to the necessity of developing new methods aimed at detecting high-tech crimes and providing a more accurate assessment of their latency. The Honeypot system is given as an example. It is concluded that high-tech crimes should be viewed as high latency crimes with an increasing negative trend for latency. The specific correlation between latency and public danger of these crimes is pointed out. The conducted research should contribute to organizing the counteraction to modern high-tech crimes. The obtained results could improve the effectiveness of criminalistic methods and recommendations used at the initial stage of investigating high-tech crimes and improve the rate of solving them.

Введение

Латентность является одной из важных характеристик преступности, поскольку всегда существует часть преступлений, которая скрыта от правоохранительных органов. Как справедливо отмечал С.М. Иншаков, криминологическое исследование латентной преступности может «изменить представление не только о масштабах этого явления, но и о сущности преступности» [1, с. 107]. Такое исследование становится особенно актуальным в случае появления новых видов преступлений, отличающихся повышенной сложностью выявления, учета и раскрываемости и одновременно высокой общественной опасностью. Примером могут служить компьютерные преступления, совершаемые дистанционным образом, их высокая латентность по отношению к большинству традиционных преступлений отмечалась в различных исследованиях [2, с. 95; 3, с. 148; 4, с. 46; 5–7]. Компьютерные преступления — это доктринальное собирательное понятие, объединяющее как уже относительно изученные виды преступлений, так и появившиеся в последнее время и вызывающие особые сложности в расследовании высокотехнологичные преступления. Для этой новой группы преступлений исследования латентности практически не проводились. В то же время полученные при таком исследовании знания представляют существенную значимость для построения криминалистических методик расследования этих преступлений, и прежде всего для формирования их криминалистической характеристики. Эта значимость связана с тем, что первоначальный этап расследования высокотехнологичных преступлений практически всегда сопровождается формированием проблемных ситуаций, характеризующихся высокой информационной неопределенностью [8]. Важность изучения латентности высокотехнологичных преступлений определяется также тем обстоятельством, что новые группы преступных посягательств, по справедливому мнению Ю.П. Гармаева, «еще не проявили себя репрезентативно для обобщения правоприменительной практики, но реальная, укрытая завесой латентности степень их общественной опасности достаточно велика» [9, с. 63].

Проблематика латентности высокотехнологичных преступлений, на наш взгляд, требует комплексного исследования, включающего как криминологический, так и криминалистический подходы, способные в совокупности дать синергетический эффект, которым смогут воспользоваться обе науки — криминология и криминалистика. С одной стороны, криминологические знания реальных масштабов данного вида преступности, а также тех ее отличительных черт, которые приводят к заниженной регистрации и, следовательно, к отсутствию возбужденных уголовных дел, должны учитываться при разработке криминалистической методики расследования высокотехнологичных преступлений. Полагаем, что можно согласиться с тем, что криминологический анализ «образует базу для формирования общей программы начального этапа расследования» [10, с. 16] и выступает как фактор, «облегчающий разработку методики расследования» [11, с. 1]. С другой стороны, криминалистические факторы, затрудняющие расследование высокотехнологичных преступлений, в частности выявляемые криминалистикой специфические способы противодействия расследованию и сокрытия следов преступления в виртуальном пространстве [12, с. 208], представляют несомненный интерес и, на наш взгляд, должны учитываться при криминологическом анализе высокотехнологичной преступности.

Понятие латентности высокотехнологичных преступлений

При рассмотрении высокотехнологичных преступлений необходимо определиться с исходной терминологией. Анализ судебно-следственной практики и экспертных мнений сотрудников правоохранительных органов и специалистов в области информационной безопасности позволил выделить характерные признаки и особенности этих преступлений. Высокотехнологичные преступления можно определить как общественно опасные противоправные деяния, совершаемые высокотехнологичным способом, включающим элементы подготовки, совершения и сокрытия следов преступлений, осуществляемые преступной группой путем применения специально созданных или модифицированных в преступных целях программных, программно-аппаратных или аппаратных средств, с использованием дистанционного доступа к компьютерной информации с помощью информационно-коммуникационных сетей и сопровождаемые противодействием расследованию [13].

Переходя к понятию латентности, необходимо отметить отсутствие общепринятой трактовки данной дефиниции. Так, И.В. Афанасьева и Ю.С. Афонина определяют латентность как «совокупность преступных деяний, которые не были заявлены или зарегистрированы правоохранительными органами, а также деяния, в отношении которых не было принято никаких последующих действий по каким-либо причинам» [14, с. 46]. По мнению П.А. Кривенцова, латентность складывается из «совокупности незаявленных и незарегистрированных в установленном законом порядке преступлений» [15, с. 20]. А.М. Смирнов полагает, что преступления являются латентными, когда «дело без достаточных на то оснований прекращено судом или виновный оправдан без наличия для этого всех необходимых оснований» [16, с. 260]. По мнению Ю.А. Шахаева, латентной является совокупность преступлений, неучтенных правоохранительными органами и учтенных, «но нераскрытых либо неполно раскрытых» [17, с. 143]. Отметим, что перечень дискуссионных точек зрения может быть продолжен.

