УДК 004.056:621.311.1

# КИБЕРАТАКИ НА КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

С.Ю. Воробьев, Е.А. Ханчевский
*РУП «Белэнергосетьпроект», Минск, Беларусь*

**Аннотация.** Энергетика является одной из наиболее важных отраслей национальной экономики государства. Кибератаки на энергетические объекты могут привести к сбоям в подаче электроэнергии, авариям, значительному экономическому ущербу, человеческим жертвам. В данной статье рассмотрена тенденция государств к созданию киберподразделений в составе национальных вооруженных сил, проведению в киберпространстве учебных и боевых операций, сделан акцент на внимании, уделяемом руководством Республики Беларусь вопросам кибербезопасности и защиты критически важной инфраструктуры от кибератак, приведены кейсы зафиксированных инцидентов на объектах энергетики вследствие применения кибероружия. Перечислены основные нормативные правовые акты, регулирующие вопросы информационной безопасности и защиты информации, в том числе по вопросам организации противодействия кибератакам. В качестве примера описаны мероприятия организационного, правового и технического характера, осуществленные на одном из предприятий ГПО «Белэнерго» Министерства энергетики Республики Беларусь.
**Ключевые слова:** кибератака; кибербезопасность; защита информации; информационная безопасность; энергетика; объекты энергетики; жизнеобеспечение; критически важный объект; критически важный объект информатизации; гибридная война.

# CYBER ATTACKS ON CRITICAL ENERGY INDUSTRY FACILITIES

S.Yu. Vorobyov, E.A. Khanchevsky
*RUE «Belenergosetproekt», Minsk, Belarus*

**Abstract.** Energy is one of the most important sectors of the national economy of the state. Cyber attacks on energy facilities can lead to power outages, accidents, significant economic damage, and casualties. This article examines the tendency of states to create cyber units as part of national armed forces, conduct training and combat operations in cyberspace, emphasizes the attention paid by the leadership of the Republic of Belarus to issues of cybersecurity and protection of critical infrastructure from cyber attacks, and provides cases of recorded incidents at energy facilities due to the use of cyber weapons. The main regulatory legal acts governing information security and information protection issues, including those related to organizing counteraction to cyber attacks, are listed. As an example, organizational, legal and technical measures implemented at one of the enterprises of the State Production Association «Belenergo» of the Ministry of Energy of the Republic of Belarus are described.
**Keywords:** cyber attack; cyber security; information protection; information security; energy; energy facilities; life support; critical facility; critical information facility; hybrid war.

## Введение

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

## Основная часть

Тенденцией последних двух десятилетий явилась «милитаризация» киберпространства. Военно-политический блок НАТО в 2016 году на Варшавском саммите официально объявил киберпространство новой сферой проведения операций –

наряду с воздушной, сухопутной и морской [1]. Менее чем в 800 км от Минска в Таллине функционирует Центр передового опыта по совместной киберзащите НАТО, на базе которого проходят многочисленные учения и тренировки, в том числе флагманские ежегодные учения НАТО по действиям в киберпространстве «Кибер Коалиция».

Следует отметить, что Соединенные Штаты – одна из немногих стран, государственная политика которых рассматривает киберпространство как поле боя, а потому направлена на полный контроль этой сферы при наличии средств и возможностей на осуществление этого контроля [2]. При этом 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 [3].

Кратно вырос круг государств, создавших или создающих в составе национальных вооруженных сил подразделения информационной безопасности, включая кибервойска, задачей которых является проведение кибероперации. Реальный практический «боевой» опыт в киберпространстве имеют подразделения вооруженных сил США, Китая, КНДР, Ирана и др. Подразделение радиоэлектронной разведки «8200» Армии обороны Израиля известно не только участием в успешных кибератаках на иранские объекты атомной энергетики, но и тем, что выходцы из «8200» являются зачинателями многочисленных прибыльных стартапов в сфере информационной безопасности, например, Check Point Software Technologies Ltd.

Особый интерес представляет тот факт, что Министерство энергетики Соединенных Штатов наряду с такими спецслужбами, как ЦРУ, ФБР, АНБ, РУМО, 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 контразведки) [4]. Необходимо отметить, что Соединенные Штаты со всей серьезностью относятся к защите электроэнергетической системы от киберугроз в связи с чрезвычайной значимостью энергетического сектора национальной инфраструктуры.

Президент Республики Беларусь 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.

Глубокое проникновение энергетики во все отрасли экономики и в социальную сферу определяет ее особую роль в сфере безопасности. Система управления энергосистемой должна быть устойчивой к кибервоздействиям. Достигшая поставленных целей кибератака с высокой вероятностью нанесет урон сопоставимый с применением ядерного оружия: отключение важных инфраструктурных объектов мгновенно введет в хаос крупные мегаполисы и целые регионы [5]. Среди зафиксированных кибератак наибольший интерес вызывают следующие:

– инцидент на Игналинской АЭС (Литва) в 1994 году;

– совместная операция «Олимпийские игры» спецслужб США и Израиля по выведению из строя объектов атомной энергетики Ирана с применением

компьютерного вируса Stuxnet (данный вредонос был обнаружен в 2010 году белорусской антивирусной компанией);

– внедрение вредоносного программного обеспечения в информационные системы Korea Hydro & Nuclear Power Co., Ltd в 2014 году и немецкой АЭС «Gundremmingen» в 2015 [6].

