УДК 347.77/.78

# НЕКОТОРЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ТРАНСНАЦИОНАЛЬНОЙ КИБЕРПРЕСТУПНОСТИ

**Яковец Евгений Николаевич**

Российская таможенная академия, Московская обл., г. Люберцы
e-mail: koshka997@mail.ru

# SOME PROBLEMS OF COUNTERING TRANSNATIONAL CYBERCRIME

**Yakovets Evgeny N.**

Russian Customs Academy, Moscow region, Lyubertsy

*Аннотация:* В статье рассматриваются вопросы информационно-аналитического обеспечения противодействия транснациональной киберпреступности с использованием автоматизированных логико-аналитических систем. Анализируются проблемы, связанные с созданием интегрированного банка данных оперативно-розыскного назначения и организацией межведомственного информационного взаимодействия в ходе организации противодействия компьютерным преступлениям.

*Ключевые слова:* киберпреступность, российские правоохранительные органы и спецслужбы; автоматизированные логико-аналитические системы; искусственный интеллект; интегрированный банк данных оперативно-розыскного назначения, межведомственное и международное информационное взаимодействие.

*Abstract:* The article deals with the issues of information and analytical support for countering transnational cybercrime using automated logical and analytical systems. The problems associated with the creation of an integrated data bank for operational investigative purposes and the organization of interdepartmental information interaction in the course of organizing counteraction to computer crimes are analyzed.

*Keywords:* cybercrime, Russian law enforcement agencies and special services; automated logical and analytical systems; artificial intelligence; integrated database of operational investigative purposes, interdepartmental and international information interaction.

*Для цитирования: Яковец Е.Н. Некоторые проблемы противодействия транснациональной киберпреступности // Проблемы правовой и технической защиты информации. 2024. №12. С.107-115.*

*For citation: Yakovets E.N. Some problems of countering transnational cybercrime // Legal and Technical Problems of Information Security. 2024. No. 12. P.107-115.*

Киберпреступность в наши дни продолжает оставаться общественно-политической проблемой номер один, поскольку её масштабы приобрели поистине глобальный характер. Она создаёт проблемы безопасности для всего мира, детерминируя угрозы не только военного, но также экономического, политического и психологического свойства. Размах киберпреступности в современных условиях настолько широк, что для неё не существует государственных границ. Злоумышленники вооружены сегодня передовыми техническими средствами и в совершенстве владеют современными информационными технологиями. Так, по оценкам специалистов, технологическая вооружённость киберпреступников к 2025 г.

позволит им совершать тяжкие и особо тяжкие киберпреступления, включая целенаправленные атаки на различные объекты критической информационной инфраструктуры с целью выведения их из строя и убийства людей. Как прогнозируют сотрудники исследовательской компании “Gartner”, использование боевых операционных технологий и других IT-систем только с учётом причинения смерти потерпевшим способно нанести всем странам мира в ближайшей перспективе ущерб в размере более $50 млрд [1].

В связи с этим возникают вопросы: насколько эффективно Российская Федерация способна противодействовать данному вселенскому злу и что необходимо предпринять для повышения эффективности антикриминальной деятельности в кибернетическом пространстве?

Чтобы получить на них ответы, прежде всего, следует определить основные причины и условия, способствующие совершению киберпреступлений, в том числе – и террористических актов, которые должны чётко отслеживаться от момента зарождения преступного замысла до попыток их возможной реализации. Результаты экспертного опроса, проведённого среди сотрудников антитеррористических подразделений ФСБ России, показывают, что к детерминантам кибертерроризма чаще всего относятся резкое снижение уровня жизни и степени социальной защищенности людей, обострение политического противостояния и правовой нигилизм, рост сепаратизма и национализма, несовершенство федерального законодательства, низкий авторитет государственных структур, непопулярные среди населения шаги органов власти и др. Другими словами, питательной средой растущих проявлений киберпреступности, включая и её крайне опасные формы проявления, являются в первую очередь противоречия и социальная напряжённость в обществе [2]. Наряду с этим весьма существенную роль в рассматриваемом аспекте играют внешние факторы, просчитать которые с помощью традиционных средств и методов оперативно-розыскной деятельности бывает крайне затруднительно.

