УДК 330

КИБЕРБЕЗОПАСТНОСТЬ В ЭНЕРГЕТИКЕ

Тарасюк А. В. – студент,
Научный руководитель – Корсак Е. П., м. э. н., старший преподаватель
кафедры «Экономика и организация энергетики»,
Белорусский национальный технический университет,
г. Минск, Республика Беларусь

Аннотация: в данной статье рассматривается информационная безопасность, как одно из приоритетных направлений современной энергетической отрасли. Главная цель доклада заключается в определении основных тенденций дальнейшего повышения уровня защищенности данных на предприятиях энергетической системы. Для ее достижения рассма-триваются основные методы защиты от киберургоз, изучается опыт зарубежных компаний, которые подвергались кибератакам или сталкивались с хакерами, и выявляются основные направления и пути решения данной проблемы.

Ключевые слова: информационная безопасность, энергетическая отрасль, кибератака, энергосистема, промышленность.

CYBER SECURITY IN ENERGY

Abstract: this article replaces information security as one of the priorities of the modern energy industry. The main summary report solves the main problems associated with increasing the level of security of enterprises in the energy system. To study it, the main methods of protection against cyberurgosis, the achievements of foreign companies that have been subjected to cyberattacks or encountered hackers are evaluated, and the main directions and ways to solve this problem are identified.

Keywords: information security, energy industry, cyberattack, energy system, industry.

В современном мире все непрерывно совершенствуется, происходит автоматизация производства. Цифровые технологии внедряются во многие сферы человеческой деятельности, совершенствуя ручные процессы. В связи с этим увеличиваются объемы обрабатываемой информации, возникает необходимость снижения рисков подверженности кибератакам и инцидентам в области кибербезопастности.

Растущая цифровизация в современной энергетической отрасли создает необходимость постоянно улучшать параметры информационной безопасности. Защита огромного массива данных об энергетических объектах является одним из приоритетных направлений энергетического сектора.

Первая масштабная кибератака энергосистемы произошла в 2010 году с помощью программы Stuxnet. Данную программу называют также комью-

терный червь. Она распространялась на компьютеры с помощью USB-накопителей и перепрограммировала промышленные ПЛК (программируемый логический контроллер), уничтожая центрифуги на иранском предприятии по обогащению урана [1].

С тех пор энергетическая отрасль постоянно подвергается кибератакам.

В 2021 году крупная информационная атака произошла в США. Компания Colonial Pipeline, которая соединяет нефтеобрабатывающие заводы по всей территории США, потеряла управление над системами и для того чтобы его вернуть выплатила вымогателям выкуп в размере 4,4 миллиона долларов [2]. По данным компании IBM энергетика занимает четвертое место среди промышленных секторов, наиболее подверженных кибератакам секторов в 2021. Поэтому повышение уровня информационной безопасности является важнейшим направлением современной энергетической отрасли [3].

Основные методы защиты данных в энергетической отрасли:

– обеспечение безопасности поставок. Каждое звено в цепочке поставок должно быть защищено, так как компоненты содержат потенциальные недостатки, открывающие пространство для атак;

– обучение осведомленности о рисках. Сотрудники являются одним из самых ценных активов, часто из-за своей неосведомленности становятся объектами атак. Необходимость обучения информационной безопасности играет важную роль в повышении уровня киберзащиты;

– постоянный мониторинг рисков. Энергетическая отрасль нуждается в круглосуточном мониторинге, чтобы доставлять оповещения в случае возникновения инцидентов или сбоев.

Однако сложность заключается в том, что оборудование на энергопредприятиях рассчитано на несколько десятилетий, поэтому осуществить быструю модернизацию или замену оборудования для обеспечения дополнительной киберзащиты вызывает определенные трудности. Последствия этого перехода значительны как с финансовой, так и с операционной точки зрения. Таким образом, обеспечение информационной безопасности возможно только в длительном периоде. Необходимо, чтобы компании сообщали о новых методах обеспечения кибербезопасности и учитывали опыт предыдущих атак.

Список литературы

1. Stuxnet: what lessons can be learned twelve years on? [Электронный реесурс]. – Режим доступа: https://www.stormshield.com/news/stuxnet-what-lessons-can-be-learned-twelve-years-on/. – Дата доступа: 17.10.2022.

2. Energy sector: A cybersecurity obligation in the face of attacks to ensure the provision of essential services? [Электронный реесурс]. – Режим доступа: https://www.riskinsight-wavestone.com/en/2022/03/17662/. – Дата доступа: 19.10.2022.

3. X-Force Threat Intelligence Index 2022 [Электронный реесурс]. – Режим доступа: https://www.ibm.com/reports/threat-intelligence/. – Дата доступа: 23.10.2022.