УДК 658:005.5

КИБЕРАТАКИ НА КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ КАК ИСТОЧНИК УГРОЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Воробьёв Станислав Юрьевич, заведующий сектором
информационной езопасности
Ханчевский Евгений Анатольевич, начальник отдела
информационных технологий
РУП «Белэнергосетьпроект»
Varabyou Stanislau Yuryevich, head of the information security sector,
s.varabyou@besp.by
Khanchevsky Evgeny Anatolyevich, head of the information technology department,
zh@besp.by
Republican unitary enterprise «Belenergosetproekt»

Аннотация. В статье рассматривается возникновение нового вида угроз в информационной сфере – кибератак, а также повышенная опасность последних, как одного из элементов гибридной войны, целью которых являются критически важные объекты, в том числе в сфере экономики

Ключевые слова: кибератака, критически важные объекты, критически важные объекты информатизации, кибербезопасность

В настоящее время в мире с высокой степенью интенсивности и динамичности происходят значительные политические, военные, экономические, социальные изменения. Следствием технологического прогресса стало возникновение нового вида угроз, в том числе в информационной сфере. Информационные технологии

широко применяются для управления важнейшими объектами жизнеобеспечения, которые представляют собой мишень для случайных и преднамеренных воздействий. Расширился круг государств, создавших или создающих в составе национальных вооруженных сил подразделения информационной безопасности, включая кибервойска, задачей которых является проведение кибероперации. Так, например, в США циркулирует концепция так называемой дешевой войны (War on the Cheap), сторонники которой утверждают, что один миллион долларов и 20 человек, проводя компьютерные атаки, могут обеспечить успех, сопоставимый с действиями многотысячной группировки войск [1], а в 2016 году НАТО на Варшавском саммите официально объявила киберпространство новой сферой проведения операций – наряду с воздушной, сухопутной и морской [2]. Также необходимо отметить возросшее количество киберпреступлений, совершаемых как отдельными лицами, так и преступными группами: информационные системы и ресурсы не только стали предметом преступлений, но и средством совершения последних.

Республика Беларусь на современном этапе представляет собой состоявшееся правовое и суверенное государство, которое проводит миролюбивую внешнюю и социальноориентированную внутреннюю политики и вместе с тем в силу своего географического положения и открытости в полной мере подвержена большинству геополитических процессов, происходящих в мире. Перед государством стоит масштабная задача по развитию, поддержанию и совершенствованию системы обеспечения кибербезопасности.

Глава Государства неоднократно обращал внимание на особую опасность, такого элемента гибридной войны, используемого против Республики Беларусь, как кибератаки, их направленность на экономические объекты, предприятия, банковскую систему, основные пункты жизнеобеспечения, отмечал, что целью кибератак является нанесение максимального ущерба экономике и дестабилизация общества [3-4].

В соответствии Концепцией информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18.03.2019 №1 (далее - Концепция информационной безопасности), под кибератакой понимают 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 угроз безопасности обрабатываемой такими объектами информации. Так, успешная кибератака может нанести не меньший урон, чем применение ядерного оружия: отключение важных инфраструктурных объектов мгновенно введет в хаос крупные мегаполисы и целые регионы [5]. Так, в финансовом секторе экономики, включая банковскую сферу и небанковские кредитно-финансовые организации, фактически сформировалась тотальная зависимость последнего от надежности электронных систем хранения, обработки и обмена данными.

Согласно закону Республики Беларусь от 03.01.2002 № 77-З «О борьбе с терроризмом» под критически важным объектом понимают объекты социальной, производственной, инженерно-транспортной, энергетической, информационно-коммуникационной и иной инфраструктуры, нарушение функционирования которых в результате акта терроризма может способствовать дестабилизации общественного порядка и достижению иных целей терроризма и (или) повлечь за со-

бой человеческие жертвы, причинение вреда здоровью людей или окружающей среде, значительный материальный ущерб и нарушение условий жизнедеятельности людей. Защита подобных объектов и их совокупности, которую называют критически важной инфраструктурой (критической инфраструктурой) является одной из наиболее важных задач обеспечения национальной безопасности любой страны.

Концепцией национальной безопасности Республики Беларусь, принятой решением Всебелорусского народного собрания 25.04.2024 № 5 (далее – Концепция национальной безопасности), в перечень основных угроз национальной безопасности включены в том числе нарушение безопасности функционирования критической инфраструктуры и критически важных объектов. Данным документом дается определение понятию экономической безопасности – состояние защищенности отраслей и сфер экономики от воздействия угроз, препятствующих устойчивому социально-экономическому развитию Республики Беларусь.

