УДК 342

ПРАВОВОЙ РЕЖИМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Я. Д. БОНДАРЧУК
(Представлено: канд. юрид. наук, доц. И. В. Шахновская)

В статье рассматривается правовой режим критической информационной инфраструктуры в Республике Беларусь, построенный вокруг категории «критически важный объект информатизации». Раскрыты критерии и порядок отнесения объектов, обязанности владельцев, устройство национальной системы кибербезопасности и ответственность по нормам.

Работа энергетики, транспорта, связи, банков и систем жизнеобеспечения населения зависит от информационных систем, поэтому их отказ причиняет ущерб далеко за пределами одной организации. Концепция национальной безопасности Республики Беларусь относит нарушение киберустойчивости национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем к основным угрозам национальной безопасности [1]. Термин «критическая информационная инфраструктура» (далее – КИИ) в белорусском законодательстве не закреплён: правовой режим КИИ строится вокруг категории «критически важный объект информатизации» (далее – КВОИ).

Регулирование является многоуровневым и преимущественно подзаконным. Общие основы защиты информации закреплены в Законе «Об информации, информатизации и защите информации» [2]. Специальный режим КВОИ определяют акты Президента Республики Беларусь: Указом были утверждены Положение о технической и криптографической защите информации (далее – Положение о защите информации) и Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации (далее – Положение об отнесении) [3]; Указом «О кибербезопасности» создана национальная система обеспечения кибербезопасности [4]. Их реализуют постановление Совета Министров «О центрах кибербезопасности»[5], и приказы Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ): определивший показатели уровня вероятного ущерба [6]. Ответственность предусмотрена Кодексом Республики Беларусь об административных правонарушениях (далее – КоАП).

Согласно Положению о защите информации, КВОИ – это объект информатизации, включённый в Государственный реестр критически важных объектов информатизации (далее – реестр) на основании критериев отнесения и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах [3]. Следовательно, статус определяется не только соответствием критериям, но и формальным включением в реестр, который ведёт ОАЦ: объект считается критически важным со дня его включения в реестр. Требования этих положений не распространяются на объекты, предназначенные для обработки государственных секретов [3]. Указ вводит более широкую категорию – объекты информационной инфраструктуры, в которую КВОИ входят наряду с информационными сетями, системами и ресурсами государственных органов и иных организаций [4].

Критериями отнесения являются социальная, экономическая, экологическая и информационная значимость. Социальная значимость относится к объектам, обеспечивающим жизнедеятельность населения (жилищно-коммунальное хозяйство, здравоохранение, образование, труд, занятость и социальная защита); экономическая – к объектам основных отраслей экономики, безналичных (межбанковских) расчётов и процессинга; экологическая – к объектам, нарушение работы которых может причинить ущерб окружающей среде; информационная – к объектам связи и средств массовой информации [3]. Количественные показатели вероятного ущерба утверждены приказом ОАЦ, например: нарушение водо-, газо-, тепло- или энергоснабжения, водоотведения более чем для 50 тысяч человек; экономический ущерб свыше 100 000 базовых величин; невозможность межбанковских расчётов в белорусских рублях более двух часов; нарушение доступа к точке обмена национальным трафиком более одного часа [6].

Владелец объекта составляет заключение о его соответствии критериям и показателям и в течение трёх рабочих дней направляет его в государственный орган либо в облисполком или Минский горисполком; второй экземпляр направляется в ОАЦ. Государственный орган в течение десяти рабочих дней принимает решение в виде приказа (распоряжения), копию которого в течение пяти рабочих дней направляет в ОАЦ, а ОАЦ в течение пяти рабочих дней включает объект в реестр [3]. Независимо от инициативы владельца ОАЦ вправе вынести письменное требование об отнесении объекта к критически важным, и владелец в течение месяца обязан совершить необходимые действия. Исключение из числа КВОИ возможно

по согласованию с ОАЦ, если объект перестал соответствовать критериям либо его эксплуатация прекращена [3]. Помимо реестрового порядка, приложение к Указу содержит перечень владельцев КВОИ из 27 организаций, которые обязаны создать центры кибербезопасности [4].

В течение шести месяцев со дня принятия решения об отнесении владелец проектирует и создаёт систему информационной безопасности (совокупность правовых, организационных и технических мер защиты) и в течение пяти рабочих дней после её создания информирует об этом ОАЦ [3]. Проектирование, создание и аудит системы, мониторинг угроз информационной безопасности и реагирование на риски образуют комплекс мероприятий, предусмотренный Положением о защите информации. Для проведения работ создаётся подразделение защиты информации либо назначается уполномоченное должностное лицо, имеющее профильное образование или прошедшее переподготовку. Применяются средства защиты информации, имеющие сертификат соответствия Национальной системы подтверждения соответствия либо положительное экспертное заключение государственной экспертизы ОАЦ. Аудит системы проводится владельцем не позднее чем через год после завершения мероприятий по её созданию и далее ежегодно, результаты оформляются актом. [3]. Персональную ответственность за организацию технической и криптографической защиты информации несёт руководитель организации [3]; Указ дополнительно возлагает на него персональную ответственность за обеспечение кибербезопасности [4].

