УДК 347.775:621.311.1

С. Ю. Воробьёв
Научно-исследовательское и проектно-изыскательское республиканское унитарное предприятие «Белэнергосетьпроект», 1-й Твердый пер., 5, 220037 Минск, Республика Беларусь

ОСУЩЕСТВЛЕНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ, НА ПРЕДПРИЯТИЯХ И В ОРГАНИЗАЦИЯХ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ РЕСПУБЛИКИ БЕЛАРУСЬ

Энергетика, как неотъемлемая часть белорусской экономики, переживает совместно с последней процесс цифровизации. Кибератаки при воздействии на информационные системы организаций и предприятий энергетической сферы представляют опасность как при производстве (передаче) электроэнергии, так и для сведений, содержащих коммерческую тайну. Применение мер по защите информации в соответствии с требованиями национального законодательства позволит минимизировать риск разглашения коммерчески ценных сведений, избежать судебных тяжб и минимизировать финансовые издержки.

Ключевые слова: энергетика; цифровизация; коммерческая тайна; защита информации; кибератаки.
Библиогр.: 30 назв.

S. Yu. Vorobyov
Research and Design and Survey Republican Unitary Enterprise “Belenergosetproekt”, 5 1st Hard lane, 220037 Minsk, the Republic of Belarus

IMPLEMENTATION OF MEASURES TO PROTECT INFORMATION CONSTITUTING A COMMERCIAL SECRETY AT ENTERPRISES AND ORGANIZATIONS OF THE ENERGY SECTOR OF THE REPUBLIC OF BELARUS

The energy sector, as an integral part of the Belarusian economy, is undergoing a digitalization process together with the latter. Cyberattacks affecting the information systems of organizations and enterprises in the energy sector pose a danger both to the production (transmission) of electricity and to information containing a commercial secret. The application of information protection measures in accordance with the requirements of national legislation will minimize the risk of disclosure of commercially valuable information, avoid litigation and minimize financial costs.

Key words: energy; digitalization; commercial secrets; information protection; cyber attacks.
Ref.: 30 titles.

Введение. Белорусская энергетика, будучи одной из основных отраслей национальной экономики, полностью подвержена процессам, протекающим в последней, в том числе цифровизации. Ахиллесовой пятой цифровизации является чувствительность к кибератакам, которые путем воздействия на автоматизированные системы объектов энергетики могут не только «отключать» от энергоснабжения предприятия и организации промышленности, социальные объекты (а то и целые регионы), но и «похищать» и (или) блокировать доступ к сведениям, составляющим коммерческую тайну (далее — КТ).

Проблемам противодействия кибератакам на объекты энергетики и минимизации их последствий посвящены работы белорусских и российских авторов С. Ю. Воробьёва, Е. А. Ханчевского, А. И. Белоуса, И. А. Костомахи, И. Н. Колоска, Е. С. Коркиной, М. Г. Головенчик, Г. Г. Краско, Г. Г. Головенчик, В. А. Северина, Д. Хитрых [1—7]. Вопросы обеспечения защиты сведений, содержащих КТ [в том числе от воздействия кибератак и их последствий в информационных системах (далее — ИС) организаций и предприятий], подымались в работах Д. А. Колбасина, А. М. Бокшиц, Р. Н. Ключко, Д. А. Бондарь, Г. Г. Камаловой, Н. М. Имомовой, И. В. Муравьева [8—13].

Вместе с тем в настоящее время отсутствует комплексное исследование, посвященное проблематике защиты информации, содержащей сведения, являющиеся КТ, на предприятиях и организациях энергетической отрасли.

Целью данной статьи является исследование текущего состояния защиты КТ на предприятиях и в организациях сферы национальной энергетики, проблемных вопросов, а также предложение мероприятий по повышению состояния защищенности коммерчески ценных сведений.

Материалы и методы исследования. При написании данной статьи использовались сравнительно-правовой, формально-юридический и методы системного анализа.

Были изучены и проанализированы работы по информационному, уголовному, гражданскому праву и нормативные правовые акты (в том числе технические нормативные правовые акты).

Результаты исследования и их обсуждение. Предприятия и организации, входящие в систему Министерства энергетики Республики Беларусь, при осуществлении производственной, хозяйственной, научной, проектной, а также иных видов деятельности создают, обрабатывают и хранят в ИС значительное количество сведений, содержащих КТ. Активно протекающий процесс цифровизации белорусской энергетики ставит перед собой в том числе прикладную задачу по обеспечению защиты информации, содержащей КТ, от кибератак, осуществляемых в отношении организаций.