Российские спецслужбы и правоохранительные органы в борьбе с проявлениями киберпреступности в целом и кибертерроризмом в частности, должны эффективно использовать все имеющиеся организационно-тактические формы антикриминальной деятельности – от выявления и предупреждения первичных признаков преступных деяний – до раскрытия и оперативного сопровождения расследования каждого из них. Последствия любого киберпреступления следует оперативно минимизировать и устранять. Для этого необходимо своевременно устанавливать организаторов и исполнителей компьютерных преступлений; незамедлительно предупреждать или пресекать их действия, а лиц, причастных к криминальной деятельности, привлекать к строгой юридической ответственности. Силы и средства, предназначенные для выявления, предупреждения и пресечения криминальной деятельности в киберпространстве, минимизации или ликвидации её последствий – должны поддерживаться в постоянной оперативной готовности к их применению. Особое значение это имеет для предотвращения кибератак террористического характера, которые в условиях нарастания военной опасности могут сопровождаться применением как кибернетических, так и «обычных» методов и средств нападения. Поэтому в местах массового скопления людей, нахождения важных объектов жизнеобеспечения, транспортных магистралей, пунктов пропуска через государственную границу, таможенных постов, объектов оборонной и гражданской инфраструктуры и др. – наряду с применением превентивных технических мер по защите киберпространства должно обеспечиваться и непрерывное наблюдение за обстановкой с целью оперативного распознания злоумышленников, орудий и средств совершения преступлений, включая предметы двойного назначения, а также

признаков подготовки самих этих преступных деяний.

В связи с проведением Россией специальной военной операции на украинском направлении, а также дестабилизацией обстановки в некоторых регионах Ближнего Востока и Центральной Азии, – применение подобных комплексных мер приобретает в настоящее время особую важность для обеспечения безопасности нашей страны [3].

Как известно, био- и нанотехнологии, квантовые вычисления, искусственный интеллект и прочие технологические новации используются сегодня не только силовыми структурами, но и криминальными элементами, в том числе и киберпреступниками. Этим самым последние нередко лишают представителей правоохранительных органов их традиционных преимуществ. Американцы, например, вынуждены были приспосабливаться к этим тенденциям, поскольку так и не смогли победить исламских террористов не только в Афганистане и на Ближнем Востоке, но и в виртуальном пространстве [4, с. 19]. Возможно поэтому перед американскими силовыми структурами в своё время была поставлена глобальная задача – заполучить персональные биометрические данные, включая геномную информацию, всего населения Земного шара [5]. Правда, основные цели подобных шагов американцев до конца пока неясны и к проблемам противодействия кибертерроризму они могут иметь лишь косвенное отношение. Тем не менее, если указанные данные будут использованы для обеспечения контроля за потенциальными террористами, действующими в том числе и в виртуальном пространстве, то безусловно, эти меры внесут существенный вклад в борьбу с данным серьёзнейшим видом транснациональной преступности.

Однако в рассматриваемом нами аспекте важен эффективный анализ не только персональных биометрических данные физических лиц, причастных к киберпреступности, но и прочих сведений, имеющих к ним прямое или косвенное отношение. Речь в данном случае идёт о так называемых «больших данных», накапливаемых в различных базах и банках данных. Однако ограничиваться одним лишь накоплением подобных сведений нельзя, в противном случае они не принесут никакой пользы. Необходима их эффективная, тщательная переработка, осуществляемая в режиме реального времени. Для осуществления анализа «больших данных» целесообразно применять автоматизированные логико-аналитические системы (АЛАС), основанные на использовании искусственного интеллекта (ИИ). Подобные системы уже давно и весьма эффективно применяются правоохранительными органами и спецслужбами как на Западе, так и на Востоке. Ю.Н. Жданов и В.С. Овчинский справедливо отмечают в этой связи, что ИИ создаёт принципиально новые возможности для правоохранительной деятельности и что особенно важно, – для обеспечения национальной безопасности государства. В настоящее время полиция США, Великобритании, Нидерландов, Китая, Индии и других стран широко используют ИИ для сбора, классификации и анализа информации. Причём, при обработке сведений на первый план выходят принципиально новые, ранее не применявшиеся методы распознавания различных криминальных событий, соответствующие цифровые следы которых всегда присутствуют в компьютерной среде. Указанные авторы отмечают, что ближайшие годы станут временем тотальной экспансии методов применения ИИ в полицейской практике [6]. Примечательно, что даже в Испании – стране, не «хватающей звёзд с неба» в области развития информационных технологий, спецслужбы объявили тендер на разработку приложения, которое будет выявлять потенциальных террористов и киберпреступников. Как сообщает местное онлайн-издание «El Confidencial», искусственный интеллект поможет полиции выявлять криминогенно активных лиц и целые группы риска, а также предупреждать

террористические нападения и другие угрозы [7].

