УДК 330.9

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ПРОДУКТОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ЭНЕРГЕТИКИ
THE USE OF INFORMATION PRODUCTS TO ENSURE THE SAFETY OF ENERGY FACILITIES

В.М. Барщевская
Научный руководитель – Е.П. Корсак, старший преподаватель
Белорусский национальный технический университет, г. Минск
V. Barshchevskaya
Supervisor – E. Korsak, Senior Lecturer
Belarusian national technical university, Minsk

Аннотация: *статья рассматривает важность повышения уровня кибербезопасности в энергетике, причины возникновения такой необходимости, описывает основные угрозы и мотивы со стороны киберприступников, масштабы последствий кибератак, предлагает пути решения имеющейся проблемы.*

Abstract: *the article examines the importance of improving cyber security in the energy sector, the reasons for this need, describes the main threats and motives of cyber criminals, and the scale of the consequences of cyber-attacks. the main threats and motives of cybercriminals, the scale of the consequences of cyber-attacks, and suggests ways to solve the problem.*

Ключевые слова: *кибербезопасность, автоматизация, цифровизация, электроэнергетическая система, энергоэффективность.*

Keywords: *cybersecurity, automation, digitalization, energy system, energy efficiency.*

Введение

Энергетический переход, происходящий в современных условиях, непосредственно связан с внедрением процессов автоматизации и цифровизации в сектор энергетики. Они позволяют осуществлять оперативный контроль и учёт показателей системы, ее дистанционное управление, обработку данных, защиту и блокировку действий, нарушающих технологический процесс, своевременно обнаруживать и устранять утечки энергии в сетях. Внедрение автоматизации и цифровизации значительно ускорилось за счёт пандемии covid-19 за счет появления необходимости дистанцировать протекающие в энергосистеме процессы. Использование новых технологий оптимизирует ход производства и распределения энергии, позволяет увеличить энергоэффективность системы за счёт оперативного подключения/выключения дополнительных мощностей с учетом изменения графика нагрузки и сезонных изменений в потреблении энергии, повысить качество показателей поставляемой энергии, однако одновременно служит причиной возникновения новых проблем. Основная из них – обеспечение кибербезопасности электоэнергетических систем.

Основная часть

Энергетика в настоящее время стоит в центре обеспечения деятельности всех отраслей экономики, так как их функционирование завязано на

технологиях, потребляющих электроэнергию. По этой причине основной её задачей является обеспечение бесперебойного энергоснабжения потребителей. В условиях расширения использования интеллектуальных технологий повышается необходимость пристального контроля за их безопасностью [1]. Объекты энергетики являются привлекательной мишенью для киберпреступников, заинтересованных в организации перебоев работы систем, выведении их из строя, получении скрытых данных энергетических предприятий. Среди таких киберпреступников могу оказаться представители сторонних государств, конкурирующих организаций и прочие лица, заинтересованные в перебоях работы энергосистемы или в получении ею убытка, который может достигать колоссальных сумм. Организация кибератак требует тщательного планирования, необходимо четко понимать слабые стороны программного обеспечения и знать, каким образом загрузить туда вредоносные программы. Из чего следует, что за подобными махинациями стоят зачастую не отдельные лица, а группы специалистов, работающие по поручению заинтересованных организаций/государств. Вычисление киберпреступников является практически невозможной задачей, так как атаки происходят удаленно, за частую, с территории других государств. Для предотвращения внедрений в систему из вне следует, в первую очередь, определить слабые стороны имеющейся системы защиты. К ним может относиться неактуальность используемого программного обеспечения, отсутствие системы безопасного удаленного доступа, халатность персонала и другие в зависимости от конкретной рассматриваемой ситуации. После анализа этих данных предпринимаются защитные меры и выстраивается система безопасности [2]. Электроэнергетические системы требуют постоянного аудита, так как в зависимости от цели атак имеют различную степень сложности их выявления. Так, например, при атаке с целью кражи информации системы, заметить наличие «шпиона» в системе невооруженным глазом непросто. Для надежной защиты следует постоянно обновлять программное обеспечение и использовать сразу несколько систем защиты. Некоторые организации держат в тайне, используемые на станциях системы защиты, так как без этой информации поиск путей внедрения в систему становится слишком время- и ресурсо-затратным для хакеров. Не менее важным является знание правил информационной безопасности сотрудниками, так как в таком случае они смогут избежать ошибок, приводящих к внедрению киберпреступников в сеть, а в случае, если это произошло, своевременно их обнаружить.

Заключение

Электроэнергетическая система является сложным техническим объектом, который обеспечивает энергией все отрасли промышленности, стратегически важные объекты для жизнедеятельности населения и государства, частных потребителей энергии и требует обеспечения максимально возможного уровня безопасности. Обеспечение кибербезопасности – достаточно дорогостоящий процесс, однако, учитывая возможные последствия кибератак, является целесообразным.

Литература

1. Пять шагов к цифровизации энергетики. – Режим доступа: https://trends.rbc.ru/trends/innovation/5d6796719a7947b5b36a5972 - Дата доступа: 23.10.2022.

2. Современный взгляд на безопасность. Энергетика. – Режим доступа: https://www.evraas.ru/industries/energy/ - Дата доступа: 23.10.2022.