БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 1 (112). – 9–22

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-1-9-22

ОБЗОР ОСНОВНЫХ КОМПОНЕНТОВ, ОСОБЕННОСТЕЙ И РЕШЕНИЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ*

Е.И. БЫЧКОВА[1], М.В. ЛЫСЕНКО[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: e.bychkova.2018@stud.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: m.v.lysenko@corp.nstu.ru*

Описана структура, основные компоненты и задачи типовых автоматизированных систем управления технологическими процессами (АСУ ТП). Определены основные отличительные особенности автоматизированных систем и их влияние на проектирование системы обеспечения информационной безопасности (СОИБ). Дан краткий обзор проблем информационной безопасности автоматизированных систем управления технологическими процессами. Приведены основные принципы, которые необходимо учитывать при создании СОИБ.

Ключевые слова: автоматизированные системы управления технологическими процессами, автоматизированные системы управления, автоматизация, технологические системы, система защиты, защита информации, информационная система, системы обеспечения информационной безопасности

ВВЕДЕНИЕ

Автоматизированные системы управления технологическими процессами (АСУ ТП) играют большую роль в организации сложных процессов с высокой точностью и эффективностью. Для эффективной защиты таких систем необходимо понимать структуру и основные компоненты, а также их роль в обеспечении операционной эффективности.

* Статья получена 10 февраля 2024 г.

Сегодня АСУ ТП применяют в разных сферах, таких как энергетика, медицина, телекоммуникации, сфера ЖКХ, производство и многие другие. Информационная безопасность АСУ ТП имеет решающее значение для корректной работы системы, поскольку уязвимости могут быть использованы для физической атаки людей, окружающей среды (техногенные риски) и материальных активов и влекут за собой операционные, финансовые, репутационные и нормативные последствия. Своевременные и эффективные меры реагирования имеют решающее значение для смягчения этих последствий.

Типичная АСУ ТП представляет собой совокупность аппаратного и программного обеспечения для управления и оптимизации производственных процессов. От датчиков, фиксирующих данные в режиме реального времени, до программируемых логических контроллеров, выполняющих сложные команды, каждый компонент играет ключевую роль в организации производственной деятельности. Понимание этой взаимосвязанной структуры имеет первостепенное значение для осознания проблем, возникающих при защите этих систем от потенциальных угроз, и позволяет проектировать надежные системы обеспечения информационной безопасности.

Автоматизированные системы отличаются важностью циркулирующих данных и критичностью времени отклика и реакции. Потеря или искажение данных влечет за собой остановку работы всей системы, поэтому разработка СОИБ требует полного понимания работы системы. Среди преимуществ, приносимых автоматизацией, обратная сторона вызывает множество опасений относительно безопасности и целостности критически важных данных. В статье представлен краткий обзор распространенных проблем, влияющих на информационную безопасность

Построение системы защиты – необходимый этап для корректной работы автоматизированной системы. Проектирование системы защиты необходимо начинать с определения объектов защиты, моделирования угроз и определения возможных рисков. Различные компоненты автоматизированной системы управления технологическими процессами могут быть уязвимы для различных типов атак. В статье приведены наиболее уязвимые для кибератак компоненты системы.

Многие компоненты системы чувствительны к внесению изменений в конфигурацию и могут привести к нарушению технологического процесса. В статье рассмотрены принципы проектирования СОИБ для систем автоматизации технологического процесса, учитывающие работу системы в реальном времени.

1. ОПИСАНИЕ СТРУКТУРЫ АСУ ТП

Автоматизированные системы управления технологическими процессами (далее – АСУ ТП) предназначены для повышения эффективности операций и процессов за счет их автоматизации, а также для повышения надежности и согласованности операций за счет осуществления мониторинга параметров технологического процесса в реальном времени; осуществляют автоматизированный контроль и управление технологическими процессами и сопутствующими локальными автоматическими подсистемами.