В последнее время автоматизированные аналитические системы, основанные на использовании ИИ, стали появляться и в России. Национальная стратегия развития искусственного интеллекта, на период до 2030 года, утверждённая Указом Президента РФ от 10.10.2019 № 490, определяет ИИ как комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.

Этот комплекс включает в себя информационно-коммуникационную инфраструктуру и программное обеспечение. К технологиям ИИ данная Стратегия относит в частности «компьютерное зрение», «обработку естественного языка», «распознавание и синтез речи», «интеллектуальную поддержку принятия решений» и «перспективные методы искусственного интеллекта» [8].

Без сомнения, АЛАС, использующие возможности ИИ, позволяют не только осуществлять наблюдение в виртуальном пространстве за лицами, подозреваемыми в совершении киберпреступлений, с целью оперативного распознания и отождествления последних, но и обрабатывать имеющие к ним отношение структурированные, неструктурированные и полуструктурированные данные, получаемые из самых различных источников. Что самое интересное, специалистами, погружёнными в эти проблемы, подобные методики предлагались уже давно. Как известно, активное обсуждение вопросов использования искусственного интеллекта, в том числе – применительно к деятельности силовых ведомств – в нашей стране началось лишь в последнее время, тогда как автор данной статьи вместе со своими коллегами начали заниматься вопросами внедрения АЛАС в оперативно-розыскную деятельность – более четверти века назад. Уже тогда по инициативе ГУВД г. Москвы Институтом проблем информатики РАН были созданы опытные образцы этой системы, которые успешно применялись в деятельности информационно-аналитических подразделений московской криминальной милиции [9–11]. Однако те должностные лица, от которых напрямую зависело в тот период внедрение ИИ в практику, не понимали, о чём именно идёт речь. Или делали вид, что не понимали... Поэтому отрадно, что хотя бы в наши дни этот процесс сдвинулся с «мёртвой точки» в плане создания систем распознавания и отождествления лиц, подозреваемых в совершении различных преступлений, в том числе и совершаемых в киберпространстве [12].

Как справедливо отмечает известный российский криминолог В.С. Овчинский, – в нашей стране правоохранительная система в своих ответных действиях на технологизацию преступного мира явно запаздывает. Чтобы это запаздывание не оказалось фатальным, необходима коренная перестройка всей системы подготовки кадров правоохранительных органов в интересах борьбы с киберпреступностью. По словам этого учёного, в ближайшее десятилетие все силовые структуры, должны превратиться в киберполицию, использующую новейшие технические достижения в работе с «большими данными», в сборе иной представляющей интерес информации и её анализе [13].

Наряду с применением ИИ в рассматриваемом аспекте необходимо реализовать и другие организационные меры. В частности, большое значение для осуществления антитеррористических мер имеет создание в каждом ведомстве, прямо или косвенно вовлечённом в противоборство с киберпреступностью, интегрированного банка данных оперативно-розыскного назначения (ИБДОРН), призванного консолидировать различные данные персонального и

событийного характера. Зададимся вопросом: что должен представлять из себя подобный ИБД?

Сразу отметим, что чёткого определения сущности интегрированного банка данных в действующем российском законодательстве не содержится. Поэтому следует дать научное определение последнего, основанное на анализе содержания его отдельных элементов.

Термин «интеграция» имеет латинское происхождение, он означает объединение в единое целое каких-либо частей, элементов. Соответственно глагол «интегрировать» означает «объединять части в одно целое» [14]. Под словосочетанием «банк данных» в информатике понимается совокупность баз данных, а также программных, языковых и других средств, предназначенных для централизованного накопления сведений и их использования с помощью электронных вычислительных машин [15].

Таким образом, в банки данных входят автоматизированные учёты, представляющие собой ни что иное, как базы данных. База данных определяется действующим российским законодательством следующим образом: это «представленная в объективной форме совокупность самостоятельных материалов (статей, расчётов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины» [16].

Обработка учётно-регистрационных данных с помощью ЭВМ предусматривает наличие определённых алгоритмов, заложенных в соответствующих программах для ЭВМ. Законодатель определяет программу для ЭВМ как «объективную форму представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин и других компьютерных устройств с целью получения определённого результата, включая подготовительные материалы, полученные в ходе разработки программ для ЭВМ, и порождаемые ею аудиовизуальные отображения» [17].