В то же время анализ различных трактовок латентности показывает, что в них фигурируют преступления, которые могут быть сгруппированы, по нашему мнению, следующим образом: необнаруженные преступления; обнаруженные, но не заявленные в правоохранительные органы; обнаруженные и заявленные в правоохранительные органы, но незарегистрированные; зарегистрированные преступления, по которым не были возбуждены уголовные дела; преступления, которые после возбуждения уголовного дела не были раскрыты; раскрытые преступления, по которым преступники избежали привлечения к ответственности. Именно различные сочетания этих групп преступлений включаются в определения данного понятия, предлагаемые разными авторами.

Полагаем, что наиболее адекватной задаче расследования высокотехнологичных преступлений является трактовка, принадлежащая С.М. Иншакову, согласно которой к латентным должны быть отнесены фактически совершенные преступления, которые не были зарегистрированы государственными органами [1, с. 110]. Принципиальные преимущества данного понятия заключаются в следующем:

– во-первых, оно является формальным, за счет четкости используемых терминов обеспечивается однозначность в понимании определяемой дефиниции;

– во-вторых, с позиций практики расследования важно наличие формального повода (основания) для проведения следственных действий, таким основанием является регистрация сообщения о преступлении;

– в-третьих, оно позволяет проводить количественную оценку латентности для отдельных видов преступлений;

– в-четвертых, определение «прозрачно» для интерпретации и в силу его простоты удобно для практической работы правоохранительных органов.

Подводя итог, сформулируем используемое в настоящей работе определение, отвечающее целям проводимого исследования: латентные высокотехнологичные преступления — это не зарегистрированная правоохранительными органами часть всех фактически совершенных высокотехнологичных преступлений.

Структура латентности высокотехнологичных преступлений

В зависимости от содержания механизма, посредством которого преступления были сокрыты от регистрации, они могут быть разделены на два вида: естественно-латентные и искусственно-латентные. К первому виду относят фактически совершенные преступления, о которых не поступало сообщений в правоохра-

нительные органы, в связи с чем они не могли быть зарегистрированы. Полагаем, что можно выделить следующие две разновидности таких преступлений: не обнаруженные потерпевшими, свидетелями или правоохранительными органами преступления и обнаруженные преступления, сообщение о которых для регистрации не подавалось.

Ко второму виду относятся преступления, сообщения о которых поступали в правоохранительные органы, но не были официально зарегистрированы и поэтому не вошли в соответствующую статистику. По мнению Б.Я. Гаврилова, именно недостатки в порядке учета регистрации уголовных дел являются одной из основных причин «высочайшей латентности» [18, с. 8]. Среди преступлений данного вида также можно выделить разновидности в зависимости от формы отказа в регистрации сообщения о преступлении. Так, С.М. Иншаков выделяет следующие формы неправомерного отказа: принятие заявления и его последующее уничтожение, отказ от принятия заявления, отказ в возбуждении уголовного дела, необоснованное прекращение дела [1, с. 110]. Помимо этих форм могут быть выделены и другие, в том числе «снижение активности в плане выявления незаявленных преступлений» [19, с. 58], нарушение «установленных правил регистрации и учета преступлений» [20, с. 83] и иные.

На естественную и искусственную латентность высокотехнологичных преступлений существенно влияют как общие факторы, так и факторы, отражающие специфику преступных деяний именно преступлений данной группы. К числу последних нами были отнесены следующие факторы:

– полноструктурный характер способа преступления [21], включающего в себя действия по подготовке, непосредственному совершению преступления и сокрытию его следов;

– особенности следовой картины преступления, образованной электронно-цифровыми следами [22; 23], которые могут быть легко уничтожены или модифицированы;

– дистанционный характер преступного посягательства на компьютерную информацию, основанный на использовании информационно-телекоммуникационных сетей для обеспечения анонимизации личности преступников [24];

– наличие в составе преступных групп соучастников, обладающих специальными познаниями в сфере компьютерных технологий;

– транснациональный характер [25] наиболее опасных разновидностей высокотехнологичных преступлений;

– противодействие расследованию, направленное на воспрепятствование регистрации преступления и последующего возбуждения уголовного дела;

– недостаточный уровень знаний сотрудников правоохранительных органов в области современных информационных технологий;

– виктимогенные факторы, влияющие на поведение самих потерпевших (как физических, так и юридических лиц), по различным причинам отказывающихся от обращения в правоохранительные органы с заявлением о преступлении (T. Brosowski, S. Wachs, H. Scheithauer и A.T. Vazsonyi считают, что проявления виктимизации для киберпреступлений более характерны, чем для традиционных [26]).

Полагаем, что именно совокупность всех названных факторов приводит к повышению уровня латентности высокотехнологичных преступлений. При этом влияние криминалистически значимых факторов на естественно-латентные и искусственно-латентные преступления различно. Именно первые из приведенных факторов (способ преступления, сокрытие следов, профессионализм преступников) способствуют естественной латентности. В то же время фактор, отражающий противодействие расследованию, на наш взгляд, влияет как на естественную, так и на искусственную латентность. Так, его воздействие может проявляться в запугивании потерпевших и свидетелей, вследствие чего они не обращаются в правоохранительные органы (естественная латентность), или в подкупе должностных лиц с целью воспрепятствования регистрации поступившего заявления (искусственная латентность).

