УДК 342.951+351.81

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ

Д.В. Перевалов

Государственное учреждение образования
«Институт пограничной службы Республики Беларусь»,
ул. Славинского 4, г. Минск, 220103, Беларусь

В статье рассматриваются отдельные проблемные вопросы правового регулирования обеспечения безопасности критически важных объектов информатизации Республики Беларусь в современных условиях. В качестве решение имеющихся проблем предлагается на основе подходов, сложившихся в юридической науке, осуществить восполнение пробелов в законодательстве, регулирующим отношения в области обеспечения безопасности критически важных объектов информатизации, административную и уголовную ответственность за правонарушения в данной области. В первую очередь это относится к регулированию импортозамещения оборудования и программного обеспечения для соответствующих категорий объектов.

***Ключевые слова*:** критически важные объекты информатизации, обеспечение безопасности, правовое регулирование, кибербезопасность, хакерские атаки, административные правонарушения в области информации, преступления против компьютерной безопасности.

SEPARATE PROBLEMS OF LEGAL REGULATION SAFETY CRITICAL OBJECTS OF INFORMATIZATION AT THE PRESENT STAGE

D.V. Perevalov

State Educational Institution
«Institute of the Border Service of the Republic of Belarus»,
4 Slavinsky street, Minsk, 220103, Belarus

The article deals with certain problematic issues of legal regulation of ensuring the security of critically important objects of informatization of the Republic of Belarus in modern conditions. As a solution to the existing problems, it is proposed, on the basis of approaches that have developed in legal science, to fill in the gaps in the legislation governing relations in the field of ensuring the security of critical informatization objects, administrative and criminal liability for offenses in this area. First of all, this applies to the regulation of import substitution of equipment and software for the relevant categories of objects.

Keywords: critical objects of informatization, security, legal regulation, cybersecurity,

hacker attacks, administrative offenses in the field of information, crimes against computer security.

Введение

Современное общество характеризуется переходом к качественно новому состоянию – информационному обществу, в котором отмечается подавляющее влияние новых информационных технологий на все сферы общественной жизни, обусловленное лавинообразным развитием систем передачи данных. Разработка новейших технологий, которые призваны обеспечить потребности личности и общества в информации, влечет за собой поступательное развитие новых средств коммуникации, рост их производства и модификации. Вместе с тем, трансформация общества в условиях информационной революции формирует новые угрозы информационной безопасности как отдельных государств, так и конкретных регионов. Актуальной данная проблема является и для государств – членов Организации Договора о коллективной безопасности, в том числе и Республики Беларусь.

Так, число кибератак в мире в 2021 г. выросло на *50 %* по сравнению с 2020 г. В России количество атак увеличилось на *54 %*. Экспертами отмечается, что большая часть кибератак в 2021 г. пришлась на государственные учреждения – почти *20 %* преступлений. В *10 %* случаев жертвами кибермошенников становятся промышленные предприятия, по *8 %* атак направлены на медицинские и образовательные учреждения, а также финансовые организации [1], [2].

При этом хакерским атакам во многих случаях подвергаются объекты, которые в Беларуси отнесены к критически важным объектам (далее – КВОИ) – IT-инфраструктуры топливно-энергетических, производственных, транспортных, информационно-коммуникационных, коммунальных, финансовых и других систем жизнеобеспечения государства и населения. В частности, 7 мая 2021 г. один из крупнейших трубопроводных операторов в США – Colonial Pipeline Company – подвергся хакерской атаке и был вынужден приостановить работу трубопровода. В 19 штатах был объявлен режим чрезвычайной ситуации. Стоимость нефти отреагировала коротким взлетом, вернувшись вечером 10 мая 2021 г. к уровню до остановки. Эксперты называют происходящее крупнейшей в истории кибератакой на энергетическую инфраструктуру, которая может повлиять и на мировой рынок нефти, и на политику всей отрасли в области безопасности [3]. В начале июня 2021 г. была произведена кибератака на крупнейшего в мире производителя мяса JBS SA, которая вызвала остановку всех заводов по производству говядины в США, обеспечивающих почти четверть американских поставок. Все мясокомбинаты компании и региональные предприятия по производству говядины были вынуждены закрыться, а работа остальных мясоперерабатывающих предприятий JBS проходила со сбоями [1].

