УДК 004.896

КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМАХ АВТОМАТИЧЕСКОГО КОНТРОЛЯ

Андрей Юрьевич Астапов
кандидат технических наук, доцент
astapow_a@mail.ru
Диана Юрьевна Стурова
студент
dianasturova04@yandex.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. Данная статья посвящена проблемам кибербезопасности систем автоматического контроля (АСК) в эпоху цифровизации. Среди ключевых уязвимостей — отсутствие надёжной аутентификации устройств, устаревшее ПО, небезопасный обмен данными, недостаточная сетевая сегментация, человеческий и физический факторы риска.

Ключевые слова: системы автоматического контроля (АСК), кибербезопасность, киберугрозы, уязвимости, информационная безопасность.

В эпоху стремительной цифровизации системы автоматического контроля (АСК) — комплексы из датчиков, контроллеров, серверов и ПО — становятся ключевым инструментом оптимизации производства. Они повышают точность и надёжность производственных циклов, минимизируют влияние человеческого фактора. Однако интеграция IT-технологий несёт не только преимущества, но и серьёзные риски: АСК уязвимы перед киберугрозами [1].

Анализ архитектуры АСК выявляет целый спектр критических уязвимостей. Во-первых, многие устройства (от датчиков до контроллеров) не имеют надёжных механизмов аутентификации — это позволяет злоумышленникам имитировать работу оборудования, перехватывать управление и провоцировать сбои. Во-вторых, широкое распространение устаревшего ПО создаёт предпосылки для внедрения вредоносного кода и несанкционированного доступа: из-за отсутствия обновлений в программах накапливаются уязвимости. В-третьих, небезопасный обмен данными — либо без шифрования, либо через скомпрометированные протоколы — даёт возможность перехватывать информацию и дестабилизировать работу системы. Серьёзную угрозу несёт отсутствие сетевой сегментации: прямая интеграция АСК с корпоративной ИТ-инфраструктурой без изоляции повышает вероятность проникновения вредоносного ПО. Злоумышленники могут использовать менее защищённые участки сети для атак на критически важные системы управления [2].

Не менее значим человеческий фактор. Ошибки персонала — от недостаточной квалификации до подверженности социальной инженерии — формируют многочисленные бреши в защите. Сотрудники могут раскрыть учётные данные, подключить неавторизованные устройства или пренебречь правилами эксплуатации.

Физические уязвимости тоже нельзя игнорировать. Несанкционированный доступ к аппаратуре (контроллерам, датчикам, серверам) позволяет напрямую вмешиваться в работу системы. Риски

возрастают, если помещения с оборудованием не защищены базовыми средствами охраны: видеонаблюдением, контролем доступа, сигнализацией.

Совокупность этих факторов создаёт комплексную угрозу безопасности АСК. Нейтрализовать её можно только системным, комплексным подходом — сочетанием технических и организационных мер [3].

Основой защиты служит шифрование данных с помощью протоколов TLS и IPSec, гарантирующее конфиденциальность информации. Усиливает безопасность многофакторная аутентификация: помимо логина и пароля, система запрашивает дополнительные подтверждения личности (одноразовые коды, цифровые сертификаты). Важную роль играет сегментация сети: промышленную инфраструктуру делят на изолированные зоны с дифференцированным доступом, а критически важные узлы размещают в защищённых сегментах. Это минимизирует риски распространения вредоносного ПО. Регулярное обновление ПО и мониторинг оборудования позволяют своевременно устранять уязвимости и выявлять угрозы. Для анализа трафика и блокировки попыток атак применяют системы IDS/IPS. Защиту конечных точек (серверов, контроллеров, рабочих станций) обеспечивают антивирусное ПО и межсетевые экраны (файерволы) [4].

Прозрачность работы системы поддерживают журналирование и мониторинг событий: анализ логов помогает отследить инциденты и оценить эффективность защиты. Снизить риски физического доступа помогают пропускные системы, электронные замки, видеонаблюдение, сигнализация и специализированные шкафы для оборудования.

Ключевой элемент защиты — подготовленность персонала. Инструктажи по кибергигиене, тренинги по распознаванию фишинга и симуляции кибератак существенно снижают вероятность инцидентов.

Наконец, работоспособность системы после кибератаки гарантируют механизмы резервного копирования и восстановления. Сюда входят регулярное создание резервных копий критически важных данных, их хранение в защищённых хранилищах, разработка планов восстановления (disaster recovery

plan) и отработка сценариев восстановления в ходе учений. Реализация этих взаимосвязанных мер создаёт многоуровневую систему защиты, способную противостоять большинству киберугроз.

На этапе проектирования любой системы критически важно заложить базовые принципы информационной безопасности. Рассмотрим ключевые из них.

Во-первых, принцип наименьших привилегий предполагает, что каждый компонент системы — будь то программный модуль, датчик или сервер — получает только те права доступа, которые строго необходимы для выполнения его задач. Такой подход минимизирует риски в случае взлома отдельных элементов.

Во-вторых, безопасность должна изначально входить в архитектуру системы, а не добавляться как дополнительная «надстройка». Этот принцип известен как Security by Design («заложенная защита»). На практике это означает одновременную разработку основных функций и защитных механизмов: аутентификации, шифрования, сегментации сети, журналирования событий, физической защиты [5].