Методы оценки латентности высокотехнологичных преступлений

Анализ латентности преступлений определенного вида проводится на основе оценок, позволяющих делать выводы об ее уровне и динамике. В 2000-х гг. были проведены количественные оценки латентности отдельных групп преступлений, методика которых описывалась в работах Б.Я. Гаврилова, С.М. Иншакова и других отечественных авторов [1; 27; 28], а также в публикациях зарубежных исследователей [29–31].

Нужно подчеркнуть, что получаемые при оценке уровня латентности результаты принци-

пиально не могут рассматриваться как точные, они всегда имеют вероятностный характер. Это связано с тем, что число фактически совершаемых преступлений, в отличие от числа регистрируемых преступных деяний, неизвестно и точно не может быть установлено в принципе. Кроме того, в качестве количественной характеристики латентности могут применяться разные величины, отражающие долю латентных преступлений от их общего или зарегистрированного числа. При оценке латентности высокотехнологичных преступлений нами был использован коэффициент К, показывающий «вклад» скрытых и скрываемых преступлений в фактическую преступность. Обозначим через N_F число фактически совершенных преступлений данного вида, через N_R — число зарегистрированных преступлений, тогда число латентных преступлений — $N_L = N_F – N_R$ и коэффициент К определится следующим образом:

$$К = N_L / N_F \cdot 100\ \% = (N_F – N_R) / N_F \cdot 100\ \%.$$

При качественном анализе все преступления могут быть распределены по группам с различными количественными характеристиками латентности. Так, С.М. Иншаков выделял четыре группы с особо высокой, высокой, промежуточной и низкой латентностью [1, с. 124]. Полагаем, что для высокотехнологичных преступлений, в случае которых надежные количественные оценки затруднены, целесообразно использовать менее детальное разбиение на три группы — высоколатентные, среднелатентные и низколатентные. Для этих групп могут быть предложены следующие интервалы коэффициента К: высоколатентные преступления, если К изменяется в интервале 80–100 % (подавляющая часть преступлений не регистрируется); среднелатентные преступления, если К ограничивается интервалом 50–80 % (преступления с промежуточной латентностью); низколатентные преступления, если коэффициент К составляет менее 50 % (регистрируется более половины преступлений).

Для анализа латентности существенную роль играет выбор методов и методик, используемых при количественной оценке фактически совершенных высокотехнологичных преступлений. Согласно эвристическому методу аналогии, проводится сопоставление со статистическими материалами, относящимися к близким видам преступных деяний, а именно к экономическим преступлениям, преступлениям в сфере компьютерной информации, преступлениям, совершаемым организованными преступными группами. В работе Л.В. Бертовкого и И.В. Глазуновой было установлено, что для организованной преступности в сфере экономической деятельности число латентных преступных деяний может превышать число зарегистрированных в сотни раз [3, с. 148]. Особую значимость имеют данные по латентности в сфере преступлений, совершаемых с привлечением информационно-коммуникационных технологий. По мнению П.А. Кривенцова, преступность в этой сфере относится к числу самых высоколатентных, поскольку доля скрытых компьютерных преступлений может превышать 90 % от числа всех совершенных [15, с. 7].

К оценке искусственной высокотехнологичной латентности может быть привлечен информационно-сравнительный метод, основывающийся на изучении отказных материалов, прекращенных производством уголовных дел, исследовании заявлений граждан о совершении преступления [14, с. 49], а также материалов оправдательных приговоров.

В то же время анализ материалов судебно-следственной практики существенно затрудняет то обстоятельство, что высокотехнологичные преступления включают в себя преступные деяния, подпадающие под разные статьи Уголовного кодекса РФ и регистрирующиеся именно в таком качестве. На аналогичное обстоятельство обращали внимание M. McGuire и S. Dowling: поскольку отсутствует такое правонарушение, как «киберпреступление», то полиция при регистрации преступления не делает различий, связано оно с кибератаками или нет [7, p. 5]. Проблемы со статистикой уголовного судопроизводства и мониторингом киберпреступлений отмечались и другими зарубежными исследователями [6; 31].

Отметим, что привлечение ряда распространенных методов оценки латентности высокотехнологичных преступлений может оказаться сопряженным с дополнительными трудностями. Например, анализ виктимизации затруднен тем, что виктимологические опросы, как правило, проводятся среди физических лиц, тогда как высокотехнологичные преступления наносят максимальный по величине материальный ущерб финансовым организациям. Эти организации не склонны участвовать в статистических исследованиях и стремятся разрешать компьютерные инциденты своими силами [7,

p. 4], поскольку расследование может причинить вред их деловой репутации и, кроме того, как справедливо отмечал Н.Л. Коликов, «убытки от расследования могут оказаться выше суммы причиненного ущерба» [32, с. 31].

