ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.89

DOI: 10.21822/2073-6185-2025-52-1-39-48 Оригинальная статья/ Original article

Обеспечение информационной безопасности в производственной сети промышленного предприятия

А.Р. Айдинян, Д.Г. Кирсанов
Донской государственный технический университет,
344003, г. Ростов-на-Дону, пл. Гагарина, 1, Россия

Резюме. Цель. Цель исследования состоит в разработке подходов для повышения информационной безопасности в производственной сети управления технологическим процессом промышленного предприятия до необходимого уровня. Привычные, и некогда эффективные методы защиты, основанные на физической изоляции, устарели и требуются новые подходы, учитывающие особенности автоматизированных систем управления технологическим процессом. **Метод**. Используемые в ходе исследования методы анализа выявляют различия между автоматизированными системами управления технологическим процессом и классическими информационными системами, основываясь на стандарте NIST SP 800-82, и оценивают их уникальные требования и уязвимости. Применены методы повышения информационной безопасности, включая регулярные тренинги, аудит, сегментацию сети и использование специализированных систем защиты. **Результат**. Разработан алгоритм действий для защиты системы АСУ ТП, обеспечивающий предприятиям соответствие требованиям регуляторов и минимизацию рисков кибератак, а также защиту критически важных производственных процессов. Предложен комплекс профилактических мер и методов устранения уязвимостей в системах АСУ ТП для защиты промышленных сетей. **Вывод**. Обеспечение информационной безопасности в АСУ ТП требует всестороннего подхода, включающего стратегии управления рисками, технические средства и постоянное повышение квалификации персонала. Внедрение предложенных мер и стратегий повысит общую устойчивость промышленных систем к современным угрозам информационной безопасности.

Ключевые слова: информационная безопасность, угроза информационной безопасности, промышленная безопасность, безопасность АСУ ТП

Для цитирования: А.Р. Айдинян, Д.Г. Кирсанов. Обеспечение информационной безопасности в производственной сети промышленного предприятия. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(1):39-48. DOI:10.21822/2073-6185-2025-52-1-39-48

Ensuring information security in the production network of an industrial enterprise

A.R. Aydynan, D.G. Kirsanov
Don State Technical University,
1 Gagarin Square, Rostov-on-Don 344003, Russia

Abstract. Objective. The purpose of this article is to explore issues and develop approaches to enhance information security in the production control networks of industrial enterprises to the necessary level. Traditional and once-effective protective methods based on physical isolation have become outdated, necessitating new approaches that consider the characteristics of automated process control systems. **Method.** The analysis presented in the article identifies differences between automated process control systems and classical information systems, based on the NIST SP 800-82 standard, and evaluates their unique requirements and vulnerabilities. Methods for improving information security are proposed, including regular training, audits, network segmentation, and the use of specialized protection systems. **Result.** An action algo-

rithm has been developed to protect the APCS system, ensuring that enterprises comply with regulatory requirements and minimize the risks of cyber attacks, as well as protect critical production processes. A set of preventive measures and methods for eliminating vulnerabilities in APCS systems to protect industrial networks is proposed. **Conclusion.** Ensuring information security in APCS requires a comprehensive approach, including risk management strategies, technical means and continuous personnel training. The implementation of the proposed measures and strategies will increase the overall resilience of industrial systems to modern information security threats.

Keywords: training program, competencies, distance learning, requirements, information security, specialty, protection measures, risks, residual risks

For citation: A.R. Aydynan, D.G. Kirsanov. Ensuring information security in the production network of an industrial enterprise. Herald of Daghestan State Technical University. Technical Sciences. 2025;52(1):39-48. (In Russ.) DOI:10.21822/2073-6185-2025-52-1-39-48