По логике вещей, именно базы данных, а также программы для ЭВМ в сочетании друг с другом и образуют банк данных. Вместе с тем, «совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий», то есть фактически – программ для ЭВМ – фигурирует в Федеральном законе «Об информации, информационных технологиях и о защите информации» как информационная система [18]. Таким образом, термины «банк данных» и «информационная система» можно рассматривать как тождественные.

На сегодняшний день единой трактовки сущности и устоявшейся классификации информационных систем, а также общепринятого представления об их структуре не существует, поскольку работы по проектированию и созданию последних проводятся параллельно сразу по нескольким не вполне совместимым между собой направлениям. По мнению автора данной статьи, наиболее оптимальным является следующее определение информационной системы, сформулированное в своё время профессором В.Н. Лопатиным: «информационная система – это технологическая система, представляющая совокупность технических, программных и иных средств, объединённых структурно и функционально для обеспечения одного или нескольких видов информационных процессов и предоставления информационных услуг» [19]. Принимая во внимание указанную модель, интегрированный банк данных или единое информационное пространство оперативных подразделений органов, уполномоченных на осуществление ОРД, целесообразно рассматривать в качестве совокупности двух основных элементов, проявляющихся на территориальном и ведомственном уровнях:

1) информационных ресурсов – массивов документов, учётов и баз данных, всех видов архивов и пр., содержащих

данные, сведения и знания, зафиксированные на соответствующих носителях информации, консолидирующим ядром которых является оперативно-розыскной учёт;

2) информационной инфраструктуры, включающей в себя:

а) организационные структуры, обеспечивающие функционирование и развитие единого информационного пространства, в частности, поиск, сбор, фиксацию, обработку, хранение и предоставление информации (основную роль здесь играет научно-методическое, информационное, лингвистическое, техническое, кадровое и финансовое обеспечение);

б) информационно-телекоммуникационные структуры – территориально распределённые государственные и ведомственные компьютерные сети, телекоммуникационные сети и системы специального назначения и общего пользования, сети и каналы передачи данных, средства коммутации и управления информационными потоками;

в) информационные, компьютерные и телекоммуникационные технологии;

г) системы средств массовой информации.

Подобное определение в принципе соответствует составу информационной системы, фигурирующему в п. 3 Требований о защите информации, содержащейся в информационных системах общего пользования, утверждённых приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 [20], которое включает в себя средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки информации, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Эти определения могут быть приняты за основу в ходе дальнейших рассуждений. Однако, по сути, содержание ИБДОРН в большей мере соответствует определению, предложенному в своё время Л.Ю. Миллер, которая рассматривала близкое к нему понятие информационно-поисковой системы оперативно-розыскного назначения. По её мнению, применительно к деятельности органов внутренних дел, «информационно-поисковая система оперативно-розыскного назначения – это обработанная с помощью технических средств информация, содержащаяся в специальных статистических, справочных, оперативно-розыскных, криминалистических учётах, материалах ОРД ОВД, а также базах и банках данных АИПС других правоохранительных ведомств, организаций, предприятий, в средствах массовой информации, Интернете, и систематизированная при закладке для хранения, обеспечения поиска и выдачи сведений о лице, событии, предмете или иной оперативно-значимой информации».

Вместе с тем, основную миссию в создании этой системы Л.Ю. Миллер отводит ГИАЦ МВД России, а также ИЦ МВД республик, ГУ(У) МВД России по иным субъектам РФ, призванным сформировать единую информационную вертикаль, объединяющую, в первую очередь, криминалистические, статистические и оперативно-справочные учёты ОВД [21]. Однако, перечисленные информационные подразделения, не являющиеся субъектами ОРД, не могут представлять собой организационную основу для создания ИБДОРН. При его формировании основным функциональным ядром должен являться оперативно-розыскной учёт [22], создаваемый в оперативно-розыскных органах, прежде всего, – специализированными субъектами аналитической работы в сфере ОРД, а также сотрудниками, работающими по линии противодействия киберпреступности. Все прочие виды учётов, формируемых в

информационных центрах и криминалистических подразделениях правоохранительных органов и спецслужб, многообразие которых сводится к трём основным видам – криминалистический, криминологический и административный, – могут выполнять в данном случае лишь вспомогательную роль. Они должны консолидироваться вокруг оперативно-розыскного учёта, дополняя и актуализируя его.