Под кибератакой в соответствии с Указом Президента Республики Беларусь от 14.02.2023 № 40 «О кибербезопасности» (Указ № 40) понимается целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Аналогичная дефиниция содержится и в Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1.

Таким образом, вредоносное программное обеспечение, используемое в качестве орудия при проведении таргетированной, тщательно подготовленной кибератаки в отношении конкретной организации, может не только осуществить хищение информации, содержащей КТ, из ИС организации (т. е. совершить коммерческий шпионаж), но и модифицировать (изменить) содержимое данных сведений либо заблокировать к ним доступ.

Первые два десятилетия XXI века ознаменовались не только цифровизацией «всего и вся», но и стойкой милитаризацией цифрового пространства: государства активно и целенаправленно создают в составе национальных вооруженных сил структуры информационной безопасности, включая киберподразделения, основной задачей которых является проведение кибероперации. К текущему моменту реальный «боевой» опыт в киберпространстве имеют подразделения вооруженных сил США, Китая, КНДР, Ирана, Украины и др. Подразделение радиоэлектронной разведки «8200» Армии обороны Израиля (Цахал) известно не только участием в успешных кибератаках на иранские объекты атомной энергетической отрасли, но также и тем, что «питомцы» из «8200» являются зачинателями многочисленных прибыльных стартапов в сфере информационной безопасности, например, Check Point Software Technologies Ltd [14; 15].

Военно-политический блок НАТО, который является ударным тараном «Коллективного Запада», в 2016 году в Варшаве официально объявил киберпространство новой сферой проведения военных операций наряду с воздушной, сухопутной и морской [16]. Менее чем в 900 км от Минска (Таллин, Эстония) функционирует Центр передового опыта по

совместной киберзащите НАТО, на базе которого в рамках многочисленных учений и тренировок не только отрабатываются сценарии по действиям в киберпространстве, но и проводятся реальные операции.

США рассматривают киберпространство как поле боя и направляют усилия в рамках реализации своей государственной политики на полный контроль этой сферы [17]. В Соединенных Штатах циркулирует концепция так называемой «дешевой войны» (War on the Cheap), приверженцы которой утверждают, что один миллион долларов и 20 человек, проводя компьютерные атаки, могут обеспечить успех, сопоставимый с действиями многотысячной группировки войск [18].

В Америке крайне скрупулезно относятся к защите электроэнергетической системы от киберугроз в связи с чрезвычайной значимостью данного сектора национальной инфраструктуры. Министерство энергетики Соединенных Штатов наряду с такими «мощными» спецслужбами, как Центральное разведывательное управление, Федеральное бюро расследований, Агентство национальной безопасности, разведывательное управление Министерства обороны, входит в состав разведывательного сообщества США. В составе Министерства энергетики США действует Управление разведки и контрразведки, основными задачами которого являются научно-техническая разведка в ядерной области и защита ядерных секретов. В феврале 2016 года Министерство энергетики США официально объявило о создании Управления по кибербезопасности, энергетической безопасности и экстренному реагированию (структурно вошло в состав Управления разведки и контрразведки) [2].

Президент Республики Беларусь неоднократно обращал внимание на особую опасность такого элемента гибридной войны, используемого против Республики Беларусь, как кибератаки, их направленность на энергетические объекты, предприятия, банковскую систему, основные пункты жизнеобеспечения, отмечал, что целью кибератак является нанесение максимального ущерба экономике и дестабилизация общества [19—21]. Глава белорусского государства считает необходимым принятие международного правового акта о кибернападении, который предполагает как отказ от применения кибероружия, так и формирование системы контроля за его разработкой и использованием [22].

Необходимо отметить существенно возросшее количество киберпреступлений: ИС и ресурсы не только стали предметом преступлений, но и средством совершения последних. Так, цифровизация и виртуализация пространства способствовали как формированию преступности цифрового мира, так и отдельному типу злоумышленника, использующего новейшие информационно-коммуникационные технологии [23].