Введение. В современных организациях используется широкий спектр ИТ-систем, поэтому обеспечение требуемого уровня информационной безопасности становится особенно важным. Промышленные предприятия стали все более цифровизированными и широко внедряют передовые технологии, такие как Интернет вещей (IoT), машинное обучение и искусственный интеллект. Благодаря данным нововведениям, компании сумели оптимизировать свои производственные процессы и значительно повысить эффективность управления цепочками поставок. Тем не менее, ценой этих преимуществ является более высокая уязвимость к кибератакам. Ранее автоматизированные системы управления технологическим процессом (АСУ ТП) были хорошо защищены благодаря физической изоляции от внешних сетей, использованию в качестве управляющих воздействий аналоговых сигналов и отчасти релейного управления, что обеспечивало высокую степень безопасности. Тем не менее, в современных условиях такой подход уже утратил свою эффективность. Многие предприятия перешли к цифровому формату устройств на всех уровнях системы АСУ, что сделало традиционную модель безопасности, основанную на физической изоляции, устаревшей. Поскольку компании все больше связывают IT системы с внешними сетями и облачными сервисами, это приводит к значительному расширению сетевого периметра. Это открывает новые возможности для атак со стороны потенциальных злоумышленников. Для того чтобы обеспечить безопасность в этой новой цифровой среде, необходимо пересмотреть подход к защите промышленных сетей и разработать стратегии, которые учитывали бы актуальные угрозы информационной безопасности.

Постановка задачи. Целью данной статьи является исследование вопросов обеспечения информационной безопасности в АСУ ТП в условиях современной цифровизации промышленных предприятий. В статье рассматриваются ключевые отличия АСУ ТП от обычных информационных систем, анализируются специфические угрозы и уязвимости, а также предлагаются методы и стратегии по защите данных в этих системах. Особое внимание уделяется сравнительному анализу ИТ-систем и АСУ ТП согласно стандарту NIST SP 800-82, а также профилактическим мерам и законодательным аспектам обеспечения безопасности.

Методы исследования. С ростом цифровизации промышленных предприятий и использованием передовых технологий, таких как машинное обучение, интернет вещей (IoT) и искусственный интеллект, произошла революция в сфере автоматизации и управления производством. Эти инновации позволили компаниям оптимизировать производственные процессы, сделать управление цепочками поставок более эффективным и повысить эффективность обслуживания клиентов. Но так же, вместе с этими преимуществами приходит и увеличенная уязвимость к кибератакам.

Ранее, АСУ ТП обладали высокой степенью защиты благодаря своей физической изоляции от внешних сетей. Однако, в современном мире такой подход уже не является

достаточно эффективным. Переход многих предприятий к цифровому формату привел к тому, что традиционная модель безопасности, основанная на физической изоляции, оказалась устаревшей. Вместе с тем, как компании становятся все более связанными с внешними сетями и облачными сервисами, сетевой периметр значительно расширяется, предоставляя потенциальным злоумышленникам больше возможностей для атак.

Таким образом, хотя цифровые технологии приносят значительные выгоды для промышленных предприятий, необходимо признать, что они также увеличивают уровень угрозы кибератак. Для обеспечения безопасности в этом новом цифровом ландшафте требуется пересмотреть подход к защите промышленных сетей и разработать стратегии, учитывающие современные вызовы и угрозы информационной безопасности.

Отличие АСУ ТП от классических информационных систем заключается в их специфике и функциональности, а также в особенностях их архитектуры и взаимодействия с другими устройствами в промышленной среде.

Для информационной связи всех подсистем АСУ ТП используются промышленные протоколы (Modbus, Profinet, EtherCAT) которые в большинстве случаев не выделены в отдельный сегмент сети предприятия. Это отличает их от информационных систем, где используются общие сети связи, такие как Интернет или локальные сети офисного типа. Промышленные сети специально разработаны для обеспечения надежной и безопасной передачи данных в условиях промышленного производства.

Кроме того, в промышленной автоматизации сетевые интерфейсы могут быть неотъемлемой частью соединяемых устройств (ПЛК, исполнительные механизмы, датчики), что делает физическое отделение сетевой части от устройств практически невозможным. Это отличается от других информационных систем, где сетевые интерфейсы чаще всего являются отдельными компонентами и могут быть легко отделены от основных устройств.

Так же, сетевое программное обеспечение прикладного уровня модели OSI исполняется на основном процессоре ПЛК, что дополнительно подчеркивает уязвимость специфики АСУ ТП. Это означает, что управление и контроль сети интегрированы непосредственно в устройства, работающие в составе системы управления технологическим процессом.