Внешний контроль осуществляет ОАЦ в форме проверок по плану, который размещается на его официальном сайте не позднее 30 декабря предшествующего года, а при наличии сведений о нарушениях – внеплановых. При выявлении нарушений ОАЦ выносит письменное требование (предписание) об их устранении, а при необходимости – о приостановлении функционирования КВОИ; срок устранения не может превышать шести месяцев, а решения ОАЦ могут быть обжалованы в суд [3].

Её элементами являются ОАЦ, Национальный центр кибербезопасности в структуре ОАЦ, центры кибербезопасности, авторизованный оператор электросвязи, объекты информационной инфраструктуры и сети передачи данных [4]. Центры кибербезопасности проходят аттестацию в ОАЦ до начала работы и далее не реже одного раза в три года, автоматизированно собирают данные о кибербезопасности, выявляют и исследуют кибератаки, реагируют на киберинциденты и информируют Национальный центр кибербезопасности не позднее одного часа с момента их выявления [4]. Перечень государственных органов и организаций, которые создают такие центры или приобретают услуги у организаций, их создавших, определён приложением 2 к постановлению № 246 с указанием сроков по каждой организации; приложение 1 называет 23 организации, у которых государственные органы вправе приобретать эти услуги по процедуре закупки из одного источника [5]. Руководители организаций из перечня и владельцев КВОИ из приложения 1 к Указу назначают одного из заместителей ответственным за организацию работы по обеспечению кибербезопасности [4].

С 2026 года вводятся три уровня киберинцидентов – высокий, средний и низкий (ранее было два). К высокому относятся вызванные кибератакой нарушение на срок более трёх часов или прекращение функционирования КВОИ, а также объектов, подлежащих отнесению к КВОИ; нарушение конфиденциальности служебной информации ограниченного распространения и ряда категорий персональных данных; нарушение целостности или доступности информации, повлёкшее распространение недостоверной общественно значимой информации [7]. О киберинцидентах высокого и среднего уровня центры информируют Национальный центр кибербезопасности не позднее одного часа с момента выявления. До принятия мер по сохранности сведений об индикаторах компрометации не допускается изменять конфигурации средств, удалять вредоносное программное обеспечение, обновлять программное обеспечение и восстанавливать информацию из резервных копий [7].

Во-первых, режим КИИ раздроблен: единого законодательного акта о кибербезопасности и КИИ нет, а ключевые нормы содержатся в указах и приказах ОАЦ, которые часто меняются; терминология (КВОИ, объекты информационной инфраструктуры, объекты, подлежащие отнесению к КВОИ) нуждается в унификации. Во-вторых, круг субъектов определяется двумя механизмами – поимённым перечнем в приложении к Указу и критериально-реестровым порядком Положения об отнесении; их соотношение целесообразно уточнить. В-третьих, приказ относит к киберинцидентам высокого уровня события на объектах, подлежащих отнесению к КВОИ, это перекладывает на владельца риск самостоятельной оценки объекта и требует чётких методических разъяснений по критериям. Единообразие практики зависит от доступности и определённости этих критериев, а практика применения норм, действующих с лета 2026 года, только формируется. В-четвертых, требования к владельцам ресурсоёмки, что делает актуальной дифференциацию мер по уровню значимости объекта.

Правовой режим КИИ в Республике Беларусь построен вокруг КВОИ и характеризуется формальным статусом, обязанностью владельца создать систему информационной безопасности и ежегодно проводить её аудит, встроенностью в национальную систему кибербезопасности с обязательным обменом информацией о киберинцидентах и специальной административной ответственностью. Дальнейшее совершенствование

целесообразно связать с консолидацией норм в едином законодательном акте, унификацией терминологии, уточнением критериев оценки киберинцидентов и дифференциацией требований к владельцам.

ЛИТЕРАТУРА

1. Концепция национальной безопасности Республики Беларусь: утв. решением Всебелорус. нар. собр., 25 апр. 2024 г., № 5 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь.
2. Об информации, информатизации и защите информации: Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З: с изм. и доп. // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь.
3. О некоторых мерах по совершенствованию защиты информации: Указ Президента Респ. Беларусь, 16 апр. 2013 г., № 196: в ред. Указа Президента Респ. Беларусь от 6 июня 2025 г. № 227 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь.
4. О кибербезопасности: Указ Президента Респ. Беларусь, 14 февр. 2023 г., № 40 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь.
5. О центрах кибербезопасности: постановление Совета Министров Респ. Беларусь, 14 мая 2026 г., № 246 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь.
6. О показателях уровня вероятного ущерба национальным интересам Республики Беларусь: приказ Оператив.-аналит. центра при Президенте Респ. Беларусь, 20 февр. 2020 г., № 65 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь.
7. О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40: приказ Оператив.-аналит. центра при Президенте Респ. Беларусь, 25 июля 2023 г., № 130: в ред. приказа от 27 мая 2026 г. № 98 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь.