УДК 004.896

КИБЕРБЕЗОПАСНОСТЬ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

К. О. Алексеева[1)], К. Д. Малахова[2)]

[1)] *студент, Белорусский государственный университет, г. Минск, Беларусь, karina.alexeeva777@gmail.com*
[2)] *студент, Белорусский государственный университет, г. Минск, Беларусь, kristina.malakhova.06@bk.ru*

Научный руководитель: **Т. А. Бронская**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, bronska.tatiana@yandex.ru

В статье рассматриваются ключевые аспекты кибербезопасности в автоматизированных системах управления. Исследуется влияние киберугроз на эффективность и надежность этих систем, а также подчеркивается важность внедрения современных методов защиты информации. В работе акцентируется внимание на необходимости комплексного подхода к обеспечению безопасности, включая технические, организационные и правовые меры, что позволяет адаптировать системы управления к постоянно меняющимся киберугрозам.

Ключевые слова: кибербозопаность; киберугрозы; автоматизированные системы управления.

CYBER SECURITY IN AUTOMATED CONTROL SYSTEMS

K. O. Alexeeva[1)], K. D. Malakhova[2)]

[1)] *student, Belarusian State University, Minsk, Belarus, karina.alexeeva777@gmail.com*
[2)] *student, Belarusian State University, Minsk, Belarus, kristina.malakhova.06@bk.ru*

Supervisor: **T. A. Bronskaia**

senior lecturer, Belarusian State University, Minsk, Belarus, bronska.tatiana@yandex.ru

The article discusses key aspects of cyber security in automated control systems. It explores the impact of cyber threats on the efficiency and reliability of these systems and emphasises the importance of implementing modern methods of information protection. The paper focuses on the need for an integrated approach to security, including technical, organisational and legal measures, which allows management systems to adapt to ever-changing cyber threats.

Keywords: cyber security; cyber threats; automated control systems.

В современном мире автоматизированные системы управления (АСУ) – это комплекс аппаратных и программных средств, а также персонала, предназначенный для обеспечения и автоматизации эффективного управления процессами на предприятии. Они играют критически важную роль в оптимизации и модернизации процессов в различных отраслях. Их внедрение способствует повышению производственной эффективности, улучшению качества обслуживания и сокращению временных затрат. АСУ обеспечивают интеграцию множества функций и процессов, что позволяет организациям оперативно реагировать на изменения внешней среды и требования рынка. Однако с ростом популярности этих технологий возрастает и их уязвимость к киберугрозам. Под киберугрозой понимается незаконное проникновение в информационное пространство для достижения политических, социальных или иных целей.

В условиях быстро меняющегося технологического ландшафта, когда кибератаки становятся все более сложными и разнообразными, обеспечение кибербезопасности становится неотъемлемой частью успешной работы любой организации.

Кибербезопасность в автоматизированных системах управления (АСУ) является важной темой, требующей особого внимания. Кибербезопасность – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации от кибератак.

Современные АСУ применяются в различных отраслях, включая энергетику, транспорт, здравоохранение и науку. Они обеспечивают автоматизацию процессов, что повышает их эффективность и снижает затраты. Однако с ростом использования АСУ и увеличением зависимости от них увеличивается и риск кибератак, которые могут привести к серьезным последствиям, таким как остановка производства, утечка данных и финансовые потери. Кибербезопасность охватывает методы и технологии, направленные на защиту компьютерных систем, сетей и конфиденциальной информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Она снижает физические, программные и сетевые риски для производства; производственные операции в значительной степени зависят от систем управления и других технологий, которые уязвимы для киберугроз.

Киберугрозы можно классифицировать на несколько категорий, таких как вредоносное ПО, атаки типа «отказ в обслуживании» (DoS), фишинг и целенаправленные атаки. Уязвимости в программном обеспечении могут быть использованы злоумышленниками для получения несанкционированного доступа к системам. Человеческий фактор, включая ошибки пользователей и недостаточную осведомленность о киберугрозах, также

играет значительную роль в обеспечении безопасности. Атаки на АСУ могут привести к серьезным последствиям, включая остановку производства и угрозу безопасности людей, что делает вопрос кибербезопасности особенно актуальным.

Современные методы защиты информации включают технические, организационные и правовые меры. Технические методы защиты информации играют ключевую роль в обеспечении кибербезопасности АСУ. Эти методы включают в себя различные технологии и подходы, направленные на предотвращение несанкционированного доступа, защиту данных и обеспечение целостности и конфиденциальности информации. К техническим мерам относятся шифрование данных, аудит и мониторинг системного трафика, а также системы предотвращения вторжений.

Организационные меры включают обучение персонала и разработку политик безопасности, а также контроль за соблюдением политик, что способствует улучшению общей защиты. Автоматизированные системы управления технологическими процессами имеют свою специфику, поэтому для обеспечения безопасности АСУ необходимы специалисты с особыми навыками и знаниями, которые позволят эффективно защищать эти системы от киберугроз.

В правовом аспекте важным является соблюдение международных стандартов, таких как GDPR и ISO/IEC 27001, что помогает в управлении рисками и повышении защиты информации. GDPR (General Data Protection Regulation) – это регламент Европейского союза о защите персональных данных, который вступил в силу в 2018 году. Он устанавливает строгие требования к обработке и защите личных данных граждан ЕС. GDPR требует от организаций соблюдения определённых мер безопасности, включая шифрование данных, ограничение доступа, регулярное тестирование систем на уязвимости и другие меры. Несоблюдение этих требований может привести к штрафам и юридическим последствиям.

ISO/IEC 27001 – это международный стандарт по информационной безопасности, разработанный Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC). Стандарт определяет требования к системе управления информационной безопасностью (СУИБ), которая помогает организациям обеспечивать защиту своих информационных активов. ISO/IEC 27001 включает в себя такие аспекты, как управление рисками, контроль доступа, обеспечение целостности данных и другие меры безопасности.

Таким образом, для достижения надежной кибербезопасности в АСУ необходим комплексный подход, который интегрирует все вышеперечисленные меры. Создание многослойной защиты делает системы более устойчивыми к киберугрозам. Важно, чтобы системы управления имели

возможность адаптироваться к новым вызовам, что требует регулярного аудита безопасности и обновления мер защиты.

Кибербезопасность в автоматизированных системах управления требует постоянного внимания и выделения ресурсов для противодействия эволюционирующим угрозам. Эффективная киберзащита не только предотвращает инциденты, но и способствует созданию устойчивой инфраструктуры, обеспечивающей безопасность и целостность данных. В условиях, когда киберугрозы становятся все более сложными и разнообразными, необходимость в высококвалифицированных специалистах, обладающих уникальными знаниями и навыками, становится особенно актуальной.

Библиографические ссылки

1. О кибербезопасности [Электронный ресурс] : Указ Президента Республики Беларусь, 14 февраля 2023 г., № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

2. *Алпеев А. С.* Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5(8). С. 39–42.

3. *Зегжда Д. П. и др.* Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации //Вопросы кибербезопасности. 2018. № 2(26). С. 2–15.