Таким образом, отличие АСУ ТП от классических информационных систем заключается не только в их специализированных функциях и задачах, но и в особенностях их архитектуры, взаимодействия с другими устройствами и принципах построения сетей связи. Сравнительный анализ информационных систем и АСУ ТП из стандарта NIST SP 800-82 необходим для выявления особенностей и различий в обеспечении информационной безопасности между обычными информационными системами и системами управления технологическим процессом.

Такой анализ позволяет определить уникальные угрозы и уязвимости, а также разработать соответствующие стратегии и меры по защите информации в контексте промышленной автоматизации.

Исходя из анализа представленных характеристик информационных систем и АСУ ТП в табл. 1, можно сделать вывод о значительных различиях между ними.

Важно отметить, что данные различия делают системы менеджмента информационной безопасности (ИБ) неподходящими для систем управления технологическими процессами (АСУ ТП). Одним из ключевых отличий является характер требований к функционированию.

В то время как IT-системы, как правило, не являются системами реального времени и имеют различные приоритеты в экстренных ситуациях, АСУ ТП должны выполнять критически важные функции в режиме реального времени, где даже небольшая задержка или потеря данных могут быть недопустимыми.

Таблица 1. Сравнительный анализ информационных систем и АСУ ТП из стандарта NIST SP800-82
Table 1. Comparative analysis of information systems and automated process control systems from the NIST SP800-82 standard

Сравниваемые характеристики Comparable characteristics	**IT система IT system**	**АСУ ТП Automated process control system**
Требования к функционированию Requirements for operation	Не является системой реального времени. Время реакции не всегда критично. Требуется высокая пропускная способность. Задержка и потеря данных могут быть приемлемыми. Менее критичные функции в аварийных ситуациях. Управление доступом определяется требованиями к ИБ.	Является системой реального времени. Время реакции критично. Не требуется высокая пропускная способность. Задержка и потеря данных не приемлемы. Критична реакция в аварийных ситуациях. Управление доступом должно осуществляться, но не препятствовать функциям управления посредством человеко-машинного интерфейса.
Требования к надежности и готовности. Requirements for reliability and availability	Перезагрузка является приемлемой. Дефициты готовности иногда могут быть приемлемыми, в зависимости от эксплуатационных требований.	Перезагрузка может быть неприемлема из-за требований к готовности. Требования к готовности, как правило, требуют внедрения резервирования. Планово-предупредительные работы планируются заранее. Высокая готовность требует всестороннего предварительного тестирования.
Требования к управлению рисками Risk Management Requirements	Управления рисками относится, в первую очередь, к управлению данными. Первостепенное значение имеет конфиденциальность и целостность данных. Отказоустойчивость менее важна, поскольку кратковременный простой не является основным риском. Основным риском является задержка бизнес-операций.	Управление рисками относится, в первую очередь, к управлению физическими процессами. Первостепенное значение имеет безопасность людей, вытекающая из безопасности физических процессов. Отказоустойчивость имеет важное значение, даже кратковременный простой может быть неприемлемым. Основным риском являются несоответствия регулирующим требованиям, воздействие на окружающую среду, жизнь и здоровье людей, оборудование и производство.
Операционные системы Operating systems	Используются различные типы коммерчески доступных операционных систем. Обновления для операционных систем могут устанавливаться автоматически.	Наряду с широко распространенными операционными системами, используются специализированные операционные системы, в том числе, без встроенных функций ИБ. Изменения ПО тщательно контролируются и выполняются, как правило, поставщиками ПО, из-за специализированных алгоритмов управления и влияния на конфигурацию аппаратных средств, а так же из-за значительных затрат на лицензирование изменений.
Ограничения системных ресурсов System resource limitations	Системы имеют достаточно вычислительных ресурсов для добавления дополнительных приложений, связанных с обеспечением ИБ.	Системы разработаны для поддержки промышленных процессов и могут не иметь достаточно памяти или вычислительных ресурсов для поддержки функций безопасности.
Коммуникации Communications	Применяются стандартные коммуникационные протоколы. Применяются в основном уже существующие сети. Применяются типовые сетевые решения.	Применяются специально разработанные (проприетарные) коммуникационные протоколы. Часто прокладываются специальные сети. Сети базируются на различных типах медиа и могут требовать экспертных инженерных знаний.
Управления изменениями Change Management	Изменения ПО выполняются периодически под управлением процедур безопасности. Процедуры изменений ПО зачастую автоматизируются.	Изменения ПО должны быть протестированы, и должно быть подтверждено сохранение целостности системы после внесения изменений. Остановки в работе системы должны быть спланированы заранее. АСУ ТП может использовать не поддерживаемое более ПО.
Поддержка эксплуатации Support operating	Может быть реализована различными поставщиками.	Как правило, реализуется единственным поставщиком.
Продолжительность эксплуатации Duration of operation	Типовая продолжительность жизненного цикла: 3-5 лет	Типовая продолжительность жизненного цикла: 10-15 лет, а для некоторых. Объектов может доходить до 30 лет.
Физическое расположение компонентов. Physical arrangement of components.	Компоненты обычно локализованы и к ним можно получить физический доступ.	Компоненты могут быть изолированными, удаленными и с физически сложным доступом.