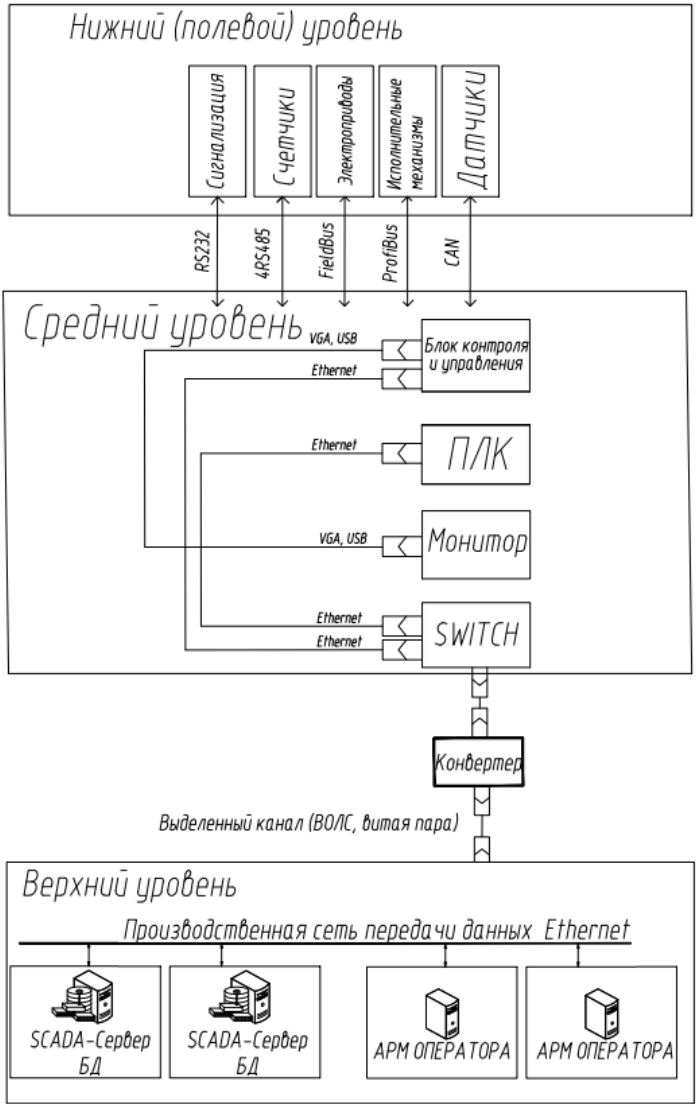
АСУ ТП выполняют широкий спектр задач, в зависимости от области применения и отрасли задачи могут варьироваться, однако можно выделить общие задачи автоматизации:

– автоматическое управление процессами объекта автоматизации, в том числе удаленно;
– мониторинг состояния работы объекта управления в реальном времени;
– сбор, обработка и анализ информации о состоянии объекта управления;
– выработка и передача управляющих воздействий на исполнение;
– контроль выполнения управляющих воздействий;
– обмен информацией с взаимосвязанными автоматизированными системами;
– генерация аварийных сигналов и оповещений о внештатных ситуациях;
– повышение безопасности и надежности функционирования объекта;
– создание отчетов о производительности системы и событиях;
– уменьшение влияния человеческого фактора на управляемый процесс.

В большинстве случаев АСУ ТП состоит из трех уровней, которые представляют собой единую систему управления технологическим процессом.

1. Нижний уровень (в разной литературе также можно встретить термин «полевой уровень») регулирует работу датчиков, осуществляет контроль различных счетчиков и исполнительных механизмов, а также передает данные от устройств по линиям связи на средний уровень (рисунок).

2. Средний уровень включает в себя программируемые логические контроллеры (ПЛК) и операторские панели, осуществляющие управление и мониторинг работы объекта. Обработка информации на этом уровне происходит по единому алгоритму: контроллеры и панели получают данные с нижнего уровня, производят их анализ и обработку, затем обработанные данные передают на верхний уровень для принятия решения по управлению объектом или процессом и выдачи команд на нижний уровень.



Уровни АСУ ТП

Automated control system levels

3. Верхний уровень основан на базе серверного оборудования (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, автоматизированных рабочих мест (АРМ) операторов, телекоммуникационного оборудования (маршрутизаторы, коммутаторы) и каналов связи, обеспечивающих сбор и хранение данных, архивацию информации, полученной от контроллеров, и представление ее в виде визуальных средств. Таким образом, оператор системы может ознакомиться с параметрами процесса, протекающего на объекте, и при необходимости отправить команды для корректировки работы того или иного процесса. Участие оператора в АСУ ТП сведено к минимуму, но всё же оно есть на уровне реализации и принятия наиболее ответственных решений.