В России в 2021 г. было зафиксировано свыше *300 кибератак*, совершенных профессионалами, что на треть превышает показатели 2020 г. При этом абсолютное большинство (*92 %*) проведенных попыток профессиональных кибератак было направлено на объекты критической информационной инфраструктуры (далее – КИИ) – государственные организации, предприятия энергетики, промышленности и военно-промышленного комплекса [4], [5]. В результате киберпреступлений российские компании понесли колоссальные убытки, по некоторым оценкам они достигают *6 трлн рублей*. Основной ущерб связан с последствиями инцидентов – хищением денежных средств со счетов, выходом из строя оборудования, а также с перерывами в хозяйственной деятельности организации [1], [6]. Так, в августе и сентябре 2021 г. Альфа-банк, ВТБ, Сбербанк подверглись мощным DDoS-атакам, которые в ряде случаев повлияли на проведение платежей клиентов в удаленных каналах обслуживания и привели к сбоям на стороне внешнего поставщика услуг, что могло повлечь непродолжительные задержки в работе отдельных сервисов [7].

В Беларуси в 2021 г. установлено около *1 100* кибератак, которые были осуществлены в том числе и на КВОИ [8]. В частности, 25 апреля 2021 г. Министерство энергетики Республики Беларусь сообщило о взломе сайта Белорусской атомной электростанции. В результате кибератаки хакеры разместили на интернет-ресурсе предприятия фейковую информацию. В конце июля 2021 г. стало известно о взломе в Беларуси автоматизированной информационной системы «Паспорт», которая является инструментом автоматизации служебной деятельности подразделений паспортно-визовой службы уровня ГУВД Мингорисполкома, УВД облисполкомов, а также подчиненных им подразделений паспортно-визовой службы территориальных органов внутренних дел [1]. 24 января 2022 г. возникли проблемы с доступом к справочным web-ресурсам Белорусской железной дороги и сервисам оформления электронных проездных документов. На предприятии это связали с техническими причинами и заявили, что занимаются восстановлением работоспособности системы. На этом фоне одна из группировок, признанная в Беларуси террористической, заявила о проведении атаки на предприятие, целью которой было «замедлить и нарушить работу дороги», утверждалось, что для этого ее представители зашифровали основную часть серверов, баз данных и рабочих станций [9].

Несмотря на актуальность проблемы обеспечения безопасности КВОИ в специальной литературе ей уделяется недостаточно внимания. Рассматриваются лишь отдельные вопросы применительно к техническим мерам обеспечения безопасности таких объектов [10, с. 2-18], [11, с. 666–677], [12, с. 39-40]. Правовые аспекты исследуются фрагментарно [13, с. 57–61]. В связи с этим представляется обоснованным рассмотреть актуальные

современные проблемы правового регулирования обеспечения безопасности КВОИ и определить пути их преодоления.

Основная часть

В настоящее время актами национального законодательства ***КВОИ*** - определяется как объект информатизации, который на основании критериев отнесения объектов информатизации к КВОИ и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр КВОИ (*абз. 7 п. 33 Положения о технической и криптографической защите информации», утв. Указом Президента Республики Беларусь от 16.04.2013 № 196 (в ред. Указа Президента Республики Беларусь от 09.12.2019 № 449) [14]*). При этом ***объект информатизации*** рассматривается как средства электронной вычислительной техники вместе с программным обеспечением, в том числе системы управления различного уровня и назначения, информационные системы и сети, автономные стационарные и персональные электронные вычислительные машины, используемые в соответствии с заданной информационной технологией, системы управления информационными, производственными и (или) технологическими процессами (*абз. 10 п. 33 указанного Положения*).

