УДК 004.056.5:681.5

Пономарев Максим Сергеевич,
студент направления подготовки 15.03.04 «Автоматизация технологических процессов и производств»
ФГАОУ ВО «МГТУ «СТАНКИН»
Россия, г. Москва
Кищенко Роман Валерьевич,
студент направления подготовки 15.03.04 «Автоматизация технологических процессов и производств»
ФГАОУ ВО «МГТУ «СТАНКИН»
Россия, г. Москва

КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Аннотация: *В статье рассмотрены особенности обеспечения кибербезопасности промышленных автоматизированных систем управления с учётом требований непрерывности технологического процесса, функциональной безопасности и ограниченной возможности оперативного обновления оборудования. Систематизированы основные угрозы для SCADA-систем, программируемых логических контроллеров, инженерных станций и промышленных сетей. Предложена многоуровневая архитектура защиты, основанная на сегментации, выделении промышленной демилитаризованной зоны, контролируемом удалённом доступе, регистрации событий и резервировании критически важных компонентов. Разработан иллюстративный индекс приоритета риска, позволяющий ранжировать сценарии атак по вероятности, тяжести последствий и степени экспозиции. Сформулированы практические рекомендации по организации мониторинга, управлению уязвимостями и реагированию на инциденты без нарушения устойчивости производства.*

Ключевые слова: *промышленная автоматизация, АСУ ТП, кибербезопасность, SCADA, программируемый логический контроллер, сегментация сети, управление рисками.*

Annotation: *The article examines cybersecurity of industrial automated control systems with regard to process continuity, functional safety and limited opportunities for rapid equipment updates. The main threats to SCADA systems, programmable logic controllers, engineering workstations and industrial networks are systematized. A defence-in-depth architecture based on network segmentation, an industrial demilitarized zone, controlled remote access, event logging and redundancy of critical components is proposed. An illustrative risk-priority index is introduced to rank attack scenarios by likelihood, consequence severity and exposure. Practical recommendations for monitoring, vulnerability management and incident response without disrupting production stability are formulated.*

Key words: *industrial automation, industrial control system, cybersecurity, SCADA, programmable logic controller, network segmentation, risk management.*

Промышленная АСУ представляет собой киберфизическую систему, в которой информационное воздействие способно изменить состояние материального объекта. Компрометация инженерной станции может привести к загрузке изменённой программы в контроллер, а подмена данных датчика — к ошибочному управляющему воздействию. Поэтому конфиденциальность информации важна, но приоритетными свойствами обычно являются целостность команд, доступность управления, подлинность источника данных и сохранение безопасного режима.

Существенной особенностью является длительный жизненный цикл оборудования. Контроллеры, станции и сетевые устройства могут эксплуатироваться десять и более лет, тогда как поддержка операционных систем и встроенного программного обеспечения заканчивается значительно раньше. Замена компонента часто требует остановки установки, повторной аттестации алгоритмов и технологических испытаний. В результате

уязвимость нельзя устранять теми же темпами, что и в офисной инфраструктуре, а компенсирующие меры приобретают особое значение.

Ещё одно ограничение связано с производственной совместимостью защитных средств. Активное сканирование, агрессивная проверка уязвимостей или неверно настроенная система предотвращения вторжений способны перегрузить устаревшее устройство либо нарушить протокол обмена. По этой причине мониторинг промышленной сети должен начинаться с пассивного анализа трафика, инвентаризации и проверки изменений в согласованное технологическое окно.

Матрица MITRE ATT&CK for ICS выделяет тактики, связанные не только с первоначальным доступом и перемещением по сети, но также с подавлением функций реагирования, нарушением управления процессом и непосредственным воздействием на производство [7]. Это позволяет связывать технические события с возможным физическим результатом и строить защиту вокруг критических функций, а не только вокруг отдельных компьютеров.

Таблица 1.