Белорусское законодательство содержит в себе целый ряд нормативных правовых актов, регулирующих вопросы защиты информации и информационной безопасности. Непосредственно правоотношения, связанные с правовой охраной и режимом КТ, регулируются Законом Республики Беларусь от 05.01.2013 № 16-З «О коммерческой тайне» (Закон о КТ), который под КТ понимает сведения технического, производственного, организационного, коммерческого, финансового и иного характера, в том числе секреты производства (ноу-хау), соответствующие требованиям Закона о КТ, в отношении которых установлен режим КТ — правовые, организационные, технические и иные меры, принятые в целях обеспечения конфиденциальности данных сведений. Последний возлагает на владельца информации, содержащей КТ, обязанность по принятию необходимых и достаточных мер для обеспечения конфиденциальности вышеуказанных сведений. Под защитой информации в соответствии с Законом Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (далее — Закон № 455) понимается комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. При этом ст. 17 Закона № 455 относит КТ к информации, распространение и (или) предоставление которой ограничено.

Таким образом, информация, обрабатываемая в объектах информационной инфраструктуры предприятий национальной энергетической отрасли и содержащая КТ, должна быть надежно защищена как от внешних, так и от внутренних угроз. Правовые и организационные основы технической и криптографической защиты информации подобного рода изложены в Указе Президента Республики Беларусь от 16.04.2013 № 196 «О совершенствовании государственного регулирования в области защиты информации» [в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449 (Указ № 196)] меры по реализации последнего содержатся в приказе Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ) от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (Приказ № 66).

Регулятором в лице ОАЦ устанавливаются более жесткие требования по защите ИС, в которых обрабатывается служебная информация ограниченного распространения (ДСП — для служебного пользования), по сравнению с ИС, в которых обрабатывается КТ (пп. 6.4, 6.6, 7.7, 7.17, 7.18 приложения 3 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному Приказом № 66), несмотря на то, что КТ и ДСП Законом № 455 отнесены к информации, распространение и (или) предоставление которой ограничено.

Национальным законодательством предусмотрена ответственность за нарушение конфиденциальности сведений, составляющих КТ. Так, к работнику организации могут быть применены следующие виды ответственности: дисциплинарная, материальная, гражданско-правовая, административная, уголовная.

При этом привлечение к административной или уголовной ответственности не исключает наложения на виновное лицо дисциплинарного взыскания с одновременным привлечением к материальной или гражданско-правовой ответственности. Контрагентов и иных третьих лиц возможно привлечь к гражданско-правовой, административной и уголовной ответственности соответственно. Представляет интерес тот факт, что в случае разглашения ДСП виновный работник организации может быть привлечен к дисциплинарной ответственности, а за аналогичные действия в отношении КТ — к административной или уголовной.

Правоприменительная практика привлечения к ответственности за разглашение КТ в Республике Беларусь сформирована слабо, что, по мнению правоохранительных органов, обусловлено правовой неграмотностью лиц, отвечающих за соблюдение режима КТ [24]. Как правило, руководители не предпринимают надлежащих мер для введения во вверенном предприятии (организации) режима КТ, не разрабатывают механизма по соблюдению работниками последнего. Это приводит к тому, что разнообразные сведения, связанные с производством, технологией, инновациями и другими вопросами деятельности предприятия, на разработку которых затрачены значительные денежные средства и ресурсы, становятся достоянием конкурентов [25]. Так, в 2023 году работниками правоохранительных органов было предотвращено разглашение коммерческих сведений о препаратах, на разработку и испытание которых было потрачено в общей сложности более 1 млн белорус. руб. [26].

В целях надлежащего обеспечения безопасности сведений, включающих в себя КТ, в организации необходимо выполнить требования, содержащиеся в Законе о КТ:

– определить состав сведений, подлежащих охране в режиме КТ;

– установить порядок обращения с носителями КТ, а также контроль за соблюдением данного порядка;

– вести учет лиц, получивших доступ к КТ;

– истребовать обязательства о неразглашении КТ у работников, получающих доступ к последней;

– заключить соглашения о конфиденциальности с контрагентами (при необходимости);

– определить работников, ответственных за принятие мер по обеспечению конфиденциальности сведений, составляющих КТ.

Вышеперечисленные требования относятся к режиму установления КТ, алгоритм которого подробно описан в источнике [27].

Закон о КТ позволяет владельцу тайны применять технические средства и иные методы для обеспечения защиты коммерчески ценных сведений. Наиболее подходящим решением данной задачи является применение системы предотвращения утечек конфиденциальной информации (DLP-система) [28; 29]. Так как DLP-система является средством защиты информации (СЗИ), то в соответствии с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» должно быть осуществлено подтверждение данного СЗИ соответствию в Национальной системе подтверждения соответствия Республики Беларусь.

Так, ИС, в которых обрабатывается КТ, согласно Указу № 196 и Закону № 455, должны иметь аттестованную в соответствии с Приказом № 66 систему защиты информации.