Специалисты отмечают, что объектам критической инфраструктуры и органам власти важно в принципе не допустить реализации кибератак. Это требует принципиально нового подхода к выстраиванию информационной безопасности. В ее рамках нужно сформировать единую дорожную карту по цифровой трансформации и проектам информационной безопасности. Они должны включать повышение порога входа в базовую инфраструктуру, процессы обеспечения безопасности, особенно в уязвимых точках (удаленный доступ, управление доступом и двухфакторная аутентификация, контроль ИТ-подрядчиков). Затем требуется сформировать план экстренного восстановления систем при сбое или атаке и отработать все взаимодействия внутри этого плана, чтобы они были слаженными. Работу должна контролировать независимая группа профессионалов, которые организуют киберучения. Отдельного внимания требует повышение киберграмотности сотрудников – это позволит вовремя распознать методы социальной инженерии, используемой хакерами. Наконец, необходимо создать центр управления безопасностью, который будет не только выявлять и реагировать на возникающие инциденты, но и оценивать защищенность болевых точек компании, новых систем защиты, контролировать цифровизацию [15].

Однако это, в первую очередь, – меры технического, аппаратно-программного характера. Вместе с тем требует совершенствования и правовое регулирование обеспечения безопасности КВОИ.

Учитывая это, в современный период в Беларуси можно выделить ряд проблем в рассматриваемой сфере правового регулирования.

1. Пробелы в формировании системы правовых норм, регулирующих обеспечение безопасности КВОИ.

В настоящее время рассматриваемая сфера правового регулирования распространяется на:

деятельность владельцев КВОИ по обеспечению информационной безопасности соответствующих объектов;

деятельность уполномоченных государственных органов, осуществляющих контроль в этой сфере;

противоправную деятельность лиц, создающих угрозы информационной безопасности КВОИ.

Деятельность первых двух групп в современный период регламентируется следующими актами законодательства:

Положение о технической и криптографической защите информации», утв. Указом Президента Республики Беларусь от 16.04.2013 № 196 (в ред. Указа Президента Республики Беларусь от 09.12.2019 № 449);

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 65 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь» [16];

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 44» [17], которым, в частности, утверждаются: Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено; Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено; Положение о порядке технической и криптографической защиты информации, обрабатываемой на КВОИ, и ряд других комплексов нормативных требований в области информационной безопасности КВОИ.

Вместе с тем видится, что объем регулирования деятельности владельцев КВОИ является недостаточным.

Так, например, руководство профильного управления Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК) считает, что одним из главных условий сложившейся ситуации в сфере обеспечения безопасности объектов КИИ является невыполнение владельцами таких объектов требований законодательства о безопасности КИИ (в первую очередь – требований Федерального закона «О безопасности критической информационной инфраструктуры Российской

Федерации» [18]). В качестве характерных неправомерных действий таких субъектов выделяются [19]:

многие пытаются уклониться от реализации федерального закона: с одной стороны – не относят себя к субъектам КИИ, несмотря на то, что все прямые и косвенные признаки на это указывают; с другой – отрицают, что у них есть объекты КИИ, которые необходимо категорировать;

ряд владельцев объектов КИИ нарушают сроки предоставления перечней объектов КИИ;

отдельные организации уведомляют регулятора не обо всех имеющихся у них объектах КИИ;

нарушаются сроки категорирования объектов КИИ;

искусственно занижаются категории значимости имеющихся объектов КИИ;

предоставляются недостоверные сведения об объектах КИИ и учитывают не все показатели;

субъекты КИИ недооценивают потенциал нарушителя и имеют проблемы с силами безопасности – у отдельных организаций безопасность значимых объектов обеспечивают подразделения по экономической безопасности, у некоторых – вообще юридические службы;

на многих объектах, особенно это касается автоматизированных систем управления технологическими процессами, применяются только средства антивирусной защиты и штатные средства операционных систем, что недостаточно для противостояния серьезным угрозам.

Для решения указанных проблем ФСТЭК во взаимодействии с заинтересованными государственными органами в начале 2021 г. был разработан и внесен в Государственную Думу РФ проект закона, предусматривающий изменения и дополнения в Кодекс Российской Федерации об административных правонарушениях в части введения административной ответственности за нарушение норм законодательства о безопасности КИИ, который был принят 26 мая 2021 г. [20]. В указанный Кодекс введены:

ст. 13.12.1, устанавливающая ответственность за Нарушение требований в области обеспечения безопасности КИИ Российской Федерации;

ст. 19.7.15, закрепляющая ответственность за непредставление сведений, предусмотренных законодательством в области обеспечения безопасности КИИ Российской Федерации.