Также следует обратить внимание на различия в требованиях к надежности и доступности. В IT системах перезагрузка может быть приемлемой, тогда как в АСУ ТП такие ситуации могут быть недопустимыми из-за критической важности времени реакции и требований к непрерывной работе. Другим важным аспектом является управление рисками. Для IT-систем первостепенное значение имеет конфиденциальность и целостность данных, то в АСУ ТП основной акцент делается на безопасности физических процессов и обеспечении отказоустойчивости, что делает подходы к управлению рисками в этих двух типах систем существенно различными.

Таким образом, на основе представленного сравнения можно заключить, что применение методов и стандартов информационной безопасности, разработанных для IT систем, к системам управления технологическим процессом является неприменимым и может представлять серьезные риски для безопасности и надежности производственных процессов. В обычной IT системе необходимо уделять особое внимание безопасности на промышленных предприятиях. Использование межсетевых экранов, антивирусного программного обеспечения, DLP-систем и защиты от спама в сочетании с проактивным мониторингом, а также управлением сетевым оборудованием, программным обеспечением и трафиком может значительно уменьшить риск атак. Тем не менее, технические решения в области информационной безопасности не способны полностью устранить все угрозы для систем промышленного предприятия.

В контексте информационной безопасности промышленных предприятий, важно учитывать, что технические средства, такие как межсетевые экраны, антивирусное ПО, DLP-системы и защита от спама, при поддержке проактивного мониторинга и управления сетевым оборудованием, могут существенно снизить риск кибератаки. Однако, не следует рассматривать их как панацею от всех угроз для систем промышленного предприятия. Важно понимать, что угрозы могут исходить не только от злоумышленников, но и от непреднамеренных действий персонала, отказов оборудования или воздействия окружающей среды.

Основные задачи информационной безопасности в промышленности включают:

1)Защиту технологических процессов, включая автоматизированные системы управления технологическим процессом (АСУ ТП);

2) Обеспечение безопасности корпоративных ресурсов, таких как информационная инфраструктура и веб-ресурсы;

3) Защиту конечных устройств от угроз;

4) Защиту чувствительной информации и персональных данных;

5) Соблюдение требований регуляторов в области безопасности;

6) Предотвращение утечек информации;

7) Выявление внутренних нарушений и недобросовестных действий сотрудников.

Таким образом, для обеспечения информационной безопасности промышленных предприятий предлагаем реализовать комплексный подход, включающий как технические средства, так и стратегии управления персоналом и рисками.