Основные сценарии угроз для промышленной АСУ

Сценарий	Возможный источник	Последствия для процесса	Приоритетные меры
Компрометация удалённого доступа	Подрядчик, похищенная учётная запись, уязвимый шлюз	Несанкционированный вход в технологическую сеть, изменение настроек и программ	Промышленная DMZ, многофакторная аутентификация, jump-сервер, запись сеансов
Изменение логики ПЛК	Злоумышленник или ошибочное действие инженера	Неверная последовательность операций, отключение блокировок, повреждение оборудования	Разделение ролей, контроль версий, подпись и сравнение проектов, независимые защиты
Вредоносный код со съёмного носителя	USB-накопитель, сервисный ноутбук	Заражение инженерной станции, распространение по общим ресурсам	Контролируемая станция проверки, белые списки ПО, запрет неизвестных носителей
Подмена технологических данных	Атака на сетевой обмен или сервер архивов	Ошибочные решения оператора и регулятора, сокрытие аварийного состояния	Сегментация, защищённые протоколы, контроль целостности, независимые измерения

Отказ сетевого оборудования или DoS	Атака, неисправность, неверная конфигурация	Потеря связи с контроллерами и HMI, останов либо переход в локальный режим	Резервирование, ограничение трафика, локальные контуры, испытанные аварийные режимы

В Российской Федерации правовую основу защиты значимых объектов критической информационной инфраструктуры формирует Федеральный закон № 187-ФЗ. Он определяет основные понятия, полномочия субъектов и требования, связанные с обеспечением безопасности критической информационной инфраструктуры [1]. Для предприятий, чьи автоматизированные системы относятся к значимым объектам КИИ, организационные и технические решения должны быть увязаны с результатами категорирования и установленными обязанностями субъекта.

Приказ ФСТЭК России № 235 устанавливает требования к созданию систем безопасности значимых объектов КИИ, а приказ № 239 определяет требования по обеспечению их безопасности [2; 3]. Практическое значение этих документов заключается в необходимости рассматривать защиту как управляемую систему: определить ответственных, состав объектов, границы, угрозы, набор мер, порядок контроля и совершенствования.

Серия стандартов IEC 62443 и её национальные версии ориентированы на системы промышленной автоматизации и управления. ГОСТ Р МЭК 62443-2-1-2015 описывает программу обеспечения защищённости на уровне организации, а ГОСТ Р МЭК 62443-3-3-2016 содержит системные требования и уровни безопасности [4; 5]. Важным архитектурным принципом является разделение системы на зоны и соединяющие их каналы. Зона объединяет активы с близкими требованиями, а канал определяет контролируемый обмен между зонами.

Для промышленных систем целесообразно сочетать нормативный подход с практическими рекомендациями NIST и CISA. NIST SP 800-82 Rev. 3 рассматривает топологии OT, угрозы, уязвимости и защитные меры [6]. CISA публикует рекомендации по глубокоэшелонированной защите,

безопасному удалённому доступу, управлению обновлениями и реагированию на инциденты [8]. Использование нескольких источников позволяет не ограничиваться формальной проверкой наличия средства, а оценивать его реальную роль в снижении технологического риска.

Основой устойчивой защиты является принцип глубокоэшелонированной безопасности. Он предполагает, что отказ или обход одного механизма не должен автоматически предоставлять доступ к критическим функциям. Защитные уровни включают физическую безопасность, управление учётными записями, сегментацию, контроль приложений, мониторинг, резервирование и подготовленное реагирование.

Предлагаемая архитектура представлена на рисунке 1. Корпоративная ИТ-сеть отделяется от технологической среды промышленной демилитаризованной зоной. В DMZ размещаются сервер обмена данными, jump-сервер для контролируемого удалённого доступа, репозиторий проверенных обновлений и промежуточный сервер журналов. Прямое соединение пользовательского компьютера с ПЛК или инженерной станцией не допускается.