Защита критически важной инфраструктуры является одной из наиболее важных задач обеспечения национальной безопасности любой страны. 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 целях повышения уровня защиты национальной инфраструктуры от внешних и внутренних угроз Президентом Республики Беларусь 14.02.2023 подписан Указ № 40 «О кибербезопасности», регулирующий основные принципы создания и функционирования национальной системы обеспечения кибербезопасности, который по сути является правовым фундаментом национальной системы обеспечения кибербезопасности, и направленный на дальнейшую реализацию положений Концепции национальной безопасности и взаимосвязан с Концепцией информационной безопасности. В рамках реализации данного указа Оперативно-аналитическим центром при Президенте Республики Беларусь 25.07.2023 был издан приказ № 130, а Совет Министров Республики Беларусь 23.02.2024 принял постановление № 120.

Обеспечение надлежащего уровня безопасности достигается путем выполнения комплекса организационных, правовых и технических мероприятий. В качестве примера приведем обстановку, сложившуюся по состоянию на текущий момент времени на предприятии, структурно входящем в ГПО «Белэнерго» Министерства энергетики Республики Беларусь (далее - Предприятие). Так, на Предприятии осуществлено:

– создание подразделения информационной безопасности в структуре Предприятия;

– разработка и актуализация локальных правовых актов (ЛПА), регулирующих вопросы информационной безопасности и защиты информации;

– проведение на постоянной основе инструктажей с работниками Предприятия, имеющими доступ с автоматизированных рабочих мест к ресурсам сети Интернет и почтовым сервисам;

– повышение квалификации руководителей структурных подразделений и работников Предприятия на тематических курсах, семинарах, конференциях и иных обучающих мероприятиях, посвященных вопросам информационной безопасности и защиты информации;

– получение лицензии на деятельность по технической и (или) криптографической защите информации в части проектирования систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

– запланировано к приобретению и внедрению сертифицированная в Республике Беларусь система предотвращения утечек конфиденциальной информации (DLP-система).

В целях совершенствования нормативного правового регулирования защиты информации и обеспечения кибербезопасности были подготовлены и направлены предложения в адрес регулятора.

В рамках проектирования строительства (реконструкции) объектов энергосистемы, предусматривающего, в том числе создание (модернизацию) информационных систем, осуществляется разработка соответствующего раздела «Информационная безопасность».

В настоящее время на Предприятии осуществляется разработка и внедрение системы менеджмента информационной безопасности на соответствие требованиям СТБ ISO/IEC 27001 (запланировано получение сертификата в Национальной системе подтверждения соответствия Республики Беларусь на систему менеджмента информационной безопасности).

## Заключение

Слабым местом растущей цифровизации энергосистемы является «чувствительность» последней к кибератакам. Последние, при надлежащей подготовке, выборе цели, приложении сил и средств, теоретически могут вывести из строя энергетическую сеть целой страны. В Республике Беларусь на государственном уровне уделяется внимание вопросам кибербезопасности и организации противодействия кибератакам, осуществляется поддержка и поощрение к применению лучших практик применения кибербезопасности. Действующая нормативная правовая база, регулирующая вопросы информационной безопасности и защиты информации, позволяет реализовывать Предприятию комплекс правовых, организационных и технических мероприятий, в том числе с запланированной сертификацией системы менеджмента информационной безопасности в Национальной системе подтверждения соответствия Республики Беларусь.

## Список использованных источников

1. Белоус А. И., Солодуха В. А. (2021) *Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения.* Москва, Издательство «Техносфера».

2. Харрис Ш. (2020) *Кибервойна@: Пятый театр военных действий.* Москва, Издательство «Альпина нон-фикшн».

3. Бартош А. А. (2023) *Гибридная война.* Москва. Издательство «КНОРУС».

4. Белоус А. И. (2020) *Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения.* Москва; Вологда. Издательство «Инфра-Инженерия».

5. Белоус А. И. (2020) *Кибероружие и кибербезопасность. О сложных вещах простыми словами.* Москва; Вологда, Издательство «Инфра-Инженерия».

6. Воробьев С. Ю., Ханчевский Е. А. (2024) Кибератаки на критически важные объекты энергетики как источник угроз национальной безопасности. *Энергетическая стратегия.* (6), 33–36.

## References

1. Belous A. I., Solodukha V. A. (2021) *Fundamentals of Cybersecurity. Standards, Concepts, Methods and Means of Support.* Moscow, Technosfera Publishing House (in Russian).

2. Harris S. (2020) *Cyberwar@: The Fifth Theater of Military Operations.* Moscow, Alpina Non-Fiction Publishing House (in Russian).

3. Bartosh A. A. (2023) *Hybrid War.* Moscow, KNORUS Publishing House (in Russian).

4. Belous A. I. (2020) *Cybersecurity of fuel and energy complex facilities. Concepts, methods and means of support.* Moscow; Vologda, Infra-Engineering Publishing House (in Russian).

5. Belous A. I. (2020) *Cyberweapons and cyber security. About complex things in simple words.* Moscow; Vologda. Infra-Engineering Publishing House (in Russian).

6. Vorobyov S. Yu., Khanchevsky E. A. (2024) Cyberattacks on critical energy facilities as a source of threats to national security. *Energy strategy.* (6), 33–36 (in Russian).

## Сведения об авторах

**Воробьев С. Ю.,** магистр техн. наук, заведующий сектором информационной безопасности отдела информационных технологий.
РУП «Белэнергосетьпроект», s.varabyou@besp.by.
**Ханчевский Е. А.,** начальник отдела информационных технологий.
РУП «Белэнергосетьпроект», zh@besp.by.

## Information about the authors

**Vorobyov S.Yu.,** Master of Engineering. Sciences. Head of the Information Security Sector of the Information Technology Department.
RUE «Belenergosetproekt», s.varabyou@besp.by.
**Khanchevsky E.A.,** Head of Information Technology Department. RUE «Belenergosetproekt», zh@besp.by