Цели взлома АСУ ТП могут быть разнообразными и включают:

1. Кражу коммерческой тайны и интеллектуальной собственности для получения конфиденциальной информации о технологиях производства, патентах, проектах и других коммерчески значимых данных, которые могут быть использованы для незаконного обогащения или конкурентных преимуществ.
2. Промышленный саботаж для нарушение нормального функционирования промышленного процесса, что может привести к простоям, ущербу оборудованию, потере продукции и финансовым убыткам для предприятия.
3. Вымогательство прерыванием производственных процессов или утечкой конфиденциальной информации для получения выкупа.

4. Повреждение информационных систем предприятия для нанесения ущерба информационным системам предприятия путем потери данных, нарушения работы производственных процессов и финансовым потерям.

Примером может служить ситуация, когда хакеры взламывают систему управления производством на заводе с целью изменить параметры производственного процесса так, чтобы продукция вышла с дефектами или была несоответствующего качества. Это может привести к значительным убыткам для предприятия и потере репутации на рынке.

На представленном рис. 1 показана статистика с указанием процентов компьютеров, на которых были блокированы угрозы продуктами «Лаборатории Касперского». Видно, что вредоносные объекты, которые блокируются на компьютерах АСУ ТП, относятся ко многим категориям.

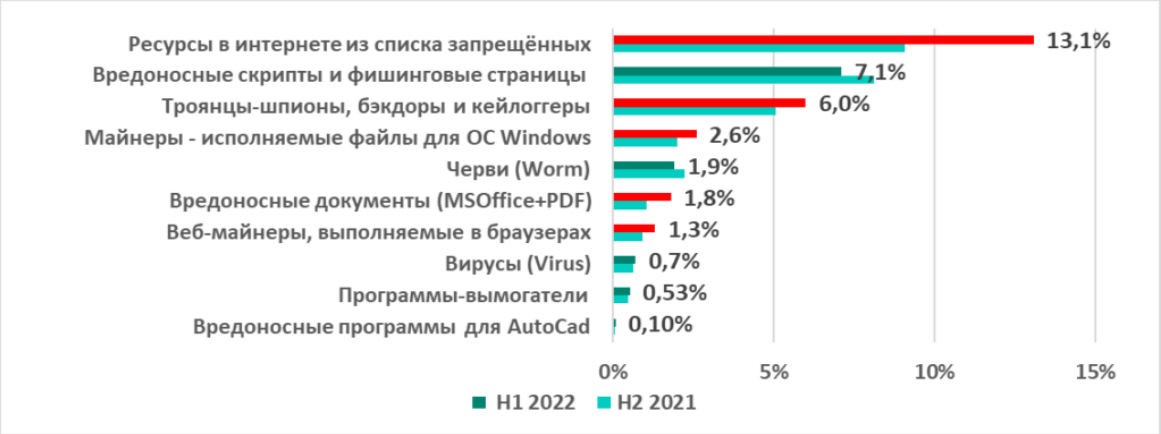

Рис. 1- Процент компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий, первое полугодие 2022 и второе полугодие 2021
Fig. 1- Percentage of ICS computers on which the activity of malicious objects of various categories was prevented, first half of 2022 and second half of 2021

Обсуждение результатов. Профилактические меры и методы устранения уязвимостей в системах АСУ ТП включают в себя следующее:

1. Проведение регулярных тренингов по информационной безопасности для повышения осведомленности сотрудников;
2. Аудит информационной безопасности и сканирование сети для выявления и предотвращения эксплуатации уязвимостей, а также своевременного внедрения обновлений (патчей);
3. Корректная сегментация сети для улучшения контроля за трафиком и повышения эффективности систем безопасности;
4. Использование специализированных систем защиты АСУ ТП для обеспечения непрерывности производственных процессов;
5. Применение технологии NTA (Network Traffic Analysis) для обнаружения аномалий в сетевом трафике и выявления кибератак на ранних этапах;
6. Реализация межсетевых экранов и систем обнаружения и предотвращения вторжений (IDS/IPS) для защиты периметра сети и обнаружения вредоносного трафика;
7. Внедрение WAF (Web Application Firewall) для защиты веб-ресурсов от различных атак, таких как XSS, SQL-инъекции и CSRF;
8. Защита конечных точек для снижения риска заражения вирусами и обеспечения соответствия политикам безопасности;
9. Обеспечение безопасного удаленного доступа к сети с помощью VPN и криптографической защиты информации (СКЗИ);
10. Внедрение DLP систем для предотвращения утечек конфиденциальной информации;
11. Использование систем управления доступом для контроля за учетными записями и правами доступа;