Практика показывает, что в организациях и на предприятиях энергетической отрасли сталкиваются с затруднениями при работе с коммерчески ценными сведениями, отнесенными к КТ. Наибольшее затруднение вызывает отнесение информации к категории «Коммерческая тайна»: зачастую под данную категорию относят сведения, перечисленные в ст. 17 Закона № 455, но не являющиеся КТ (например, персональные данные, служебная информация ограниченного распространения). Нередки случаи расширительного включения под вышеуказанную категорию любой информации, имеющей отношение к деятельности организации, но не соответствующей требованиям, предъявляемым Законом о КТ, к данным сведениям (например, нередкими являются случаи отнесения к категории КТ сведений, составляющих размер заработной платы работников, их численность или данные бухгалтерской отчетности). Также не всегда истребуются у работников, получивших доступ к КТ, обязательства о неразглашении, с контрагентами не заключаются соглашения о конфиденциальности, не определяются работники, ответственные за принятие мер по обеспечению конфиденциальности сведений, составляющих КТ.

В настоящее время не все организации белорусской энергетики осуществили комплекс мероприятий по технической и криптографической защите информации, что приводит к тому, что КТ обрабатывается в ИС с не аттестованной установленным ОАЦ порядке системой защиты информации (нельзя забывать про персональную ответственность, возложенную Указом № 40 на руководителей организации, в части обеспечения кибербезопасности последней) [30].

Предупреждение нарушения требований законодательства, регулирующего вопросы защиты информации в части обработки конфиденциальной информации (в том числе сведений, содержащих КТ) в ИС, а также утечки данных сведений, достигается путем выполнения комплекса организационных, правовых и технических мероприятий. В качестве примера приведем обстановку, сложившуюся по состоянию на текущий момент времени на одном из предприятий, структурно входящем в государственное производственное объединение электроэнергетики «Белэнерго» Министерства энергетики Республики Беларусь. В рамках производственной деятельности в ИС предприятия накапливается значительное количество проектной, технической и технологической, изыскательской, коммерческой, научной и иной информации, представляющей коммерческую ценность для предприятия, прежде всего в силу ее неизвестности третьим лицам в энергетической отрасли.

Так, на предприятии действует Положение о коммерческой тайне, разработанное и утвержденное в 2013 году, с изменениями и дополнениями 2015 года. Данным документом закреплен Перечень сведений, составляющих коммерческую тайну предприятия, а также Обязательство работника предприятия о неразглашении сведений, содержащих коммер-

ческую тайну (Обязательство). Требования данного положения доводятся до каждого вновь принимаемого работника под роспись с истребованием Обязательства о неразглашении сведений, содержащих коммерческую тайну предприятия.

С положительной стороны представляется целесообразным отметить пункт Обязательства, в котором работник предприятия обязуется в случае необходимости пройти психофизиологическое исследование с использованием полиграфа в целях контроля лояльности к предприятию, профилактики хищений, сговоров, несанкционированной передачи КТ.

В настоящее время осуществляется разработка редакции Положения (проект) с актуализированным Перечнем сведений, составляющих коммерческую тайну предприятия. В проекте будут конкретизированы должностные лица и структурные подразделения предприятия, участвующие в обеспечении применения мероприятий по защите сведений, содержащих КТ, закреплено типовое соглашение о конфиденциальности (с контрагентами).

В целях повышения состояния защищенности ИС предприятия, контроля за неукоснительным исполнением работниками требований законодательства и локальных правовых актов, регулирующих вопросы информационной безопасности и защиты информации, запланированного отнесения ИС предприятия к классу 3-дсп (ИС, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных) намечена к приобретению и внедрению DLP-система.

Заключение. Белорусская энергетика проходит процесс цифровой трансформации вместе с иными отраслями национальной экономики. Угрозу данному процессу представляет милитаризация цифрового пространства, создание странами киберподразделений в составе национальных вооруженных сил, осуществление кибератак в отношении экономических объектов суверенного миролюбивого белорусского государства и прежде всего в отношении объектов энергетической отрасли. Глава белорусского государства уделяет самое непосредственное внимание вопросам информационной безопасности и противодействию кибератакам.