При этом ст. 13.12.1 предусматривает ответственность за следующие нарушения:

часть 1 – нарушение требований к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ Российской Федерации, установленных федеральными законами и

принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния, – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 50 000 до 100 000 рублей (примерно от 2 000 до 4 000 белорусских рублей);

часть 2 – нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ Российской Федерации, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 100 000 до 500 000 рублей (примерно от 4 000 до 20 000 белорусских рублей);

часть 3 – нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ Российской Федерации, между субъектами КИИ Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, – влечет наложение административного штрафа на должностных лиц в размере от 20 000 до 50 000 рублей (примерно от 800 до 2 000 белорусских рублей); на юридических лиц – от 100 000 до 500 000 рублей (примерно от 4 000 до 20 000 белорусских рублей).

Положения ст. 19.7.15 предусматривает ответственность за следующие нарушения:

часть 1 – непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ Российской Федерации, сведений о результатах присвоения объекту КИИ Российской Федерации одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности КИИ Российской Федерации, либо об отсутствии необходимости присвоения ему одной из таких категорий – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 50 000 до 100 000 рублей (примерно от 2 000 до 4 000 белорусских рублей);

часть 2 – непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, предусмотренной законодательством в

области обеспечения безопасности КИИ Российской Федерации, за исключением случаев, предусмотренных ч. 2 ст. 13.12.1 рассматриваемого Кодекса, – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 100 000 до 500 000 рублей (примерно от 4 000 до 20 000 белорусских рублей).

Представляется, что рассмотренная ситуация является характерной и для Республики Беларусь. В связи с этим видится целесообразным внести соответствующие изменения и в Кодекс Республики Беларусь об административных правонарушениях.

Основным способом борьбы с противоправной деятельностью лиц, создающих угрозы информационной безопасности КВОИ, можно обоснованно рассматривать использование норм административного и уголовного права. Так, незаконные действия указанных лиц образуют следующие административные правонарушения и преступления:

несанкционированный доступ к компьютерной информации (*ст. 23.4 Кодекса Республики Беларусь об административных правонарушениях [21], ст. 349 Уголовного кодекса Республики Беларусь [22] (далее – УК)*);

уничтожение, блокирование или модификация компьютерной информации (*ст. 350 УК*);

разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (*ст. 354 УК*).

При этом в Беларуси в 2021 г. из всего числа совершенных киберпреступлений (*16 446*) по фактам совершения преступлений, предусмотренных ст. 349 УК, было возбуждено *6,7 %* (*1 104*) уголовных дел. По остальным статьям, предусматривающим ответственность за данные преступные деяния уголовные дела не возбуждались [8].

В Российской Федерации в 2021 г. было возбуждено *70 уголовных дел* из-за кибератак и другого неправомерного воздействия на КИИ [23]. Это составило *0,013 %* от всего числа возбужденных уголовных дел, связанных с киберпреступлениями (*518 000*) [24]. При этом отмечается, что половина уголовных дел, о которых идет речь, касается использования программ, заведомо предназначенных для неправомерного использования на КИИ. Например, по одному из дел работники локомотивных бригад Российской железной дороги воспользовались нештатным программным обеспечением, чтобы пройти тест на знание технически-распорядительных актов железнодорожных станций. По другому делу сотрудник Пермского порохового завода скачал нелицензионную версию Microsoft Word, генератор ключа для которой, по версии обвинения, установил канал обмена информацией с «принадлежащим США» IP-адресом [23].

Необходимо отметить, что в июне 2017 г. в Уголовный кодекс Российской Федерации была введена ст. 274.1, которая устанавливает повышенную уголовную ответственность за неправомерное воздействие на КИИ Российской Федерации [25]. В частности, ответственность предусмотрена за следующие противоправные действия:

часть 1 – создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, – наказываются принудительными работами на срок до 5 лет с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 5 лет со штрафом в размере от 500 000 до 1 млн рублей (примерно от 20 000 до 40 000 белорусских рублей) или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет;

часть 2 – неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ Российской Федерации, – наказывается принудительными работами на срок до 5 лет со штрафом в размере от 500 000 до 1 млн рублей (примерно от 20 000 до 40 000 белорусских рублей) или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет и с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 6 лет со штрафом в размере от 500 000 до 1 млн рублей (примерно от 20 000 до 40 000 белорусских рублей) или в размере заработной платы или иного дохода осужденного за период от одного 1 до 3 лет;