Полагаем, что для анализа естественной латентности высокотехнологичных преступлений одним из наиболее значимых является метод экспертных оценок [33, с. 512]. Пример его успешного применения был описан В.Е. Дворцовым и И.Т. Казанчевым при рассмотрении преступлений в сфере кадастровой деятельности, для которых наблюдались близкие проблемы, связанные с недостатком данных о регистрации преступлений [34, с. 3]. Этот же метод активно применяется зарубежными исследователями. Так, E.R. Leukfeldt, A. Lavorgna и E.R. Kleemans при анализе киберпреступлений, совершенных организованными группами, использовали данные опросов сотрудников прокуратуры и полиции, расследовавших соответствующие уголовные дела, а также экспертов по цифровым технологиям [5, p. 290]. Роль экспертов подчеркивалась в работе A. Lavorgna и G.A. Antonopoulos [35, p. 146]. A.M. Bossler и T. Berenblum считают, что мнения специалистов являются ключевым источником информации при исследовании киберпреступлений [36, p. 496].

Нами проводился анализ латентности преступлений, обладавших признаками высокотехнологичных преступных деяний, по методу экспертных оценок с помощью специально разработанной анкеты, включавшей в себя оценку экспертами ситуации с выявляемостью и раскрываемостью преступлений. В опросах приняли участие различные группы респондентов: сотрудники подразделений ГУ МВД России по Алтайскому краю (60 %), представители судейского корпуса (9 %), а также специалисты по информационной безопасности (31 %), всего 70 чел. Большинство анкетированных имели опыт расследования преступлений и компьютерных инцидентов, в которых использовались информационно-телекоммуникационные технологии. Как показала статистическая обработка полученных данных, большинство экспертов (свыше 70 %) указали на низкую выявляемость и высокую латентность рассматриваемых преступлений. Кроме того, раскрываемость уже выявленных преступлений была оценена выше, чем их выявляемость (уровень раскрываемости признали низким 53 % респондентов). Интересен анализ мнения респондентов о факторах, негативно влияющих на латентность. Наряду с криминалистической сложностью расследования и недостаточной защищенностью компьютерных систем сотрудники правоохранительных органов особо выделили несовершенства действующего уголовно-процессуального законодательства. Отметим, что в научной литературе большинство предложений нацелено на изменение или уточнение статей Уголовного кодекса РФ, что, по мнению практиков, является менее актуальной задачей, чем совершенствование статей Уголовно-процессуального кодекса РФ.

Таким образом, высокотехнологичные преступления должны быть отнесены к группе высоколатентных преступлений. Кроме того, полагаем, что расширяющееся применение новых средств совершения преступлений, основанных на современных достижениях в информационных технологиях, дает основания ожидать дальнейшего усиления их латентизации.

Отметим, что организованные преступные группы, совершающие высокотехнологичные преступления, могут обладать финансовыми, техническими, кадровыми и другими ресурсами, которые позволяют осуществлять преступные посягательства максимально скрытно. В силу этого, по нашему мнению, актуальной задачей является разработка и внедрение в правоохранительную практику новых перспективных методов и средств, направленных на обнаружение таких посягательств и обеспечивающих более объективную и точную оценку латентности. Одним из перспективных примеров таких средств может служить исследовательская система Honeypot, выступающая в качестве инструмента для сбора информации о преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей [37; 38].

Отдельный интерес представляет вопрос о соотношении между латентностью и общественной опасностью высокотехнологичных преступлений. В случае традиционных преступлений наименьшей латентностью обладают преступные деяния с повышенной общественной опасностью. Так, И.В. Максименко пишет об аксиоме в плане существования обратной зависимости уровня латентности преступных деяний: «он тем выше, чем меньше общественная опасность совершенного преступления» [39, с. 149]. В то же время полагаем, что случай высокотехнологичных преступлений, совершаемых преступными группами при использова-

нии специально разработанных в преступных целях компьютерных средств, по-видимому, выпадает из этого правила, поскольку таким преступлениям свойственны одновременно и повышенная общественная опасность, и высокая латентность.

Выводы

Проведенное исследование латентности высокотехнологичных преступлений позволило установить ее структуру и описать специфические факторы, способствующие ее повышению и существенно затрудняющие обнаружение и регистрацию этого нового вида преступлений. Выявление и анализ данных факторов представляются значимыми для криминологического понимания феномена высокотехнологичной преступности и идентификации основных тенденций, определяющих ее развитие. Полученные результаты могут быть также использованы при разработке и практической реализации эффективных мер предупреждения преступлений указанного вида.

С позиций криминалистики представленные в работе новые данные, отражающие характерные особенности латентности высокотехнологичных преступлений, будут способствовать формированию углубленного представления о криминалистически значимых признаках всей группы подобных преступных деяний, а не только ее регистрируемой части. Полученные данные могут быть применены при создании частной криминалистической методики расследования высокотехнологичных преступлений, прежде всего при разработке новых и эффективных рекомендаций, тактических решений и приемов для первоначального этапа их расследования.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Иншаков С.М. Латентная преступность как объект исследования / С.М. Иншаков. — EDN TIIPIL // Криминология: вчера, сегодня, завтра. — 2009. — № 1 (16). — С. 107–130.

2. Мазуров В.А. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий / В.А. Мазуров, В.В. Поляков. — EDN KXQZEL // Известия Алтайского государственного университета. — 2009. — № 2. — С. 95–98.