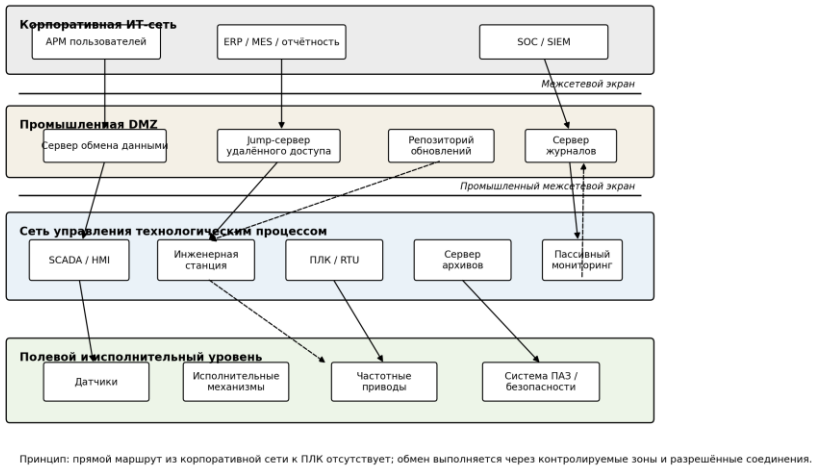

Рисунок 1. Предлагаемая сегментированная архитектура промышленной АСУ

Внутри технологической сети следует выделять отдельные зоны для SCADA-серверов, инженерных станций, контроллеров, систем противоаварийной защиты и вспомогательных сервисов. Разделение выполняется промышленными межсетевыми экранами с разрешающими правилами по принципу минимально необходимого обмена. Правила должны фиксировать источник, назначение, протокол, порт, направление, назначение соединения и ответственного владельца.

Удалённый доступ представляет один из наиболее значимых рисков, поскольку объединяет внешнюю среду и критическую технологическую сеть. Доступ необходимо предоставлять на ограниченный срок, через выделенный шлюз, с многофакторной аутентификацией и индивидуальной учётной записью. Сеанс должен регистрироваться, а передача файлов — проходить проверку. Постоянные общие учётные записи подрядчиков и прямой VPN-доступ к контроллерам противоречат принципу минимальных привилегий.

Инженерные станции требуют отдельного режима эксплуатации. На них следует запретить повседневную работу с электронной почтой и интернетом, ограничить запуск программ, вести эталонные копии проектов и регистрировать загрузку логики в ПЛК. Изменение проекта должно сопровождаться заявкой, проверкой, резервным копированием, технологическим испытанием и возможностью возврата к подтверждённой версии.

Для системы противоаварийной защиты критично сохранить независимость от обычного контура управления. Информационный обмен между зонами должен быть минимальным и преимущественно однонаправленным там, где это допускает технология. Кибератака на SCADA или инженерную станцию не должна отменять аппаратные блокировки и безопасное действие локальных защит. ГОСТ Р 59506-2021 отдельно рассматривает взаимосвязь информационной и функциональной безопасности машин [9].

Таблица 2.

Распределение защитных мер по уровням промышленной системы

Уровень	Защищаемые элементы	Ключевые меры	Контроль результата
Организационный	Персонал, подрядчики, процессы изменений	Роли и ответственность, обучение, допуск, регламент изменений, план реагирования	Аудит прав, учения, анализ нарушений регламента
Периметр и DMZ	Удалённый доступ, обмен с ИТ-сетью	Межсетевые экраны, jump-сервер, MFA, прокси и промежуточные серверы	Журналы соединений, запись сеансов, периодический пересмотр правил
Технологическая сеть	SCADA, серверы, инженерные станции	Сегментация, белые списки, контроль приложений, резервное копирование, пассивный мониторинг	Инвентаризация, контроль конфигураций, корреляция событий
Уровень управления	ПЛК, RTU, приводы, контроллеры безопасности	Уникальные учётные данные, запрет неиспользуемых сервисов, контроль проектов, ограничение программирования	Сравнение контрольных сумм и версий, журналирование загрузок
Физический процесс	Датчики, исполнительные механизмы, технологические защиты	Независимые пределы, безопасное состояние, резервирование, ручной режим	Функциональные испытания и проверка аварийных сценариев

Мониторинг промышленной АСУ должен охватывать сетевые соединения, события операционных систем, действия пользователей, изменения конфигураций, загрузку программ в контроллеры и срабатывание защитных средств. На начальном этапе целесообразно использовать пассивный анализ трафика, поскольку он не создаёт дополнительную нагрузку на устройства. Нормальная модель обмена в промышленной сети обычно стабильна, поэтому появление нового узла, неизвестного протокола или нетипичного направления связи является значимым признаком.