В-третьих, проект обязан соответствовать нормативным требованиям — учитывать положения профильных законов и стандартов. (рисунок 1):

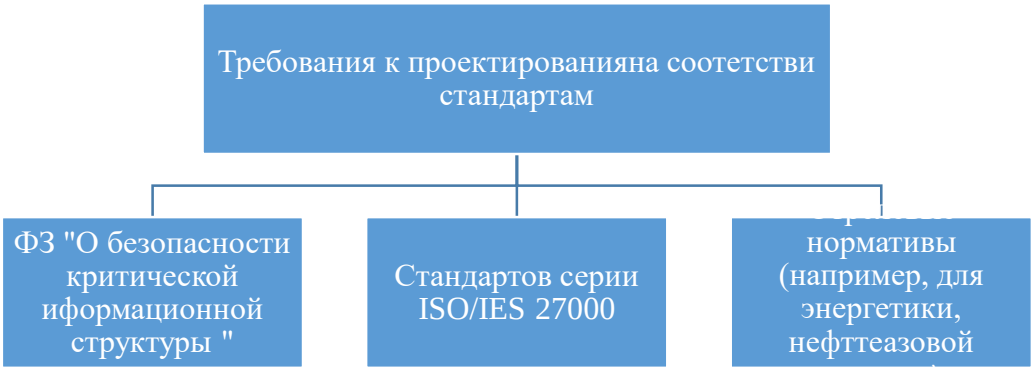

Рисунок 1– Требования профильных нормативных актов.

Помимо базовых, существуют важные дополнительные принципы информационной безопасности:

1) Оценка рисков: На этапе проектирования анализируйте угрозы и составляйте карту рисков для выявления уязвимостей и принятия мер.

2) Модульность и изоляция: Проектируйте систему так, чтобы уязвимые компоненты можно было изолировать, минимизируя последствия атак.

3) Реагирование на инциденты: Разработайте четкий регламент действий при киберугрозах, включая роли, алгоритмы и устранение последствий.

4) Тестирование на проникновение: Регулярно проводите "белые хакерские" атаки для выявления уязвимостей и корректировки защитных мер.

5) Документация мер безопасности: Четко описывайте процедуры, настройки и конфигурации для слаженной работы команды и передачи знаний.

6) Планирование жизненного цикла системы — ключевой элемент стратегии информационной безопасности. Оно подразумевает, что требования защиты необходимо учитывать на всех этапах существования системы: от разработки и внедрения до модернизации и вывода из эксплуатации.

Такой подход обеспечивает непрерывную и целостную защиту информационных активов. Иными словами, безопасность не должна рассматриваться как разовая мера или дополнение к основному процессу — она должна быть заложена в основу жизненного цикла системы и сопровождать его на каждом шаге.

Эта позиция особенно актуальна в эпоху цифровизации. Сегодня обеспечение кибербезопасности систем автоматического контроля (АСК) — критически важная задача: ошибки или взломы могут привести к серьёзным последствиям, включая финансовые потери и технологические аварии.

Основа безопасности — принцип Security by Design («безопасность через проектирование»). На этапе создания системы нужно заложить ключевые механизмы защиты: аутентификацию, шифрование данных, сегментацию сети, журналирование событий, физическую охрану оборудования. Необходимо

регулярно обновлять систему: проверять защиту, устанавливать патчи безопасности, оптимизировать настройки.

Ключевой фактор — компетентность персонала. Операторы, инженеры, администраторы должны распознавать атаки и быстро реагировать на инциденты; им нужны регулярные тренинги и разбор реальных кейсов. Важна и юридическая сторона: соблюдение отраслевых стандартов и законов (например, правил защиты критической инфраструктуры и обработки персональных данных) помогает избежать правовых рисков. Не менее значима культура информационной безопасности в организации: сотрудники должны понимать свою ответственность, избегать фишинга и социальной инженерии, соблюдать правила кибергигиены [6].

Таким образом, кибербезопасность АСК — это не разовая задача, а постоянный процесс, требующий регулярного аудита, адаптации под новые угрозы и совершенствования на всех этапах жизненного цикла системы. Соблюдение обозначенных принципов и подходов позволит обеспечить долгосрочную, устойчивую защиту систем автоматического контроля и заложить фундамент для безопасного развития промышленной цифровизации.

Список литературы:

1. Белов Е.Б., Заболотский В.П., Шаньгин В.Ф. Защита информации: учебник для вузов / М.: Юрайт, 2024. 420 с. (Высшее образование). ISBN 978-5-534-XXXX-X.

2. Игнатьев В.С., Петров А.Н. Кибербезопасность промышленных систем автоматизации // Информационная безопасность. 2024. № 3. С. 45–58.

3. Смирнов А.В., Соколов Д.И. Архитектура защищённых промышленных систем // Приборы и системы. Управление, контроль, диагностика. 2024. № 5. С. 23–37.

4. Отчёт «Кибербезопасность промышленных систем автоматизации» / Positive Technologies, 2024 г.

5. Доклад «Состояние кибербезопасности в промышленности России» / Лаборатория Касперского, 2024 г.

6. Отчёты по тестированию на проникновение (penetration testing) ведущих компаний в сфере ИБ за 2023–2024 гг. (Positive Technologies, «Лаборатория Касперского», Group-IB и др.).

UDC 004.896

CYBERSECURITY IN AUTOMATIC CONTROL SYSTEMS

Andrey Yu. Astapov
candidate of technical sciences, associate professor
astapow_a@mail.ru
Diana Yu. Sturova
student
dianasturova04@yandex.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract. This article focuses on the challenges of cybersecurity in automatic control systems (ACS) in the era of digitalization. Among the key vulnerabilities are the lack of reliable device authentication, outdated software, insecure data exchange, insufficient network segmentation, and human and physical risk factors.

Keywords: Automatic Control Systems (ACS), cybersecurity, cyber threats, vulnerabilities, and information security.

Статья поступила в редакцию 01.11.2025; одобрена после рецензирования 20.12.2025; принята к публикации 29.12.2025.

The article was submitted 01.11.2025; approved after reviewing 20.12.2025; accepted for publication 29.12.2025.