Организации и предприятия, входящие в Белорусскую энергетическую систему, в процессе практической деятельности осуществляют обработку информации, представляющей коммерческую ценность, которая в соответствии с действующим законодательством относится к информации ограниченного распространения — КТ. Применение правовых, организационных и технических мер защиты последней имеет ряд особенностей (отнесение сведений, содержащих конфиденциальную, коммерчески ценную информацию, к вышеуказанной категории, обеспечение действия режима КТ, аттестация ИС, в которых обрабатывается последняя, и т. д.). Применение режима КТ в деятельности организаций национальной энергетики имеет ряд проблемных вопросов, отсутствие своевременного решения которых может привести к наступлению неблагоприятных последствий за необеспечение законодательных требований, регулирующих сферу защиты информации по данному вопросу. По мнению правоохранительных органов, основной причиной привлечения за разглашение сведений, составляющих КТ организаций, причин и условий, способствующих совершению правонарушений в данной сфере, является правовая неграмотность должностных лиц [24].

На предприятии проводится комплекс мероприятий организационного, нормативного и технического характера, направленных на предупреждение нарушений, связанных с обеспечением режима КТ.

Вышеизложенное позволяет сделать вывод о том, что корректное применение норм действующего законодательства Республики Беларусь, регулирующего вопросы защиты информации и информационной безопасности, а также мероприятий, предусмотренных в них, в том числе повышение правовой грамотности лиц, отвечающих за соблюдение режима КТ, позволит защитить организациям энергетической отрасли коммерчески ценную информацию, избежать судебных тяжб, сохранить деловую репутацию, избежать финансовых издержек и проверок правоохранительных органов, а также укрепить дисциплинированность и правопослушное поведение работников.

Список цитируемых источников

1. *Воробьёв, С. Ю.* Кибератаки на критически важные объекты энергетики как источник угроз национальной безопасности / С. Ю. Воробьёв, Е. А. Ханчевский // Энергетическая стратегия. — 2024. — Т. 102, № 6. — С. 33—36.

2. *Белоус, А. И.* Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — М. ; Вологда : Инфра-Инженерия, 2020. — 644 с.

3. *Костомаха, И. А.* Методы удалённого проникновения злоумышленника в технологические сегменты сети предприятий электроэнергетики / И. А. Костомаха // Энергетик. — 2024. — № 8. — С. 19—22.

4. *Колосок, И. Н.* Анализ кибербезопасности объектов энергетики с учётом механизма и кинетики нежелательных процессов / И. Н. Колосок, Е. С. Коркина // Энергетик. — 2024. — № 2. — С. 3—8.

5. *Головенчик, М. Г.* Проблемы кибербезопасности умных городов / М. Г. Головенчик, Г. Г. Краско, Г. Г. Головенчик // Наука и инновации. — 2020. — № 12 (214). — С. 51—57.

6. *Северин, В. А.* Проблемы правового регулирования и методического обеспечения защиты информации в организациях ТЭК / В. А. Северин // Проблемы экономики и юридической практики. — 2022. — Т. 18, № 2. — С. 96—103.

7. *Хитрых, Д.* О цифровой трансформации энергетической отрасли / Д. Хитрых // Энергетическая политика. — 2021. — № 10 (164). — С. 76—89.

8. *Колбасин, Д. А.* Теоретико-правовая характеристика защиты коммерческой тайны, ее характерные особенности / Д. А. Колбасин, А. М. Бокшиц // Вестник Академии МВД Республики Беларусь. — 2017. — Т. 33, № 1. — С. 148—151.

9. *Ключко, Р. Н.* Информационный суверенитет государства: от доктринальных подходов к уголовно-правовым гарантиям обеспечения / Р. Н. Ключко // Юстиция Беларуси. — 2024. — № 9. — С. 43—46.

10. *Бондарь, Д. А.* Новации законодательства Республики Беларусь о кибербезопасности в контексте охраны коммерческой тайны и противодействия коммерческому шпионажу / Д. А. Бондарь // Стратегия развития экономики Беларуси: вызовы, инструменты и перспективы : сб. науч. ст. Междунар. науч.-прак. конф. : в 2 т. — Мн., 2024. — С. 493—498.

11. *Камалова, Г. Г.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : автореф. дис. … д-ра юрид. наук : 12.00.13 / Камалова Гульфия Гафиятовна ; Ин-т государства и права РАН. — М., 2020. — 52 с.

12. *Имомова, Н. М.* Особенности правового регулирования коммерческой тайны в зарубежных странах / Н. М. Имомова // Вестник Таджикского национального университета. Серия социально-экономических и общественных наук. — 2024. — № 7. — С. 235—240.

13. *Муравьев, И. В.* Коммерческая тайна как объект гражданского права / И. В. Муравьев // Вестник Могилевского института МВД. — 2024. — № 1 (9). — С. 55—59.

