УДК 343.241
ББК Х408.1
DOI: 10.14529/law210309

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Ю. А. Морозова
Южно-Уральский государственный университет, г. Челябинск

Статья посвящена правовой регламентации обеспечения информационной безопасности промышленных предприятий. Особенно это актуально для Челябинской области как промышленного региона, на территории которой расположены объекты критической информационной инфраструктуры. Информационная безопасность являясь динамичной компонентой Индустрии 4.0 требует наличия не только технической оснащенности промышленного предприятия, позволяющей выявлять атаки и прогнозировать возможные угрозы, но и соответствующих правовых инструментов для реализации мер безопасности. Проведен подробный анализ нормативно-правовых актов, закрепляющих основы обеспечения информационной безопасности в промышленной сфере. Сделан вывод о необходимости усиления локальной регламентации внутренними инструкциями деятельности по выявлению угроз и устранению последствий атак.

Ключевые слова: цифровые технологии, компоненты цифровой индустрии, информационная безопасность промышленных предприятий, Челябинская область, промышленный регион.

В современном мире важнейшим конкурентным фактором промышленного сектора является развитие информационных технологий и внедрение инноваций[1]. Такая цифровая трансформация оказывает значительное влияние на промышленный сектор. Новые прорывные технологии (breakthrough technologies), появившиеся вследствие Четвертой промышленной революции, обусловили начало «гонки за инновациями» [4, с. 42]. Не только новые цифровые технологии представляют интерес для злоумышленников, но и текущая деятельность предприятий.

Проблема резкой динамики киберинцидентов в исследуемой сфере является крайне актуальной и злободневной, поскольку промышленные предприятия по всему миру ежегодно несут колоссальные потери, ставшие следствием кибератак [9; 11]. Однако на текущем этапе моделирование киберрисков, в том числе в промышленном секторе, не достаточно развито ввиду определенной новизны проблемы, отсутствия глобальной исторической практики борьбы с кибератаками на уровне отдельных организаций, постоянно динамизирующих и изменяющихся способов реализации атак, а также сложности в анализе и оценке данного вида рисков.

По данным исследования Positive Technologies [1] – компании, специализирующейся на разработке программного обеспечения в области информационной безопасности, количество киберинцидентов в 2020 году выросло на 51 % по сравнению с 2019 годом. При этом 70 % атак носили целенаправленный характер. Количество инцидентов на промышленных предприятиях увеличилось на 91 %, и чаще всего злоумышленники в качестве вредоносного программного обеспечения применяли шифровальщики. В 2020 году зафиксированы атаки на объекты критически значимой инфраструктуры, приводившие к отключению электроэнергии, а также попытки атак на системы водоснабжения. Такие инциденты имеют долгосрочные последствия, начиная от репутационых рисков и заканчивая финансовым ущербом.

Анализ сложившейся ситуации информационной безопасности промышленных предприятий в Челябинской области показывает, что часть инцидентов оценивается только на основе индивидуальных знаний процессов и, как результат, не воспринимается сотрудниками всерьез. Порой методы выявления атак и устранения их последствий основаны на субъ-

[1] Исследование выполнено при финансовой поддержке РФФИ и Челябинской области в рамках научного проекта № 20-411-740013 «Правовое регулирование внедрения и развития компонентов цифровой индустрии (Индустрии 4.0) в промышленном регионе».

ективном восприятии и не регламентированы локальными актами. Это подтверждают данные проведенного нами социологического исследования вопросов реализации протоколов информационной безопасности на нескольких промышленных предприятиях Челябинской области. Так, установлено, что не все уполномоченные сотрудники знакомы с директивами по кибербезопасности (информационной безопасности), что закономерно влечет несоблюдение нормативных требований. В качестве возможных причин кибератаки на предприятие опрошенные сотрудники называли следующие: нарушения технологического (производственного) процесса – 61 %; остановка бизнес-процессов и вывод инфраструктуры – 59 %; получение конфиденциальной информации (шпионаж) – 57 %; удар по репутации – 45 %; незаконное завладение денежными средствами, находящимися на счетах промышленного предприятия или его контрагентов, – 37 %.