3. Бертовский Л.В. Преступное нарушение правил экономической деятельности (криминалистическая характеристика) / Л.В. Бертовский, И.В. Глазунова. — EDN WZQVVJ // Вестник Финансового университета. — 2016. — Т. 20, № 6. — С. 147–155.

4. Евдокимов К.Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты / К.Н. Евдокимов. — Иркутск : Изд-во ИЮИ (ф) УП РФ, 2016. — 267 с. — EDN YNINGZ.

5. Leukfeldt E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime / E.R. Leukfeldt, A. Lavorgna, E.R. Kleemans. — DOI 10.1007/s10610-016-9332-z // European Journal on Criminal Policy and Research. — 2017. — Vol. 23, iss. 3. — P. 287–300.

6. Dupont B. Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring / B. Dupont. — DOI 10.1080/0735648X.2019.1691855 // Journal of Crime and Justice. — 2019. — Vol. 42, iss. 5. — P. 500–515.

7. McGuire M. Cyber Crime: A Review of the Evidence : Research Report 75. Ch. 4: Improving the Cyber Crime Evidence Base / M. McGuire, S. Dowling. — UK Home Office, 2013. — 10 p.

8. Драпкин Л.Я. Принятие оперативно-розыскных и следственных решений в ситуациях информационной неопределенности, конфликта и риска / Л.Я. Драпкин, А.Е. Шуклин. — EDN JUCEBN // Российский юридический журнал. — 2006. — № 3 (51). — С. 89–97.

9. Гармаев Ю.П. Теоретические основы формирования криминалистических методик расследования преступлений : дис. ... д-ра юрид. наук : 12.00.09 / Ю.П. Гармаев. — Москва, 2005. — 342 с.

10. Бурданова В.С. Особенности расследования убийств, совершенных по найму : учеб. пособие / В.С. Бурданова, В.А. Гуняев, С.М. Пелецкая. — Санкт-Петербург : Изд-во С.-Петерб. юрид. ин-та, 1997. — 40 с.

11. Исаева К.А. Криминолого-криминалистическая характеристика насильственных преступлений, совершаемых в уголовно-исполнительных учреждениях стран СНГ / К.А. Исаева, С.А. Августхан. — DOI 10.7256/2454-0692.2018.3.2688. — EDN MOUWMN // Полицейская деятельность. — 2018. — № 3. — С. 1–11.

12. Грибунов О.П. Криминалистическая теория причинности в контексте установления механизма следообразования: философские и теоретические аспекты / О.П. Грибунов. — DOI 10.17223/15617793/446/27. — EDN PEWQIQ // Вестник Томского государственного университета. — 2019. — № 446. — С. 207–211.

13. Поляков В.В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений / В.В. Поляков. — DOI 10.17803/1729-5920.2022.187.6.085-096. — EDN UQUDGM // Lex Russica. — 2022. — Т. 75, № 6. — С. 85–96.

14. Афанасьева И.В. Выявление латентной преступности в России и зарубежных странах / И.В. Афанасьева, Ю.С. Афонина. — EDN TYYOAD // Актуальные вопросы борьбы с преступлениями. — 2015. — № 2. — С. 46–49.

15. Кривенцов П.А. Латентная преступность в России (криминологическое исследование) : автореф. дис. ... канд. юрид. наук : 12.00.08 / П.А. Кривенцов. — Москва, 2015. — 27 с. — EDN ZPPMCF.

16. Смирнов А.М. Уровень (степень) латентности отдельных видов (групп) преступлений / А.М. Смирнов. — EDN YPLKRF // Аллея науки. — 2018. — Т. 5, № 9 (25). — С. 259–262.

17. Шахаев Ю.А. Понятие и основные формы проявления латентной преступности несовершеннолетних лиц / Ю.А. Шахаев. — EDN KHRMPD // Проблемы экономики и юридической практики. — 2009. — № 2. — С. 141–144.

18. Гаврилов Б.Я. О реальности уголовно-правовой статистики о преступности / Б.Я. Гаврилов. — EDN LLRLHR // Пенитенциарная наука. — 2009. — № 6. — С. 4–10.

19. Саркисян А.Ж. Сравнительная характеристика зарегистрированных и фактических преступлений в 2001–2010 гг. / А.Ж. Саркисян. — EDN AYLIZU // Расследование преступлений: проблемы и пути их решения. — 2018. — № 2 (20). — С. 55–63.

20. Торопин Ю.В. Латентная преступность: понятие, сущность и структура / Ю.В. Торопин. — EDN NWARVL // Труды Академии управления МВД России. — 2011. — № 2 (18). — С. 82–85.

21. Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский. — DOI 10.17803/1729-5920.2019.148.3.087-099. — EDN UALFOP // Lex Russica. — 2019. — № 3 (148). — С. 87–99.

22. Мещеряков В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков. — EDN RDFWJD // Библиотека криминалиста. Научный журнал. — 2013. — № 5 (10). — С. 265–270.

23. Гавло В.К. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации / В.К. Гавло, В.В. Поляков. — EDN IIUNRX // Российский юридический журнал. — 2007. — № 5 (57). — С. 146–152.