12. Внедрение решений для управления сетевым доступом (NAC) для обеспечения видимости и контроля за подключениями к сети;
13. Применение систем классификации данных для повышения безопасности конфиденциальной информации и ее управления;
14. Использование интерактивных ловушек для обнаружения APT-атак;
15. Внедрение SIEM систем для централизованного мониторинга безопасности и анализа данных от различных инструментов безопасности.

В стране активно занимаются разработкой нормативных актов, чтобы регулировать вопросы, связанные с обеспечением безопасности промышленных систем автоматизации. Один из ключевых результатов этой работы - приказ ФСТЭК РФ № 31, который начал действовать в 2014 году.

Однако до сих пор отсутствуют методические руководства, которые разъяснили бы меры по защите информации, выявлению и устранению уязвимостей, а также реагированию на инциденты, связанные с нарушением защиты информации в системах автоматизации на производстве, указанные в приказе № 31. Из-за этого возник переходный период: в настоящее время. при обеспечении безопасности систем автоматизации на производстве согласно требованиям приказа № 31 возникает необходимость в принятии решений по неустановленным вопросам. Например, можно опираться на методические документы ФСТЭК, касающиеся ключевых систем информационной инфраструктуры (КСИИ) и других типов систем. Однако приказ № 31 имеет ряд особенностей по сравнению с ранее выпущенными документами ФСТЭК, обусловленных спецификой промышленных систем автоматизации.

Первая особенность – уникальные требования к безопасной разработке программного обеспечения (ОБР).

Другая особенность заключается в распределении обязанностей участников процесса защиты АСУ ТП (заказчик/оператор/разработчик) при определении уровня защищенности, от которого зависит набор мер защиты информации в АСУ ТП, а также используемые средства защиты информации.

Третья особенность - использование средств защиты информации, которые выбираются в соответствии с требованиями заказчика, в соответствии с Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Еще один важный аспект, вызывающий дискуссии в профессиональном сообществе, – определение структурного подразделения или должностного лица (работника), ответственного за защиту информации в системах автоматизации на производстве в соответствии с приказом № 31.

Алгоритм действий для защиты системы АСУ ТП. В первую очередь, для построения системы защиты АСУ ТП необходимо понять, является ли система субъектом КИИ. Критическая информационная инфраструктура (сокращенно - КИИ) - это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия. В свою очередь, субъекты КИИ - это компании, работающие в стратегически важных для государства областях, таких как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также организации, обеспечивающие взаимодействие систем или сетей КИИ. Чтобы определить, относится ли система к субъектам критической информационной инфраструктуры (КИИ), необходимо реализовать ряд шагов в рамках Постановления Правительства РФ № 127 от 02.02.2018 «О категорировании объектов критической информационной инфраструктуры Российской Федерации».

Согласно 187-ФЗ от 26.07.2017 и ПП РФ № 127 от 02.02.2018 необходимо установить, относится ли система к перечню сфер деятельности организации. Так же отношение

к субъекту КИИ можно проверить по кодам ОКВЭД и лицензиям на осуществление деятельности организации. Далее, если по результатам анализа мы приходим к решению, что система не является КИИ, то он всё равно требует защиты в соответствии с общими требованиями к информационной безопасности систем АСУ ТП. Действительно, по результатам оценки можно прийти к выводу, что не будет объектов КИИ, подлежащих категорированию – в этом случае нет необходимости направлять сведения в регуляторные органы. Если же мы приходим к выводу что наша система является КИИ, необходимо совершить ряд действий :

Категорирование объектов КИИ:

1. Определяем принадлежность организации к субъектам КИИ в соответствии с 187-ФЗ
2. Определяем процессы организации и составляем их перечень (управленческие, технологические, финансово-экономические, производственные).
3. Выявляем критичные объекты и процессы, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов и (или) осуществляют управление, контроль или мониторинг критических процессов.
4. Проводим анализ возможных последствий реализации угроз безопасности информации для объектов КИИ.
5. Присваиваем объекту одну из категорий значимости: первая (высшая), вторая или третья.