Значительную роль в обеспечении информационной безопасности промышленного сектора играют правовые инструменты. В России уже сформированы частично методы защиты информации на государственном уровне [5]. Существующие нормы права регулируют отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации. Нормативные акты определяют базовую терминологию, сферу действия, охраняемые объекты и круг регулируемых отношений.

Для качественного понимания предмета исследования необходимо раскрыть существующий терминологический аппарат для формирования четкой взаимосвязи киберрисков с промышленным комплексом. В узком смысле под кибербезопасностью понимают совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных [7]. Кибератака – предумышленно организованная совокупность действий с участием программно-технических средств, направленная на нанесение экономического, технического или информационного ущерба [2, с. 39].

Русско-американский словарь терминов и определений в сфере обеспечения кибербезопасности определяет кибербезопасность – свойство киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз [6].

Согласно опубликованному Международной организацией по стандартизации и Международной электротехнической комиссией стандарту в области кибербезопасности ISO/IEC 27032:2012 термин «кибербезопасность» характеризуется как безопасность в киберпространстве или как сохранения конфиденциальности, целостности, доступности и других важных свойств активов пользователей и организации [10]. В названном стандарте также охарактеризована взаимосвязь терминов «кибербезопасность», «сетевая безопасность», «безопасность приложений», «безопасность в Интернете» и «безопасность ключевых систем информационной инфраструктуры». Кибератаки, существующие в киберпространстве и требующие защиты, подразделяются на физические (существуют в реальном мире) и виртуальные (существуют только в киберпространстве) [8, с. 185–205].

Таким образом, информационную безопасность можно рассматривать как комплекс действий стратегического характера, направленный на защиту от нанесения экономического, технического или информационного ущерба вследствие угроз, совершаемых с помощью программно-технических средств, а также в результате ежедневной работы с информационными сетевыми технологиями.

Нормативная база нашей страны содержит понятие информационной безопасности. Так, в Доктрине информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646 (далее – Доктрина), определено как информационная безопасность Российской Федерации определяется как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Доктрина, являясь документом стратегического планирования в сфере обеспечения национальной безопасности России, направлена на формирование го-

сударственной политики и развития общественных отношений в области обеспечения информационной безопасности. Согласно данному документу одним из национальных приоритетов Российской Федерации в информационной сфере является обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры и единой сети электросвязи Российской Федерации. Доктрина предусматривает стратегические цели и основные направления обеспечения информационной безопасности. Одним из таких направлений является повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления.

Законодатель предусмотрел перечень правовых инструментов, направленный на обеспечение информационной безопасности в промышленной сфере. В той или иной мере подход к обеспечению информационной безопасности в промышленных отраслях Российской Федерации определяются федеральными законами от 21 июля 1993 г. № 5485-1 «О государственной тайне», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации», от 27 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» указывает, что критическая информационная инфраструктура – это совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей и систем. В п. 8 ст. 2 указанного закона перечислены субъекты критической информационной структуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей. В Челябинской области как промышленном регионе, значительная часть предприятий используют автоматизированные системы управления, а соответственно подпадают в сферу действия Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

Положительную сторону Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» в обеспечении информационной безопасности исследуемой сферы отмечает Д. Волков. При этом он подчеркивает, что наличие закона от реальных атак, естественно, не защищает [3, с. 18].

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, (утв. Указом Президента РФ от 9 мая 2017 г. № 203 (далее – Стратегия), также закрепляет понятие критической информационной инфраструктуры Российской Федерации как совокупности объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой. При этом к объектам критической информационной инфраструктуры согласно положениям Стратегии относятся информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта,

связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

В п. 31 Стратегии прописано, что для защиты данных в Российской Федерации необходимо совершенствовать нормативно-правовое регулирование в сфере обеспечения безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий, уровень которого должен соответствовать развитию этих gentехнологий и интересам общества. Данное положение подчеркивает необходимость своевременной актуализации существующих и выработки новых правовых инструментов и механизмов информационной безопасности промышленного сектора как на федеральном уровне, так и на уровне локальном.