24. Осипенко А.Л. Организованная преступность в сети Интернет / А.Л. Осипенко. — EDN PCXPYZ // Вестник Воронежского института МВД России. — 2012. — № 3. — С. 10–16.

25. Leukfeldt E.R. Origin, Growth and Criminal Capabilities of Cybercriminal Networks. An International Empirical Analysis / E.R. Leukfeldt, E.R. Kleemans, W.P. Stol. — DOI 10.1007/s10611-016-9663-1 // Crime Law and Social Change. — 2016. — Vol. 67, iss. 1. — P. 39–53.

26. Bullying Perpetration and Victimization: A Test of Traditional and Cyber-Behaviors as Latent Constructs / T. Brosowski, S. Wachs, H. Scheithauer, A.T. Vazsonyi. — DOI 10.1177/0886260518807212 // Journal of Interpersonal Violence. — 2021. — Vol. 36, iss. 11-12. — P. 6343–6369.

27. Гаврилов Б.Я. Латентная преступность: понятие, структура, факторы латентности и меры по обеспечению достоверности уголовной статистики / Б.Я. Гаврилов. — 2-е изд., перераб. и доп. — Москва : Проспект, 2007. — 118 с. — EDN QXHRZB.

28. Теоретические основы исследования и анализа латентной преступности / под ред. С.М. Иншакова. — Москва : Юнити-Дана, 2015. — 839 с.

29. Mosher C.J. The mismeasure of crime / C.J. Mosher, T.D. Miethe, D.M. Phillips. — Thousand Oaks : Sage Publication, 2002. — 214 p.

30. Understanding Crime Statistics: Revisiting the Divergence of the NCVS and the UCR / ed. J.P. Lynch, L.A. Addington. — Cambridge : Cambridge University Press, 2007. — 340 p.

31. Jehle J.-M. Implementation of Community Sanctions and Measures Across Europe at the Beginning of the Twenty-first Century / J.-M. Jehle, N. Palmowski. — DOI 10.1007/s10610-017-9348-z // European Journal on Criminal Policy and Research. — 2018. — Vol. 24, iss. 1. — P. 79–98.

32. Коликов Н.Л. Причины и условия профессиональной компьютерной преступности / Н.Л. Коликов. — EDN OEYVDX // Вестник Южно-Уральского государственного университета. Сер.: Право. — 2011. — № 19. — С. 30–33.

33. Понкин И.В. Методология научных исследований и прикладной аналитики : учебник / И.В. Понкин, А.И. Лаптева. — 2-е изд., доп. и перераб. — Москва : Буки Веди, 2021. — 567 с.

34. Дворцов В.Е. Криминологическая оценка детерминант латентности преступлений в сфере кадастровой деятельности / В.Е. Дворцов, И.Т. Казанчев. — DOI 10.7256/2454-0692.2017.2.22209. — EDN YKVZSB // Полицейская деятельность. — 2017. — № 2. — С. 1–8.

35. Lavorgna A. Criminal Markets and Networks in Cyberspace / A. Lavorgna, G.A. Antonopoulos. — DOI 10.1007/s12117-022-09450-5 // Trends Organized Crime. — 2022. — Vol. 25, iss. 2. — P. 145–150.

36. Bossler A.M. Introduction: new directions in cybercrime research / A.M. Bossler, T. Berenblum. — DOI 10.1080/0735648X.2019.1692426 // Journal of Crime and Justice. — 2019. — Vol. 42, no. 5. — P. 495–499.

37. Craig V. Honeypot Technologies and Their Applicability as a Strategic Internal Countermeasure / V. Craig. — DOI 10.1504/IJICS.2007.015503 // International Journal of Information and Computer Security. — 2011. — Vol. 1, iss. 4. — P. 430–436.

38. Polyakov V.V. Architecture of the Honeypot System for Studying Targeted Attacks / V.V. Polyakov, S.A. Lapin. — DOI 10.1109/APEIE.2018.8545323 // XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). — Novosibirsk, 2018. — P. 202–205.

39. Максименко И.В. Структура латентной преступности в Российской Федерации / И.В. Максименко. — EDN KZBXOB // Актуальные проблемы экономики и права. — 2010. — № 1. — С. 148–154.

REFERENCES

1. Inshakov S.M. Latent Crime as an Object of Research. *Kriminologiya: vchera, segodnya, zavtra = Criminology: Yesterday, Today, Tomorrow,* 2009, no. 1, pp. 107–130. (In Russian). EDN: TIIPIL.

2. Mazurov V.A., Polyakov V.V. Criminology and Criminal Prevention Crimes in Sphere of High Information and Telecommunication Technologies. *Izvestiya Altaiskogo Gosudarstvennogo Universiteta = Izvestiya of Altai State University,* 2009, no. 2, pp. 95–98. (In Russian). EDN: KXQZEL.

3. Bertovsky L.V., Glazunova I.V. Criminal Violation of Economic Activity Rules (a Criminological Characteristic). *Vestnik Finansovogo universiteta = Bulletin of the Financial University,* 2016, vol. 20, no. 6, pp. 147–155. (In Russian). EDN: WZQVVJ.

