ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ СОВРЕМЕННЫХ АСУ ТП

СЕЛИВАНОВА Марина Валерьевна
кандидат технических наук, доцент
Уфимский университет науки и технологий
г. Уфа, Россия
СЕЛИВАНОВ Владимир Константинович
студент
Национальный исследовательский ядерный университет «МИФИ»
г. Москва, Россия

В статье рассмотрены основные направления развития автоматизированных систем управления технологическими процессами (АСУ ТП) и риски в сфере их кибербезопасности. Актуальность работы связана с интеграцией АСУ ТП с корпоративными информационными системами и сетью Интернет, что приводит к появлению новых угроз информационной безопасности АСУ ТП.
Ключевые слова: АСУ ТП, кибербезопасность, промышленная автоматизация, IIoT, защита критических инфраструктур.

Автоматизированные системы управления технологическими процессами [1] прошли путь развития от локальных регуляторов до интегрированных цифровых платформ для концепции «умного производства» Industry 4.0. Современные АСУ ТП – это комплексные, гибкие и открытые системы, интегрируемые с корпоративными информационными системами и глобальными сетями. Основные тенденции их развития – это стремление к повышению эффективности и гибкости производственных процессов, необходимость обеспечения прозрачности управления, активное внедрение промышленного интернета вещей (IIoT), развитие облачных технологий и аналитики больших данных.

Однако вместе с новыми возможностями растут и риски, особенно в области кибербезопасности. Открытость, сетевое и облачное взаимодействие превращают АСУ ТП в потенциальные цели для кибератак, способных нанести ущерб технологической, экологической и промышленной безопасности. Рассмотрим основные направления развития АСУ ТП и связанные с этим риски.

1. Информационные и операционные технологии.

Современные АСУ ТП основаны на объединении информационных (IT) и операционных технологий (OT): на контроллеры устанавливают операционные системы, для объединения SCADA-серверов используют виртуализацию, для анализа информации используют облачные платформы. Это открывает возможности для повышения эффективности и гибкости управления, но одновременно приводит к появлению новых разновидностей киберугроз:

– распространение угроз из IT-инфраструктуры на OT-среду. Примеры: вирусы Stuxnet, Industroyer, Triton;

– использование общих операционных систем (Linux или Windows) и стандартных протоколов (TCP/IP, HTTP, OPC UA) делает OT-устройства уязвимыми к тем же атакам, что и обычные IT-системы;

– внедрение облачных платформ (AWS IoT, Azure IoT, MindSphere и др.) создаёт новые каналы передачи данных, выходящие за пределы завода;

– недостаточная компетентность специалистов на стыке IT и OT;

– отсутствие ограничений длительности жизненного цикла для OT-устройств.

2. Промышленный Интернет Вещей (IIoT) и облачные технологии.

Внедрение IIoT и облачных технологий приводит не только к изменению архитек-

туры АСУ ТП, обеспечивая прозрачность технологических процессов, эксплуатации и ремонта оборудования, но также к появлению новых направлений кибератак, таких как:

– эксплуатация уязвимостей в «умных» датчиках и устройствах IIoT;

– перехват, подмена или подделка данных с полевых устройств;

– несанкционированный доступ к облачным платформам аналитики и управления (например, Azure IoT, AWS IoT, MindSphere);

– атаки на каналы связи между OT-средой и облачным сервисом;

– зависимость от сторонних облачных провайдеров и «теневые» IoT-проекты, которые становятся точками входа в корпоративную инфраструктуру.

3. Цифровые двойники.

Цифровой двойник – это виртуальная модель физического объекта, которая синхронизируется с ним в реальном времени за счёт постоянного потока данных от датчиков IIoT и АСУ ТП. Она предназначена для оптимизации работы и обслуживания оборудования и повышения эффективности производства, но является основой для появления следующих киберугроз:

– компрометация целостности данных цифрового двойника: злоумышленник может подменить данные, поступающие от датчиков или АСУ ТП, что приведёт к некорректному поведению физического объекта;

– использование цифрового двойника как источника атаки на физическую систему, если цифровой двойник способен управлять этой системой;

– атака на инфраструктуру хранения и обработки данных цифрового двойника в облачных средах, уязвимости которых могут стать точкой входа для DoS-атак;

– расширение направлений кибератак за счёт новых интерфейсов программирования цифровых двойников, особенно, если используется слабая аутентификация или отсутствует шифрование данных.

4. Применение искусственного интеллекта и машинного обучения.

Искусственный интеллект (ИИ) и машинное обучение (МО) помогают анализировать данные, получаемые АСУ ТП и устройств IIoT, и использовать функционал цифровых двойников. Это открывает возможности для оптимизации, диагностики и обслуживания технологического оборудования, но также приводит к появлению новых киберугроз, таких как:

– компрометация обучающей выборки: злоумышленник может целенаправленно искажать данные, используемые для обучения модели ИИ/МО;

– манипуляции с моделью ИИ/МО и отсутствие ее прозрачности;

– длительный жизненной цикл модели ИИ, что приводит к эксплуатации злоумышленниками ее известных уязвимостей.

5. Тренд на открытость, кроссплатформенность и импортозамещение.

Обеспечение технологической независимости требует открытой, кроссплатформенной архитектуры. Хотя открытость и стандартизация повышают гибкость и совместимость оборудования разных производителей, но также создают предпосылки для появления уникальных киберугроз, таких как:

– уязвимости в новых отечественных решениях, которые внедрены при отсутствии долгосрочной эксплуатации и обратной связи с производством;

– несовместимость политик безопасности в ПО разных производителей;

– зависимость от сторонних библиотек и открытого ПО, которые могут содержать известные уязвимости при отсутствии выпуска обновлений ПО;

– риск поставки оборудования с предустановленными закладками, если отсутствуют процедуры верификации и сертификации.

Следовательно, эволюционное развитие АСУ ТП привело к появлению новых киберугроз, которые не могут быть оставлены без рассмотрения, особенно для объектов критической инфраструктуры. В дальнейшем авторы планируют исследовать перспективные направления обеспечения кибербезопасности АСУ ТП на основе комплексного подхода, сочетающего технические и организационные меры защиты с требования действующего законодательства.

СПИСОК ЛИТЕРАТУРЫ
1. *Сдобникова И.С.* Кибербезопасность АСУ ТП: как защитить промышленность в 2025 году. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/ICS-Cybersecurity-AM-Live-2025 (дата обращения: 15.10.2025).

POTENTIAL CYBERSECURITY THREATS TO MODERN APCS

SELIVANOVA Marina Valeryevna
Candidate of Sciences in Technology, Docent
Ufa University of Science and Technology
Ufa, Russia
SELIVANOV Vladimir Konstantinovich
Student
National Research Nuclear University MEPhI
Moscow, Russia

The article discusses the main directions of development of automated process control systems (APCS) and their cybersecurity risks. The relevance of the work is related to the integration of APCS with corporate information systems and the Internet, which leads to the emergence of new threats to the information security of APCS.
Keywords: APCS, cybersecurity, industrial automation, IIoT, protection of critical infrastructures.