В целях обеспечения национальных интересов в Республике Беларусь на нормативном уровне осуществляется выделение и регламентирование функционирования критически важных объектов информатизации на основании критериев социальной, экономической, экологической и информационной значимости. В соответствии с Положением о технической и криптографической защите информации, утвержденным Указом Президента Республики Беларусь от 16.04.2013 № 196, критически важный объект информатизации (далее – КВОИ) - объект информатизации, который на основании отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации. Данным положением регулируются особенности технической и криптографической защиты информации, обрабатываемой на КВОИ, в свою очередь порядок отнесения объектов информатизации к КВОИ, регулируются Положением о порядке отнесения объектов информатизации к критически важным объектам информатизации. Показатели уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае создания угроз информационной безопасности либо в результате возникновения рисков информационной безопасности в отношении объекта информатизации, не предназначенного для проведения работ с использованием государственных секретов (его составляющих элементов), утверждены приказом Оперативно-аналитического центра при Президенте Республики Беларусь (далее - ОАЦ) от 20 февраля 2020 № 65. Порядок технической и криптографической защиты информации, обрабатываемой на КВОИ регулируется Положением о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, утвержденным приказом ОАЦ от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».

В целях повышения уровня защиты национальной инфраструктуры от внешних и внутренних угроз Главой государства 14.02.2023 подписан Указ № 40 «О кибербезопасности» (далее - Указ № 40), регулирующий основные принципы создания и функционирования национальной системы обеспечения кибербезопасности. Указ № 40 является правовым фундаментом национальной системы обеспечения

кибербезопасности, комплексным и многоуровневым механизмом противодействия кибератакам на госорганы и организации, критически важную информационную инфраструктуру и направлен на дальнейшую реализацию положений Концепции национальной безопасности и взаимосвязан с Концепцией информационной безопасности. Отдельно необходимо сакцентировать внимание на том, что требованиями Указа № 40 на руководителя госоргана и иной организации напрямую возлагается персонифицированная ответственность за обеспечение кибербезопасности (документом предусмотрено назначение одного из заместителей руководителя ответственным за организацию работы по обеспечению кибербезопасности, в том числе за осуществление мероприятий по обнаружению, предотвращению и минимизации последствий кибератак). Предполагается, что данный нормативный правовой акт явится триггером для увеличения вложения средств организаций в обеспечение собственной информационной безопасности.

В рамках реализации Указ № 40 ОАЦ издан приказ от 25.07.2023 № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. N 40», которым утверждены ряд технических регламентов и требований, а также положений информационно-телекоммуникационного и оперативно-функционального характера, которые должны воплотить идеи, заложенные в Указе № 40.

В современном мире возросла роль информационно-коммуникационных технологий. Кибератаки на информационную структуру критических объектов рассматриваются в мире как одна из наиболее значимых угроз безопасности. США рассматривает киберпространство как поле боя и быстро наращивают свои возможности для доминирования в данной сфере. НАТО официально объявила киберпространство новой сферой проведения операций и регулярно проводит киберучения. Главой государства уделяется повышенное внимание вопросам кибербезопасности. На нормативном уровне в Республике Беларусь осуществляется выделение и регламентирование функционирования КВОИ. Вступил в силу и действует Указ № 40, регулирующий основные принципы создания и функционирования национальной системы обеспечения кибербезопасности в Республике Беларусь. На национальном уровне осуществляется поддержка и поощрение к применению лучших практик применения кибербезопасности, а также достижения киберустойчивости КВОИ, в том числе путем реализации комплекса правовых, организационных и технических мероприятий.

Список использованных источников

1. Бартош, А.А. Гибридная война : учебное пособие / А.А. Бартош. – Москва : КНОРУС, 2023. – 306 с.

2. Белоус, А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А.И. Белоус, В.А. Солодуха. – Москва : Техносфера, 2021. – 482 с.

3. Встреча с руководяищм и оперативным составом органов госбезопасности [Электронный ресурс] // Официальный сайт Президента Республики Беларусь. – Режим доступа : https://president.gov.by/ru/events/vstrecha-s-rukovodyashchim-i-operativnym-sostavom-organov-gosbezopasnosti. - Дата доступа : 23.09.2024.

4. Совещание по теме кибербезопасности. [Электронный ресурс] // Официальный сайт Президента Республики Беларусь. – Режим доступа : https://president.gov.by/ru/events/soveshchanie-po-teme-kiberbezopasnosti. – Дата доступа : 23.09.2024.

5. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А.И. Белоус, В.А. Солодуха. – Москва ; Вологда : Инфра-Инженерия, 2020. – 692 с.