Под интеграцией при создании ИБДОРН следует понимать не простое механическое слияние множества малых учётов в один большой, а прежде всего, – создание единой информационной инфраструктуры, предназначенной для анализа сведений, обладателями которых являются различные субъекты информационного обмена того или иного ведомства. В качестве приоритетной формы такого обмена, безусловно, должен рассматриваться удалённый доступ с использованием АЛАС.

Таким образом, можно заключить, что ведомственный интегрированный банк данных оперативно-розыскного назначения – это объединённая на базе оперативно-розыскного учёта того или иного ведомства информационно-телекоммуникационная система (ИТКС), призванная консолидировать в единый комплекс разнородные оперативно-розыскные и иные сведения об объектах (лицах, предметах, событиях и т.д.), представляющих интерес для противодействия киберпреступности.

На разных уровнях управленческой вертикали правоохранительных органов и спецслужб ИБДОРН призван интегрировать различные данные, необходимые для актуализации и расширения возможностей оперативно-розыскного учёта, представляющегося автору данной статьи в качестве «внутреннего функционального ядра» создаваемой ИТКС. Как уже подчёркивалось, в первую очередь вокруг него должны объединяться ведомственные криминалистические, криминологические и административные учёты. На следующем уровне следует систематизировать сведения, обладателями которых являются иные ведомства, не относящиеся к субъектам ОРД. Кроме того, дополнительный уровень должен обеспечивать консолидацию сведений, находящихся в ведении ведомств, учреждений, организаций или предприятий (независимо от форм их собственности), не относящихся к силовым структурам.

Как известно, одной из основных проблем организации работы по противодействию киберпреступности в России на общефедеральном уровне является информационная разобщённость государственных органов, уполномоченных на осуществление ОРД. Поэтому для совершенствования деятельности в рассматриваемом направлении необходимы совместные усилия всех ветвей и органов власти, ориентированные на достижении приемлемого уровня их информационного взаимодействия [23].

В этой связи следует создавать общую информационную инфраструктуру всех силовых ведомств, прямо или косвенно противодействующих киберпреступности. Для этого необходим единый межведомственный ИБДОРН. Структурно он должен состоять из объединённых ИБДОРН ведомств, участвующих в противодействии киберпреступности. Для того, чтобы реализовать эту идею на практике, следует обратиться к опыту деятельности специального органа, функционирующего в каждом государстве Европейского Союза (ЕС), – Национального департамента по оперативным данным (НДОД). Этот Департамент укомплектован представителями различных спецслужб и правоохранительных органов (пограничная служба, исправительные учреждения, таможенные органы, финансовая разведка, береговая охрана, полиция, службы разведки и безопасности, налоговые органы и др.), которые в рамках используемой в ЕС модели полицейской деятельности на основе оперативных данных и информации (ПДОДИ) имеют доступ к оперативным данным своего ведомства и правомочны осуществлять информационный обмен с представителями других заинтересованных органов, представленных в нём. НДОД

отвечает за ведение национальной базы оперативных данных о преступности, а также за проведение стратегического и оперативного анализа, включая оценку угроз, возникающих на национальном уровне. Он должен также оказывать помощь региональным (местным) подразделениям анализа оперативной информации. Этому способствует то обстоятельство, что на уровне государств-членов ЕС действуют взаимозависимые, совместимые между собой или одноплатформенные ИТКС, поддерживающие ИБД и предусматривающие наличие соответствующих механизмов защиты информации [24].

Таким образом, на Западе единое межведомственное информационное пространство правоохранительных органов давно уже создано и эффективно используется, в том числе для противодействия киберпреступности. Российской Федерации следует воспользоваться этим опытом и наряду с этим – активизировать развитие информационных технологий, основанных на использовании искусственного интеллекта. Этот же опыт может быть использован и для организации международного информационного взаимодействия в ходе противодействия транснациональной киберпреступности.

## Библиографический список


*1. Киберпреступники к 2025 году вооружатся технологиями для убийства людей // Securitylab.ru. 2021. 26 июля // URL: https://www.securitylab.ru/news/522696.php (дата обращения: 10.08.2024).*

*2. Россия в борьбе с терроризмом. Национальный антитеррористический комитет // URL: http://fb.ru/article/226311/rossiya-v-borbe-s-terrorizmom-natsionalnyiy-antiterroristicheskiy-komitet (дата обращения: 05.08.2024).*

*3. «Талибан»[1] – это надолго, и взаимодействовать с ними придётся: интервью Л.Г. Ивашова главному редактору еженедельника «Аргументов недели» А.И. Угланову // Аргументы недели. 2021. № 33 (777). 25–31 августа.*