Компоненты нижнего и среднего уровней связаны между собой проводными линиями связи в единую распределенную систему управления, работающую в режиме реального времени. Современной тенденцией является использование IP и Ethernet-сетей на верхнем и среднем уровнях. Доступ к датчикам осуществляется по протоколам и полевым шинам (RS485, RS232, Promwad, Modbus, HART, Profinet, Profibus, ISA, PCI, PCIe, VME, PXI, EtherCAT, CAN и др.).

Средний и верхний уровни обычно территориально изолированы друг от друга и осуществляют связь посредством организации выделенных каналов связи. При таком подключении передача данных осуществляется с помощью специального кабеля (оптоволокно или витая пара). Выделенный канал связи обозначает целенаправленно обособленный канал, зарезервированный исключительно для указанных сторон, тем самым обеспечивая безопасный, целенаправленный и конфиденциальный способ общения, изолированный от внешних сбоев или несанкционированного доступа.

2. ОСОБЕННОСТИ АСУ ТП

Автоматизированная система управления технологическими процессами (АСУ ТП) обладает определенными особенностями, которые способствуют ее функциональности и эффективности.

Как АСУ ТП, так и стандартные информационные системы корпоративного сегмента разделяют некоторые общие принципы информационной безопасности, однако меры и принципы защиты различаются в зависимости от требований и особенностей соответствующих областей.

В безопасности АСУ ТП уделяется большое внимание физической безопасности и надежности производственных процессов. При разработке системы защиты для таких систем упор делается на целостность и доступность ин-

формации, тогда как вопросу обеспечения конфиденциальности, как правило, уделяется меньше внимания. Это обусловлено тем, что нарушение целостности передаваемой информации может привести к принятию неверных решений и сбоям в работе объекта автоматизации или его остановке, что является критичным и даже неприемлемым для большинства объектов.

Также для циркулирующей в АСУ ТП информации не менее важна ее доступность. АСУ ТП является системой реального времени, в которой время реакции является критичным, а задержки и потеря данных – неприемлемыми. Контроль в режиме реального времени и принятие решений зависят от немедленного доступа к точным данным. Доступность гарантирует, что операторы могут своевременно реагировать на изменяющиеся условия, сводя к минимуму время реагирования в критических ситуациях и оптимизируя эффективность производственных процессов.

Также важной особенностью автоматизированных систем управления является продолжительность жизненного цикла, в среднем она составляет от 10 до 20 лет. В течение длительного жизненного цикла технологии развиваются, и компоненты, используемые при проектировании АСУ ТП, могут устаревать. Это может привести к проблемам с обновлениями программного обеспечения и проблемам совместимости с более новыми технологиями. Также за длительный срок эксплуатации производители программных и аппаратных компонентов системы могут прекратить поддержку устаревших версий, что затруднит получение технической поддержки и услуг по техническому обслуживанию, что повышает уязвимость системы в целом. Стоит отметить, что длительный жизненный цикл системы также влияет на эффективность и производительность АСУ ТП за счет ухудшения характеристик используемых компонентов [8].

Одной из особенностей АСУ ТП также является использование специализированных и специально разработанных протоколов. Использование таких протоколов позволяет осуществлять их настройку с учетом потребностей и функционирования конкретной системы, определять необходимые функции безопасности и оптимизировать процессы для повышения производительности. Нестандартные протоколы связи также являются более защищенными от кибератак, однако при использовании проприетарных стандартов связи следует тщательно учитывать потенциальные проблемы, связанные с совместимостью, зависимостью от поставщика и долгосрочной поддержкой.

В большинстве случаев компоненты АСУ ТП могут быть территориально удалены друг от друга (например, АРМ оператора и объект автоматизации). Исходя из этого также возникают такие проблемы, как задержка при передаче данных, которая может повлиять на скорость реагирования системы в режиме реального времени, влияя на ее способность оперативно управлять процес-

сами, а такие проблемы, как перебои в работе сети или ограничение пропускной способности, могут нарушить бесперебойный поток данных и управляющих сигналов, влияя на общую производительность системы. Во многих случаях удаленность внутренних объектов предприятия, необходимость их дополнительной интеграции с офисными системами и друг с другом затрудняют работу сетевых архитекторов, вынуждая их создавать такие сети, где множество сегментов построено на использовании внешних каналов связи, в том числе интернета.