Анализируя правовую регламентацию обеспечения информационной безопасности промышленных предприятий, необходимо сказать об указах Президента РФ и ведомственных нормативных актах, регламентирующих отдельные вопросы рассматриваемой сферы. Так, Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствии компьютерных атак на информационные ресурсы Российской Федерации» возложил на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также определил основные задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Важным правовым инструментом обеспечения защиты персональных данных является Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Данный нормативный акт предусматривает требования к защите персональных данных при их обработке в информационных системах и уровни защищенности таких данных.

Отдельные акты принимаются Федеральной службой по техническому и экспортному контролю, реализующей государственную политику, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности. Подобные документы формируют в Российской Федерации комплексную систему требований по обеспечению информационной безопасности для информационных систем различного уровня.

Постановлением Правительства РФ от 2 октября 2013 г. № 861 утверждены Правила информирования субъектами топливно-энергетического комплекса об угрозах совершения и о совершении актов незаконного вмешательства на объектах топливно-энергетического комплекса, которые обязывают должностное лицо субъекта топливно-энергетического комплекса представлять информацию об угрозе совершения и о совершении акта незаконного вмешательства на объект топливно-энергетического комплекса в уполномоченные государственные органы. К таким органам относятся территориальные органы Министерства внутренних дел Российской Федерации, органы федеральной службы безопасности, территориальный орган Федеральной службы войск национальной гвардии Российской Федерации, Министерство Российской Федерации по делам гражданской обороны и др. Правила требуют незамедлительно, но не позднее суток сообщить информацию о возможной угрозе или совершенной атаке.

Подводя итог, отметим, что анализ нормативно-правового регулирования информационной безопасности промышленных предприятий России и выработанная система защиты критической информационной инфраструктуры показывает большой спектр правовых инструментов. Это и конкретные правила категорирования объектов критической информационной инфраструктуры, к которой относятся многие промышленные предприятия, обязанности субъектов критической информационной инфраструктуры, порядок их взаимодействия с государственными органами.

Следовательно, имеющиеся правовые механизмы, с одной стороны, формируют логичную систему обеспечения информационной безопасности промышленных предприятий региона, с другой – далеко не все промышленные предприятия на локальном уровне дополнительно регламентируют внутрен-

ними инструкциями деятельность по выявлению угроз и устранению последствий атак.

Литература

1. Актуальные киберугрозы: итоги 2020 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/.

2. Алпеев, А. С. Терминология безопасности: кибербезопасность, информационная безопасность / А. С. Алпеев // Вопросы кибербезопасности. – 2014. – № 5 (8). – С. 39–42.

3. Волков, Д. Threat Intelligence выходит на новый уровень / Д. Волков // Информационная безопасность. – 2020. – № 6. – С. 16–20.

4. Громова, Е. А. Создание цифровых технологий в рамках государственно-частного партнерства: опыт БРИКС / Е. А. Громова // Вестник Южно-Уральского государственного университета. Серия «Право». – 2019. – Т. 19. – № 1. – С. 42–45.

5. Дурницин, И. Развитие права в сфере информационной безопасности / И. Дурницин. URL: https://www.garant.ru/ia/opinion/.

6. Русско-американский словарь терминов и определений в сфере информационной безопасности. URL: https://digital.report/cybersecurity-terminology/.

7. Что такое кибербезопасность? URL: https://www.kaspersky.ru/resource-center/ definitions/what-is-cyber-security.

8. Boes S. Fighting cybercrime: joint effort / S. Boes, E.R. Leukfeldt // Ciber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. Cincinnati: Springer. 2016. Pp. 185–205.

9. Hi-Tech Crime Trends 2020/2021. Available at: www.group-ib.ru/blog/trends20_21.

10. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. Available at: www.iso.org/ru/standard/73906.html.