часть 3 – нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда КИИ Российской Федерации, – наказывается принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового

либо лишением свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового;

часть 4 – деяния, предусмотренные ч.ч. 1, 2 или 3 данной статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, – наказываются лишением свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового;

часть 5 – деяния, предусмотренные частью 1, 2, 3 или 4 настоящей статьи, если они повлекли тяжкие последствия, – наказываются лишением свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

Представляется, что в настоящее время подобные преступные деяния характерны и для Республики Беларусь. В связи с этим видится обоснованным внести соответствующие изменения и в УК.

2. Пробелы в правовом регулировании использования оборудования и программного обеспечения на КВОИ.

Во многих случаях для обеспечения деятельности КВОИ используется иностранное оборудование и программное обеспечение.

В Российской Федерации отмечают, что есть порядка 10-15 импортных программных продуктов, которые широко используют ведущие российские промышленные предприятия, и ограничение или прекращение доступа к которым несет в себе критические риски. Один из популярных продуктов – платформа передачи данных PI System от Aveva (изначально разрабатывалась OSI Soft). Если вендор решит отозвать лицензии, то крупнейшие нефтеперерабатывающие предприятия России останутся без системы диспетчеризации. Более того, 90 % непрерывных производств в России используют PI System в качестве базы данных реального времени, которая собирает промышленную информацию, на основе которой осуществляется оперативное управление производством. Еще один пример – продукты для сбора данных и диспетчерского контроля уровня SCADA. Так, «Транснефть» и Мосводоканал применяют HMI/SCADA iFIX компании GE. В первом случае – для управления заглушками, насосами нефти, во втором случае – воды. Эти системы являются критически важными. Их отключение в «Транснефти» может привести к полной остановке транспортировки нефти и нефтепродуктов по трубопроводам компании и к необходимости перейти на ручное локальное управление. А если аналогичное произойдёт в Мосводоканале, то риск связан с перебоями водоснабжения многих районов мегаполиса. При этом можно перейти на полуавтоматическое локальное управление процессами,

насосами и задвижками и восстановить водоснабжение, но для этого потребовалось бы удвоить штат операторов. На большинстве российских нефтеперерабатывающих заводов для установок первичной и глубокой переработки нефти используется программное обеспечение класса DCS (распределенных систем управления (РСУ)) компаний Honeywell, Emerson, ABB, Yokogawa. Отключение РСУ приведет к остановке заводов [26].

В целях обеспечения технологической независимости и безопасности КИИ Президент России В. В. Путин 30 марта 2022 г. подписал Указ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [27]. Данный документ предусматривает с 31.03.2022 запрет на закупку иностранного программного обеспечения для обеспечения деятельности значимых объектов КИИ и услуг, необходимых для использования этого программного обеспечения, а с 01.01.2025 – запрет на использование иностранного программного обеспечения на таких объектах. При этом Правительству РФ предписано в 6-месячный срок реализовать комплекс мероприятий, направленных на обеспечение преимущественного применения субъектами КИИ российских радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им значимых объектах КИИ.

Актуальность данного шага подтверждена последующими событиями – в начале июня 2022 г. Китайская Республика (Тайвань) в связи с военными действиями на территории Украины ограничила поставки в Россию любых чипов с тактовой частотой свыше 25 МГц, а также микросхем с количеством контактов до 144 единиц, а также литографического оборудования, которое может быть использовано для изготовления подобных микросхем (на долю Тайваня приходится более 90 % такой продукции). Как отмечается, указанные микросхемы используются повсеместно: от компьютеров до автомобилей. Поэтому найти равноценную замену чипам и микросхемам будет крайне сложно. Кроме того, процессоры российского происхождения Baikal и «Эльбрус» также до недавнего времени собирались на Тайване. Беларусь при этом указана как страна, которая способна помочь РФ действовать в обход санкций [28].