4. Evdokimov K.N. *Countering Computer Crime in the Russian Federation: Criminological and Criminal Law Aspects.* Irkutsk, ILI (b) UP RF Publ., 2016. 267 p. EDN: YNINGZ.

5. 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. *European Journal on Criminal Policy and Research*, 2017, vol. 23, iss. 3, pp. 287–300. DOI: 10.1007/s10610-016-9332-z.

6. Dupont B. Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring. *Journal of Crime and Justice*, 2019, vol. 42, iss. 5, pp. 500–515. DOI: 10.1080/0735648X.2019.1691855.

7. McGuire M., Dowling S. *Cyber Crime: A Review of the Evidence. Research Report 75. Ch. 4: Improving the Cyber Crime Evidence Base*. UK Home Office, 2013. 10 p.

8. Drapkin L.Ya., Shuklin A.E. Making Operative-search and Investigation Decisions in the Situations of Information Uncertainty, Conflict and Risk. *Rossiiskii yuridicheskii zhurnal = Russian Law Journal,* 2006, no. 3, pp. 89–97. (In Russian). EDN: JUCEBN.

9. Garmaev Yu.P. *Theoretical Basis of Forming Criminalistic Methods of Crime Investigation. Doct. Diss.* Moscow, 2005. 342 p.

10. Burdanova V.S., Gunyaev V.A., Peletskaya S.M. *Specific Features of Investigating Contract Killings.* Saint Petersburg Law Institute of the Prosecutor General's Office of the Russian Federation Publ., 1997. 40 p.

11. Isaeva K.A., Avgustkhan S.A. Criminological and Forensic Description of Violence Committed at Penitentiaries of the CIS States. *Politseiskaya deyatel'nost = Police Activity,* 2018, no. 3, pp. 1–11. (In Russian). EDN: MOUWMN. DOI: 10.7256/2454-0692.2018.3.2688.

12. Gribuno O.P. The Forensic Theory of Causality in the Establishment of the Trace Creation Mechanism: Philosophical and Theoretical Aspects. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal,* 2019, no. 446, pp. 207–211. (In Russian). EDN: PEWQIQ. DOI: 10.17223/15617793/446/27.

13. Polyakov V.V. Sources and Principles of Private Methods Development for High-Tech Crimes Investigation. *Lex Russica,* 2022, vol. 75, no. 6, pp. 85–96. (In Russian). EDN: UQUDGM. DOI: 10.17803/1729-5920.2022.187.6.085-096.

14. Afanaseva I.V., Afonina Yu.S. Uncovering Latent Crimes in Russia and Abroad. *Aktual'nye voprosy bor'by s prestupleniyami = Actual Issues of Fight Against Crime,* 2015, no. 2, pp. 46–49. (In Russian). EDN: TYYOAD.

15. Kriventsov P.A. *Latent Crimes in Russia (a Criminological Study). Cand. Diss. Thesis.* Moscow, 2015. 27 p. EDN: ZPPMCF.

16. Smirnov A.M. The Level (Degree) of Latency in Specific Types (Groups) of Crimes. *Alleya nauki = Alley of Science,* 2018, vol. 5, no. 9, pp. 259–262. (In Russian). EDN: YPLKRF.

17. Shakhajev U.A. The Notion and Main Forms of the Manifestation to Latent Criminality of the Minors. *Problemy ekonomiki i yuridicheskoi praktiki = Economic Problems and Legal Practice*, 2009, no. 2, pp. 141–144. (In Russian). EDN: KHRMPD.

18. Gavrilov B.Ya. On the Reality of Criminal Law Statistics on Crime. *Penitentsiarnaya nauka = Penitentiary Science,* 2009, no. 6, pp. 4–10. (In Russian). EDN: LLRLHR.

19. Sarkisyan A.Z. Comparative Characteristics of Registered and Actual Crimes for the Period 2001–2010. *Rassledovanie prestuplenii: problemy i puti ikh reshenii = Criminal Investigation: Problems and Ways of their Solution,* 2018, no. 2, pp. 55–63. (In Russian). EDN: AYLIZU.

20. Toropin Yu.V. Latent Crime: Concept, Essence and Structure. *Trudy Akademii upravleniya MVD Rossii = Proceedings of the Management Academy of the Ministry of the Interior of Russia,* 2011, no. 2, pp. 82–85. (In Russian). EDN: NWARVL.

21. Rossinskaya E.R., Ryadovskiy I.A. Modern Means of Committing Computer Crimes and Patterns of Their Execution. *Lex Russica,* 2019, no. 3, pp. 87–99. (In Russian). EDN: UALFOP. DOI: 10.17803/1729-5920.2019.148.3.087-099.

22. Meshcheryakov V.A. Traces of Crime in the Field of High Technologies. *Biblioteka kriminalista = Library of a Criminalist,* 2013, no. 5, pp. 265–270. (In Russian). EDN: RDFWJD.

23. Gavlo V.K., Polyakov V.V. Track Picture and its Significance for Investigation of the Crimes Connected with Unlawful Remote Access to Computer Information. *Rossiiskii yuridicheskii zhurnal = Russian Law Journal,* 2007, no. 5, pp. 146–152. (In Russian). EDN: IIUNRX.