*4. Кондрашов А. В виртуальной паутине. Как террористы и спецслужбы используют социальные сети // Аргументы недели. 2019. 16 мая. № 18(662). – С. 19.*

*5. Рябова В. Дональд Трамп поручил ускорить внедрение биометрической системы на границах США // URL: d-russia.ru/donald-tramp-poruchil-uskorit-vnedrenie-biometricheskoj-sistemy-na-granitsah-ssha.html (дата обращения: 02.08.2024).*

*6. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт. – М.: Международные отношения, 2020. – 285 с.*

*7. Когалов Ю. В Испании разработают приложение для поиска террористов // Российская газета. 2021. 4 августа.*

*8. Национальная стратегия развития искусственного интеллекта на период до 2030 года: утв. Указом Президента РФ от 10 октября 2019 г. № 490. П. 5, подп. «а», «б» // URL: http://static.kremlin.ru/media/events/files/ru/AH4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf (дата обращения: 10.08.2024).*

*9. Яковец Е.Н. Перспективы автоматизации информационно-аналитического обеспечения оперативно-розыскной деятельности органов внутренних дел // Информатизация правоохранительных систем: Сборник трудов международной научной конференции. – М.: Международная академия информатизации, 1999. – С. 122–126.*

*10. Яковец Е.Н. Оперативно-розыскная идентификация: монография / Под ред. В.М. Атмажитова и Б.Я. Нагиленко. – М.: Академия управления МВД России, 2003. – 176 с.*

*11. Яковец Е.Н. К вопросу о применении технологий искусственного интеллекта в аналитической работе российских правоохранительных органов и спецслужб // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий: Международная научно-практическая конференция, 18 апреля 2024 г.: сборник научных трудов / [сост. А.В. Константинов]. – М.: Московский университет МВД России имени В.Я. Кикотя, 2024. – 561 с. – С. 105–110.*


[1] Организация, запрещённая в России.

*12. Королёв Н. Нейросеть пустят по следу. Мэрия модернизирует систему распознавания лиц специально для МВД // Коммерсантъ. № 157. 2021. 2 сентября. – С. 7.*

*13. Овчинский В.С. Преступность. Футурологический взгляд // Завтра. 2016. 27 января // URL: http://zavtra.ru/blogs/prestupnost (дата обращения: 04.08.2024).*

*14. Ожегов С.И. Словарь русского языка / Под ред. Н.Ю. Шведовой. – М., 1985. – 797 с.*

*15. Временное положение о государственном учёте и регистрации баз и банков данных: утв. постановлением Правительства РФ от 28 февраля 1996 г. № 226 (утратило силу).*

*16. Гражданский кодекс РФ. Ч. IV. Ст. 1260, ч. 2.*

*17. Гражданский кодекс РФ. Ч. IV. Ст. 1261.*

*18. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. и доп.) // Российская газета. 2006. 29 июля.*

*19. Лопатин В.Н. Теоретико-правовые проблемы защиты единого информационного пространства и их отражение в системах российского права и законодательства // Актуальные проблемы информационного права: Материалы круглого стола 27 января 2000 г. в 2 т. – М.: ИМПЭ, 2000. Т. 2 // URL: http://www.for-expert.ru/problemy_inform_prava/15.shtml (дата обращения: 09.08.2024).*

*20. Российская газета. 2010. 22 октября.*

*21. Миллер Л.Ю. Интеграционный метод в теории и практике оперативно-розыскной деятельности органов внутренних дел: препринт монографии / Под общ. ред. д-ра юрид. наук, проф., засл. деятеля науки РФ Г.К. Синилова. – М.: Издательский дом Шумиловой И.И., 2008. – 24 с.*

*22. Денисов В.В., Горошко И.В., Яковец Е.Н. и др. Организация информационно-аналитического обеспечения оперативно-розыскной деятельности органов внутренних дел: учебное пособие. – М.: Академия управления МВД России, 2017. – 256 с.*

*23. Россия в борьбе с терроризмом. Национальный антитеррористический комитет // URL: http://fb.ru/article/226311/rossiya-v-borbe-s-terrorizmom-natsionalnyiy-antiterroristicheskiy-komitet (дата обращения: 05.08.2024).*

*24. OSCE Guidebookon Intelligence-Ledpolicing. [Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации] // Серия публикаций ДТНУ/ОСВПД. – Вена. 2017. Июль. – Т. 13. – 104 с.*