Представляется, что данные проблемы характерны и для Республики Беларусь. В связи с этим представляется необходимым уже сейчас начать разрабатывать комплекс организационно-правовых мер, в первую очередь в области правового регулирования разработки и использования оборудования и программного обеспечения для КВОИ. Такие меры могут включать как разработку и совершенствование национальных актов законодательства, регламентирующих отношения в данной области, (например, по импортозамещению) так и заключение международных договоров с

дружественными странами о кооперации в сфере разработки и использования соответствующих технических и программных продуктов для КВОИ.

Заключение

Изложенное позволяет сделать следующие выводы.

1. В современный период обеспечение безопасности КВОИ является одним из важнейших направлений обеспечения национальной безопасности каждого государства, в том числе и Республики Беларусь. Актуальными угрозами безопасности КВОИ являются недостаточность мер, принимаемых собственниками (владельцами) данных объектов по созданию необходимых условий для их нормальной деятельности, а также совершение различного характера преступлений в отношении таких объектов (кибератак). Одним из ключевых факторов, способствующими реализации таких угроз, является использование на КВОИ иностранного оборудования и программного обеспечения.

2. Характер имеющих место угроз безопасности КВОИ обуславливает необходимость адекватного реагирования на них уполномоченных субъектов. Для достижения стабильного и бесперебойного функционирования КВОИ уполномоченными государственными органами и собственниками (владельцами) данных объектов предпринимаются различные меры, в том числе правового характера. В настоящее время первоочередными из них являются меры, направленные на устранение пробелов в правовом регулировании деятельности собственников (владельцев) КВОИ и противодействие угрозам таким объектам.

3. Совершенствование правового регулирования обеспечения безопасности КВОИ в современных условиях целесообразно осуществлять по следующим направлениям:

принятие национальных актов законодательства, устанавливающих требования в области разработки и использования оборудования и программного обеспечения для КВОИ, а также заключение международных договоров с дружественными странами о кооперации в данной сфере;

установление мер административной ответственности для владельцев (собственников) КВОИ за невыполнение владельцами таких объектов требований законодательства об их безопасности;

установление уголовной ответственности за деяния, направленные на неправомерное воздействие на КВОИ.

Библиографический список

1. Кибератаки [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2022/02/04. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D

0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8. – Дата доступа: 07.04.2022.

2. Check Point Research : Cyber Attacks Increased 50 % Year over Year [Electronic resource] // Check Point. – Режим доступа: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/. – Access date: 07.04.2022.

3. Бесполезные ископаемые [Электронный ресурс] / А. Наумов, Е. Черненко, О. Мордюшенко // Комменрсантъ: 10.05.021. – Режим доступа: https://www.kommersant.ru/doc/4802807. – Дата доступа: 07.04.2022.

4. Более 90% кибератак в 2021 г. пришлось на объекты критической инфраструктуры РФ [Электронный ресурс] // INTERFAX.RU: 7 декабря 2021. – Режим доступа: https://www.interfax.ru/russia/806997. – Дата доступа: 07.04.2022.

5. Хакеры с квалификацией выбирают КИИ / К. Скурат // ComNews: 08.12.2021. – Режим доступа: https://www.comnews.ru/content/217824/2021-12-08/2021-w49/khakery-kvalifikaciey-vybirayut-kii. – Дата доступа: 07.04.2022.

6. Почему киберпреступления – угроза национальной безопасности Электронный ресурс] // ВЕДОМОСТИ: 7 декабря 2021. – Режим доступа: https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti. – Дата доступа: 07.04.2022.

7. Замедление взлому подобно [Электронный ресурс] / М. Буйлов, Ю. Степанова, А. Гаврилюк // Коммерсантъ: 04.09.2021. – Режим доступа: https://www.kommersant.ru/doc/4974831. – Дата доступа: 07.04.2022.

8. Начальник ГУПК МВД Андрей Ковалев: «В текущем году прогнозируется рост интернет-мошенничеств, в том числе связанных с криптовалютой» [Электронный ресурс] // Официальный сайт МВД Республики Беларусь: 23.02.2022. – Режим доступа: https://www.mvd.gov.by/ru/news/9084. – Дата доступа: 07.04.2022.