24. Osipenko A.L. Organized Crime in the Internet. *Vestnik Voronezhskogo instituta MVD Rossii = The Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia,* 2012, no. 3, pp. 10–16. (In Russian). EDN: PCXPYZ.

25. Leukfeldt E.R., Kleemans E.R., Stol W.P. Origin, Growth and Criminal Capabilities of Cybercriminal Networks. An International Empirical Analysis. *Crime Law and Social Change*, 2016, vol. 67, iss. 1, pp. 39–53. DOI: 10.1007/s10611-016-9663-1.

26. Brosowski T., Wachs S., Scheithauer H., Vazsonyi A.T. Bullying Perpetration and Victimization: A Test of Traditional and Cyber-Behaviors as Latent Constructs. *Journal of Interpersonal Violence*, 2021, vol. 36, iss. 11-12, pp. 6343–6369. DOI: 10.1177/0886260518807212.

27. Gavrilov B.Ya. *Latent Crimes: Concept, Structure, Latency Factors and Measures for Ensuring the Accuracy of Criminal Statistics.* 2nd ed. Moscow, Prospekt Publ., 2007. 118 p. EDN: QXHRZB.

28. Inshakov S.M. (ed.). *Theoretical Elements of Research and Analysis of Latent Crime*. Moscow, Yuniti-Dana Publ., 2011. 839 p.

29. Mosher C.J., Miethe T.D., Phillips D.M. *The Mismeasure of Crime*. Thousand Oaks, Sage Publication, 2002. 214 p.

30. Lynch J.P., Addington L.A. (eds.). *Understanding Crime Statistics: Revisiting the Divergence of the NCVS and the UCR*. Cambridge University Press, 2007. 340 p.

31. Jehle J.-M., Palmowski N. Implementation of Community Sanctions and Measures across Europe at the Beginning of the Twenty-first Century. *European Journal on Criminal Policy and Research*, 2018, vol. 24, iss. 1, pp. 79–98. DOI: 10.1007/s10610-017-9348-z.

32. Kolikov N.L. Reasons and Conditions of Professional Computer Crime. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of South Ural State University. Series: Law,* 2011, no. 19, pp. 30–33. (In Russian). EDN: OEYVDX.

33. Ponkin, I.V., Lapteva, A.I. *Methodology of Scientific Research and Applied Analytics.* 2nd. ed. Moscow, Buki Vedi Publ., 2021. 567 p.

34. Dvortsov V.E., Kazanchev I.T. Criminological Assessment of Crime Latency Determinants in the Sphere of Cadastral Activities. *Politseiskaya deyatel'nost = Police Activity,* 2017, no. 2, pp. 1–8. (In Russian). EDN: YKVZSB. DOI: 10.7256/2454-0692.2017.2.22209.

35. Lavorgna A., Antonopoulos G.A. Criminal Markets and Networks in Cyberspace. *Trends of Organized Crime,* 2022, vol. 25, iss. 2, pp. 145–150. DOI: 10.1007/s12117-022-09450-5.

36. Bossler A.M., Berenblum T. Introduction: New Directions in Cybercrime Research. *Journal of Crime and Justice*, 2019, vol. 42, no. 5, pp. 495–499. DOI: 10.1080/0735648X.2019.1692426.

37. Craig V. Honeypot Technologies and Their Applicability as a Strategic Internal Countermeasure. *International Journal of Information and Computer Security,* 2011, vol. 1, iss. 4, pp. 430–436. DOI: 10.1504/IJICS.2007.015503.

38. Polyakov V.V., Lapin S.A. Architecture of the Honeypot System for Studying Targeted Attacks. *XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE*). Novosibirsk, 2018, pp. 202–205. DOI: 10.1109/APEIE.2018.8545323.

39. Maksimenko I.V. Structure of Latent Crime in the Russian Federation. *Aktual'niye problemy ekonomiki i prava = Actual Problems of Economics and Law,* 2010, no. 1, pp. 148–154. (In Russian). EDN: KZBXOB.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Поляков Виталий Викторович — доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета, кандидат юридических наук, г. Барнаул, Российская Федерация; e-mail: agupolyakov@gmail.com.

INFORMATION ABOUT THE AUTHOR

Polyakov, Vitaly V. — Ass. Professor, Chair of Criminal Procedure and Criminalistics, Altai State University, Ph.D. in Law, Barnaul, the Russian Federation; e-mail: agupolyakov@gmail.com.

ДЛЯ ЦИТИРОВАНИЯ

Поляков В.В. Латентность высокотехнологичных преступлений: понятие, структура, методы оценки уровня / В.В. Поляков. — DOI 10.17150/2500-4255.2023.17(2).146-155. — EDN CLXHHF // Всероссийский криминологический журнал. — 2023. — Т. 17, № 2. — С. 146–155.

FOR CITATION

Polyakov V.V. Latency of High-Tech Crimes: Concept, Structure and Methods of Assessing its Level. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 2, pp. 146–155. (In Russian). EDN: CLXHHF. DOI: 10.17150/2500-4255.2023.17(2).146-155.