14. *Белоус, А. И.* Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — М. ; Вологда : Инфра-Инженерия, 2020. — 692 с.

15. *Фасман, Д.* Общество контроля : как сохранить конфиденциальность в эпоху тотальной слежки / Д. Фасман. — М. : Эксмо, 2023. — 368 с.

16. *Белоус, А. И.* Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — М. : Техносфера, 2021. — 482 с.

17. *Харрис, Ш.* Кибервойна@: Пятый театр военных действий / Ш. Харрис ; пер. с англ. — М. : Альпина нон-фикшн, 2020. — 390 с.

18. *Бартош, А. А.* Гибридная война : учеб. пособие / А. А. Бартош. — М. : КНОРУС, 2023. — 306 с.

19. Встреча с руководящим и оперативным составом органов госбезопасности // Официальный сайт Президента Республики Беларусь. — URL: https://president.gov.by/ru/events/vstrecha-s-rukovodyashchim-i-operativnym-sostavom-organov-gosbezopasnosti (дата обращения: 20.04.2025).

20. Совещание по теме кибербезопасности // Официальный сайт Президента Республики Беларусь. — URL: https://president.gov.by/ru/events/soveshchanie-po-teme-kiberbezopasnosti (дата обращения: 20.04.2025).

21. Встреча с активом Могилевской области // Официальный сайт Президента Республики Беларусь. — URL: https://president.gov.by/ru/events/vstrecha-s-aktivom-mogilevskoy-oblasti (дата обращения: 20.04.2025).

22. II Минская международная конференция по евразийской безопасности // Официальный сайт Президента Республики Беларусь. — URL: https://president.gov.by/ru/events/ii-minskaa-mezdunarodnaa-konferenciа-po-evrazijskoj-bezopasnosti (дата обращения: 20.04.2025).

23. *Стальбовский, В. В.* Дуализм криминологической модели личности преступника: реальное и виртуальное измерение / В. В. Стальбовский, Т. И. Вишневская // Юстиция Беларуси. — 2025. — № 1. — С. 52—60.

24. *Александров, В.* Промышленный шпионаж. Впервые за 10 лет дело дошло до суда / В. Александров // Аргументы и факты в Беларуси. — 2017. — 5 дек. — С. 12.

25. Коммерческий шпионаж и преступления против информационной безопасности: прокуратура Партизанского района Минска поддержала обвинение по уголовному делу // Официальный сайт Генеральной прокуратуры Республики Беларусь. — URL: https://prokuratura.gov.by/ru/media/novosti/nadzor-za-resheniyami-po-

ugolovnym-i-grazhdanskim-delam/kommercheskiy-shpionazh-i-prestupleniya-protiv-informatsionnoy-bezopasnosti-prokuratura-partizanskog/ (дата обращения: 20.04.2025).

26. Коммерческую тайну фармпредприятия на сумму более Br1 млн едва не вывезла за границу борисовчанка // Белорусское телеграфное агентство. — URL: https://belta.by/regions/view/kommercheskuju-tajnu-farmpredprijatija-na-summu-bolee-br1-mln-edva-ne-vyvezla-za-granitsu-borisovchanka-601981-2023/ (дата обращения: 20.04.2025).

27. Алгоритм установления режима коммерческой тайны в организации // ilex : информ. правовая система. — URL: https://ilex-private.ilex.by/view-document/BEPBI/82303/%D0%BA%D0%BE%D0%BC%D0%BC%D0%B5%D1%80%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F%20%20%D1%82%D0%B0%D0%B9%D0%BD%D0%B0?searchKey=prfq&docSwitcherKey=88vi&searchPosition=4#M100121 (дата обращения: 20.04.2025).

28. *Глушков, В. А.* Проблема легализации данных собранных с использованием систем DLP, SIEM и DCAP на предприятии и организации / В. А. Глушков // Юридическая наука и практика. — 2024. — № 4. — С. 50—57.

29. *Тищенко, А. П.* Коммерческая тайна и технологии ее защиты / А. П. Тищенко // Молодая аграрная наука : материалы Междунар. науч.-практ. конф., Майкоп, 16 мая 2024 г. — Майкоп : Магарин Олег Григорьевич, 2024. — С. 392—395.

30. *Мячин, И. В.* Юридическая ответственность владельцев критически важных объектов информатизации: проблемы эффективности и пути совершенствования / И. В. Мячин // Предварительное расследование. — 2024. — № 1 (15). — С. 54—60.

Поступила в редакцию 10.11.2025.