9. БЖД восстановила онлайн-продажу билетов на электрички и дизель-поезда [Электронный ресурс] // Sputnik Беларусь: 03.02.2022. – Режим доступа: https://sputnik.by/20220203/bzhd-vosstanovila-onlayn-prodazhu-biletov-na-elektrichki-i-dizel-poezda-1060029514.html#pv=g%3D1060029514%2Fp%3D1043362160. – Дата доступа: 07.04.2022.

10. Маликов, В. В. Повышение эффективности информационных и инженерно-технических систем защиты критически важных объектов : автореф. дис. ... канд. техн. наук : 05.13.19 / В. В. Маликов ; Бел. гос. ун-т информатики и радиоэлектроники. – Минск, 2010. – 23 с.

11. Мелех, О. В. Классификация критически важных объектов информатизации по требованиям физической защиты с использованием методов кластерного анализа / О. В. Мелех, Е. П. Максимович, В. К. Фисенко // Искусственный интеллект. – 2010. – № 4. – С. 666–677.

12. Барановский, О. К. Актуальные вопросы технической защиты информации в системах физической защиты объектов критической инфраструктуры / О. К. Барановский // Технологии безопасности. – 2012. – № 3. – С. 39–40.

13. Рябоволов, В. Правовые аспекты государственного регулирования системы обеспечения безопасности критически важных объектов информатизации / В. Рябоволов, А. Чернолевский // Юстиция Беларуси. – 2016. – № 7. – С. 57–61.

14. Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации [Электронный ресурс] : Указ Президента Республики Беларусь, 16 апр. 2013 г. № 196 : в ред. Указа Президента Респ. Беларусь от 09.12.2019 //

ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

15. Киберхулиганы и кибернаемники: как бороться с новыми угрозами инфобеза [Электронный ресурс] / Мария Решетникова // РБК: 21.12.2021. – Режим доступа: https://trends.rbc.ru/trends/industry/61c1951e9a79475fdac24d4c. – Дата доступа: 07.04.2022.

16. О показателях уровня вероятного ущерба национальным интересам Республики Беларусь [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 фев. 2020 г., № 65 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

17. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 44 [Электронный ресурс]: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 фев. 2020 г., № 66 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

18. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федер. закон, 26 июля 2017 г., № 187-ФЗ // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

19. Безопасность критической информационной инфраструктуры РФ [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2021/12/08. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D1%8B_%D0%A0%D0%A4. – Дата доступа: 07.04.2022.

20. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] : Федер. закон, 26 мая 2021 г., № 141-ФЗ // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

21. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс]: 6 янв. 2021 г., № 92-З: принят Палатой представителей 18 дек. 2020 г.: одобр. Советом Респ. 18 дек. 2020 г.: в ред. Закона Респ. Беларусь от 04.01.2022 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

22. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г.: в ред. Закона Респ. Беларусь от 05.01.2022 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

23. Уголовные дела на рынке информационных технологий России [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2022/02/04. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D1%8B%D0%B5_%D0%B4%D0%B5%D0%BB%D0%B0_%D0%BD%D0%B0_%D1%80%D1%8B%D0%BD%D0%BA%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8. – Дата доступа: 07.04.2022.

24. Число киберпреступлений в России [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2022/02/18. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#:~:text=%D0%9F%D0%BE%20%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B5%20%D0%9C%D0%92%D0%94%2C%20%D0%B7%D0%B0%20%D1%81%D0%B5%D0%BC%D1%8C,104%20%D1%82%D1%8B%D1%81%D1%8F%D1%87%D0%B8%20%E2%80%94%20%D1%81%20%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5%D0%BC%20%D0%BA%D0%B0%D1%80%D1%82. – Дата доступа: 07.04.2022.

25. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] : Федер. закон, 26 июля 2017 г., № 194-ФЗ // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

26. Критическая инфраструктура России [Электронный ресурс] // Tadviser: Государство.Бизнес.Технологии: 2022/03/30. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8. – Дата доступа: 07.04.2022.

27. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : Указ Президента Рос. Федерации, 30 марта 2022 г., № 166 // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

28. Тайвань ввел запрет на поставку электронных чипов в Россию / А. Абрамов // SPBITRU: 03.06.2022. – Режим доступа: https://spbit.ru/news/n211027/. – Дата доступа: 05.06.2022.