Регистрация объектов КИИ:

Готовим Акт категорирования объектов КИИ для отправки во ФСТЭК.

Разработка и реализация мер защиты:

1. Разрабатываем локальные нормативные акты и политики информационной безопасности.
2. Реализуем организационные меры защиты (назначение ответственных лиц, проведение инструктажей и обучения персонала).
3. Внедряем технические средства защиты информации (системы контроля доступа, межсетевые экраны, системы обнаружения вторжений и т.д.).
4. Обеспечиваем криптографическую защиту информации в соответствии с требованиями законодательства.

Проведение оценки соответствия:

1. Проводим регулярные проверки и оцениваем соответствие системы защиты информации требованиям законодательства и нормативных документов.
2. Проводим аудит и тесты на проникновение для выявления уязвимостей.

Мониторинг и реагирование на инциденты:

1. Организуем системы мониторинга и реагирования на инциденты информационной безопасности.
2. Создаем и поддерживаем в актуальном состоянии план реагирования на инциденты.
3. Взаимодействуем с уполномоченными органами (ФСТЭК, ФСБ, ГосСОПКА) в случае выявления инцидентов.

Обеспечение непрерывности и восстановление деятельности:

1. Разрабатываем и внедряем план обеспечения непрерывности деятельности АСУ ТП.
2. Реализуем мероприятия по восстановлению системы АСУ ТП в случае инцидента.

Проведение регулярных обучений и тренингов:

1. Обучаем сотрудников правилам и методам защиты информации.
2. Проводим регулярные тренировки по реагированию на инциденты и восстановлению системы.

Эти действия должны быть интегрированы в общую стратегию управления рисками и информационной безопасностью предприятия, обеспечивая тем самым надежную защиту критической информационной инфраструктуры.

Вывод. Результаты исследования подтверждают важность комплексного подхода к обеспечению информационной безопасности в АСУ ТП, учитывающего как технические, так и организационные аспекты.

Разработанный алгоритм действий поможет предприятиям соответствовать требованиям регуляторов и минимизировать риски кибератак и обеспечить защиту критически важных производственных процессов.

Внедрение предложенных мер и стратегий повысит общую устойчивость промышленных систем к современным угрозам информационной безопасности. Новым знанием, полученным в результате данного исследования, является выявление критических различий между ИТ-системами и АСУ ТП, что позволяет более точно разрабатывать стратегии и методы защиты для промышленных систем.

Кроме того, были предложены конкретные профилактические меры и методики устранения уязвимостей, адаптированные к особенностям АСУ ТП. Также важным результатом является разработка алгоритма действий для категорирования и защиты систем АСУ ТП. Становится очевидным, что обеспечение информационной безопасности в промышленных системах автоматизации является крайне важным аспектом современной промышленности. Развитие цифровых технологий и интернета вещей (IoT) влечет за собой не только новые возможности, но и новые угрозы, связанные с кибератаками и нарушениями информационной безопасности. Стандарты и нормативные документы, такие как приказ ФСТЭК России № 31, 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации играют важную роль в обеспечении безопасности систем автоматизации, однако их применение требует дополнительных методологий и практических решений для решения конкретных проблем безопасности.

Также важно отметить, что уникальные характеристики и требования промышленных систем автоматизации делают их особенно уязвимыми перед новыми угрозами, и необходимо продолжать развивать и совершенствовать методы защиты, а также повышать квалификацию персонала, работающего с этими системами.