Журналы необходимо собирать на промежуточный сервер в технологической среде и затем передавать в систему централизованного анализа. При потере связи с корпоративным SOC локальное накопление должно продолжаться. Важна синхронизация времени, поскольку без неё

невозможно восстановить последовательность команд, сетевых соединений и технологических отклонений.

Управление уязвимостями в АСУ ТП следует строить как процесс оценки применимости, а не как автоматическую установку всех обновлений. Для каждого исправления проверяются модель устройства, версия, зависимые приложения, возможность отката, необходимость остановки и влияние на сертифицированные функции. Обновление сначала испытывается на стенде или резервном компоненте. Если немедленная установка невозможна, применяются сегментация, запрет уязвимого сервиса, ограничение маршрутов, усиленный мониторинг и контроль доступа.

Резервное копирование должно включать не только базы данных, но и проекты ПЛК, конфигурации SCADA, сетевых устройств, рецептуры, лицензии, сертификаты и инструкции восстановления. Копия считается пригодной только после проверки восстановления. Для критической системы полезно хранить автономную копию, недоступную для обычной учётной записи администратора.

План реагирования на инцидент должен учитывать, что немедленное отключение заражённого узла не всегда безопасно. Решение принимается совместно специалистами по информационной безопасности и технологами. Возможны перевод установки в локальный режим, останов по утверждённой последовательности, изоляция отдельного сегмента, блокирование удалённого доступа или сохранение ограниченной работы до достижения безопасной точки процесса.

После локализации необходимо собрать журналы и образы, проверить целостность проектов контроллеров, сравнить конфигурации с эталонными версиями и определить, были ли изменены уставки или блокировки. Восстановление должно выполняться из доверенного источника с последующим функциональным испытанием. Завершением инцидента является не только возврат к работе, но и устранение маршрута проникновения, обновление модели угроз и корректировка регламентов.

Кибербезопасность промышленной автоматизированной системы управления должна обеспечивать не только сохранность информации, но прежде всего целостность управляющих воздействий, доступность критических функций и безопасное состояние технологического объекта. Особенности АСУ ТП — длительный жизненный цикл, требования реального времени, ограниченные окна обслуживания и непосредственная связь с физическим процессом — требуют специализированных методов защиты.

Основой предлагаемой архитектуры являются разделение корпоративной и технологической сред, промышленная DMZ, зонирование внутри АСУ, контролируемый удалённый доступ, ограничение привилегий, контроль проектов ПЛК, резервное копирование и пассивный мониторинг. Критические защитные функции должны сохранять независимость от обычного контура управления и верхнего уровня диспетчеризации.

Разработанный индекс приоритета риска позволяет сопоставлять сценарии по вероятности, тяжести последствий и экспозиции. В иллюстративном расчёте наивысший приоритет получила компрометация удалённого доступа, а высокие значения также были характерны для кражи инженерных учётных данных и несанкционированного изменения логики ПЛК. Метод рекомендуется использовать как инструмент планирования с обязательным экспертным обсуждением и повторной оценкой после внедрения мер.

Практическая эффективность кибербезопасности определяется готовностью предприятия обнаружить отклонение, безопасно локализовать инцидент и восстановить доверенную конфигурацию. Поэтому технические средства должны дополняться регламентом изменений, обучением, совместными учениями и проверкой восстановления. Такой подход снижает вероятность того, что локальный информационный инцидент перерастёт в нарушение технологического процесса.

Использованные источники:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: https://publication.pravo.gov.ru/document/view/0001201707260023 (дата обращения: 05.08.2026).

2. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения: 05.08.2026).

3. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 05.08.2026).

4. ГОСТ Р МЭК 62443-2-1-2015. Сети коммуникационные промышленные. Защищённость (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищённости (кибербезопасности) системы управления и промышленной автоматики [Электронный ресурс]. URL: https://protect.gost.ru/gost/details/a4848270-3b1a-42bb-8deb-5a045a9a4d09 (дата обращения: 05.08.2026).

5. ГОСТ Р МЭК 62443-3-3-2016. Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности [Электронный ресурс]. URL: https://protect.gost.ru/gost/details/13affc54-24ab-4783-af69-7797b406f709 (дата обращения: 05.08.2026).