11. Menze T. Кибербезопасность систем промышленной автоматизации в 2019 году. URL: https://ics.kaspersky.ru/media/Kaspersky-ARC-ICS-2019-Trend-Report-Ru.pdf.

Морозова Юлия Аскаровна – кандидат юридических наук, доцент кафедры уголовного процесса, криминалистики и судебной экспертизы, Южно-Уральский государственный университет, г. Челябинск. E-mail: girl.juliy@mail.ru.

Статья поступила в редакцию 26 мая 2021 г.

DOI: 10.14529/law210309

LEGAL REGULATION OF PROVIDING INFORMATION SECURITY OF INDUSTRIAL ENTERPRISES IN THE RUSSIAN FEDERATION

Yu. A. Morozova
South Ural State University, Chelyabinsk, Russian Federation

The article is devoted to the legal regulation of ensuring information security of industrial enterprises. This is especially true for the Chelyabinsk region as an industrial region, on the territory of which objects of critical information infrastructure are located. Information security, being a dynamic component of Industry 4.0, requires not only the technical equipment of an industrial enterprise to detect attacks and predict possible threats, but also appropriate legal instruments to implement security measures. A detailed analysis of the normative legal acts establishing the basis for ensuring information security in the industrial sphere is carried out. It is concluded that it is necessary to strengthen local regulation with internal instructions for identifying threats and eliminating the consequences of attacks.

Keywords: digital technologies, components of the digital industry, information security of industrial enterprises, the Chelyabinsk region, industrial region.

References

1. *Aktual'nye kiberugrozy: itogi 2020 goda* [Current cyber threats: results of 2020]. Available at: www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/.

2. Alpeev A. S. [Terminology of security: cybersecurity, information security]. *Voprosy kiberbezopasnosti [Questions of Cybersecurity]*, 2014, no. 5 (8), pp. 39–42. (in Russ.)

3. Volkov D. [Threat Intelligence goes to a new level]. *Informacionnaâ bezopasnost' [Information Security]*, 2020, no. 6, pp. 16–20. (in Russ.)

4. Gromova E. A. [Creating Digital Technologies in the framework of public-private partnership: the experience of BRICS]. *Vestnik Ûžno-Ural'skogo gosudarstvennogo universiteta. Seriâ «Pravo» [Bulletin of the South Ural State University. Series "Law"]*, 2019, Vol. 19, no. 1, pp. 42–45. (in Russ.)

5. Durnicin I. *Razvitie prava v sfere informacionnoj bezopasnosti* [Development of law in the field of information security]. Available at: www.garant.ru/ia/opinion/.

6. *Russko-amerikanskij slovar' terminov i opredelenij v sfere informacionnoj bezopasnosti* [Russian-American Dictionary of Terms and Definitions in the Field of Information Security]. Available at: digital.report/cybersecurity-terminology/.

7. *Čto takoe kiberbezopasnost'?* [What is cybersecurity?]. Available at: www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.

11. Menze T. *Kiberbezopasnost' sistem promyšlennoj avtomatizacii v 2019 godu* [Cybersecurity of industrial automation systems in 2019]. Available at: ics.kaspersky.ru/media/Kaspersky-ARC-ICS-2019-Trend-Report-Ru.pdf.

Yulia Askarovna Morozova – Candidate of Sciences (Law), Associate Professor of the Department of Criminal Process, Criminalistics and Judicial Examination, South Ural State University, Chelyabinsk, Russian Federation. E-mail: girl.juliy@mail.ru.

Received 26 May 2021.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Морозова, Ю. А. Правовое регулирование обеспечения информационной безопасности промышленных предприятий в Российской Федерации / Ю. А. Морозова // Вестник ЮУрГУ. Серия «Право». – 2021. – Т. 21, № 3. – С. 55–60. DOI: 10.14529/law210309.

FOR CITATION

Morozova Yu. A. Legal regulation of providing information security of industrial enterprises in the Russian Federation. *Bulletin of the South Ural State University. Ser. Law*, 2021, vol. 21, no. 3, pp. 55–60. (in Russ.) DOI: 10.14529/law210309.