Библиографический список:

1. Промышленная безопасность [Электронный ресурс] – Режим доступа: https://www.evraas.ru/industries/manufacturing/. – Загл. с экрана.
2. Угрозы информационной безопасности систем промышленной автоматизации в России [Электронный ресурс] – Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2022/09/20/threat-landscape-for-industrial-automation-systems-in-russia/. – Загл. с экрана.
3. Архитектура и безопасность систем управления промышленными предприятиями [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/316184/. – Загл. с экрана.
4. NIST SP 800-82: Руководство по безопасности систем промышленной автоматизации и управления [Электронный ресурс] – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. – Загл. с экрана.
5. Категорирование объектов критической информационной инфраструктуры (КИИ). Практические примеры [Электронный ресурс] – Режим доступа: https://rtmtech.ru/articles/kategorirovanie-obektov-kii-primery/
6. КИИ - что это? Безопасность объектов критической информационной инфраструктуры [Электронный ресурс] – Режим доступа: https://www.securityvision.ru/blog/kii-chto-eto/
7. Федеральный Закон «О безопасности КИИ РФ» от 26.07.2017;
8. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ
9. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ
10. Гордиенко В.В., Лисицин А.Л. Технические и организационные методы борьбы с внутренними угрозами утечки информации организаций и предприятий // Auditorium. 2019. № 4 (24). [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/tehnicheskie-i-organizatsionnye-metody-borby-svnutrennimi-ugrozami-utechki-informatsii-organizatsiy-i-predpriyatiy

11. Андреев Ю.С., Дергачев А.М., Жаров Ф.А., Садырин Д.С. Информационная безопасность автоматизированных систем управления технологическими процессами. Текст научной статьи по специальности «Компьютерные и информационные науки», университет ИТМО, 2019

References:

1. Industrial safety [Electronic resource] – Access mode: https://www.evraas.ru/industries/manufacturing/. – Title from the screen. (In Russ)
2. Threats to information security of industrial automation systems in Russia [Electronic resource] – Access mode:https://ics-cert.kaspersky.ru/publications/reports/2022/09/20/threat-landscape-for-industrial-automation-systems-in-russia/. – Title from the screen. (In Russ)
3. Architecture and security of industrial enterprise control systems [Electronic resource] – Access mode: https://habr.com/ru/post/316184/. – Title from the screen. (In Russ)
4. NIST SP 800-82: Guide to Industrial Automation and Control Systems Security [Electronic resource] - Access mode: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. - Title from the screen. (In Russ)
5. Categorization of critical information infrastructure (CII) objects. Practical examples [Electronic resource] - Access mode: https://rtmtech.ru/articles/kategorirovanie-obektov-kii-primery/(In Russ)
6. CII - what is it? Security of critical information infrastructure objects [Electronic resource] - Access mode: https://www.securityvision.ru/blog/kii-chto-eto/(In Russ)
7. Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017; (In Russ)
8. Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 N 187-FZ (In Russ)
9. Federal Law "On Information, Information Technologies and Information Protection" dated July 27, 2006 N 149-FZ (In Russ)
10. Gordienko V.V., Lisitsyn A.L. Technical and organizational methods for combating internal threats of information leakage of organizations and enterprises. *Auditorium*. 2019;4 (24). [Electronic resource] – Access modehttps://cyberleninka.ru/article/n/tehnicheskie-i-organizatsionnye-metody-borby-svnutrennimi-ugrozami-utechki-informatsii-organizatsiy-i-predpriyatiy (In Russ)
11. Andreev Yu.S., Dergachev A.M., Zharov F.A., Sadyrin D.S. Information security of automated process control systems. Text of scientific article on the specialty "Computer and Information Sciences", ITMO University, 2019 (In Russ)

Сведения об авторах:

Айдинян Андрей Размикович, кандидат технических наук, доцент, доцент кафедры «Вычислительные системы и информационная безопасность»; andstyle@mail.ru; ORCID 0000-0001-9455-4079

Кирсанов Дмитрий Георгиевич, студент, кафедра «Вычислительные системы и информационная безопасность»; dmitriy5688@yandex.ru

Information about authors:

Andrey R. Aydinyan, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department of Computing Systems and Information Security; andstyle@mail.ru; ORCID 0000-0001-9455-4079

Dmitry G. Kirsanov, Student, Department of Computing Systems and Information Security; dmitriy5688@yandex

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 29.09.2024.

Одобрена после рецензирования/ Reviced 06.11.2024.

Принята в печать/Accepted for publication 20.01.2025.