Также исходя из того, что АСУ ТП является системой реального времени, перезагрузка системы может быть неприемлема. Таким образом, установка обновлений в большинстве случаев невозможна или затруднительна. Отсюда следует вывод, что АСУ ТП более подвержена уязвимостям, чем типовые информационные системы корпоративного сегмента, и требует подхода к защите с учетом всех компонентов и особенностей системы. Инциденты безопасности могут привести к нарушению технологических процессов и послужить причиной остановки всего промышленного комплекса в целом.

При построении системы обеспечения информационной безопасности (далее – СОИБ) АСУ ТП для защиты ресурсов АСУ ТП от актуальных угроз информационной безопасности возникают сложности при выборе средств защиты, способных обеспечить требуемый уровень защищенности, при этом не оказывающих влияние на работу компонентов системы. Также используемое в атаках на АСУ ТП вредоносное программное обеспечение (ВПО) и угрозы, как правило, узконаправленные, и база инцидентов классических антивирусов не всегда может быть актуальна для защиты АСУ ТП.

Основные проблемы информационной безопасности АСУ ТП, выделяемые экспертами [4, 5]:

– слабая парольная политика и недостаточная защита от несанкционированного доступа;

– функциональные возможности SCADA, не описанные в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;

– отсутствие контроля управляющих воздействий;

– использование беспроводных коммуникаций;

– отсутствие четких границ между сегментами сети;

– несвоевременное или некорректное обновление программного обеспечения (или отсутствие возможности установки обновления);

– удаленное управление работой системы;

– web-технологии, используемые на верхнем уровне АСУ ТП;

– отказ даже от минимальных мер безопасности (нередко ради удобства и производительности компании отказываются от установки не только,

например, антивирусной, но и даже парольной защиты критически важных активов);

– использование Windows в качестве основной операционной системы для рабочих станций и серверов;

– человеческий фактор (слабая дисциплина, отсутствие знаний в области информационной безопасности).

3. ОСНОВЫ ПРОЕКТИРОВАНИЯ СОИБ АСУ ТП

Различные компоненты автоматизированной системы управления технологическими процессами могут быть уязвимы для различных типов атак, создавая риски для целостности, доступности и общей безопасности системы.

На основе реальных инцидентов были отмечены наиболее уязвимые компоненты АСУ ТП [4, 5]:

– SCADA-серверы;
– программируемые логические контроллеры (ПЛК);
– операционные системы;
– протоколы связи;
– базы данных.

Процесс создания системы защиты АСУ ТП в большинстве случаев проходит на действующих предприятиях без остановки технологических процессов и без отрыва обслуживающего персонала от работы.

Фундаментальный аспект организации защиты АСУ ТП заключается в обеспечении достаточной защищенности систем при одновременном удовлетворении требований в высокой доступности компонентов автоматизации [6].

Многие компоненты системы чувствительны к внесению изменений в конфигурацию и могут привести к нарушению технологического процесса [7].

Проектирование системы защиты необходимо начинать с определения объектов защиты, моделирования угроз и определения возможных рисков. Важно учитывать особенности работы объекта и назначение отдельных модулей. Особенности АСУ ТП приведены в предыдущем пункте работы [1].

Проектирование СОИБ для систем автоматизации технологического процесса важно основывать на следующих принципах:

– точная и детальная настройка средств защиты с учетом критической важности автоматизированной системы управления как сложного объединения программных и аппаратных компонентов;

– использование специализированных средств, разработанных для применения в промышленной автоматизации, способных работать с промышленными (в том числе проприетарными) протоколами передачи данных;

– интеграция мер кибербезопасности в инфраструктуру автоматизированной системы управления с точки зрения не только управления системой ИБ, но и получения от данных средств событий безопасности для последующего анализа и выработки мер по ИБ на основе результатов анализа;

– контроль ресурсоемкости средств защиты и использование средств с допустимой нагрузкой на аппаратные ресурсы компонентов комплекса автоматизации;

– учет физической среды функционирования защищаемого комплекса автоматизации, выбор средств, соответствующих требованиям климата функционирования системы и учитывающих агрессивность среды.

Также важно принимать во внимание риски, связанные с персоналом и физической безопасностью компонентов. Для закрытия таких рисков используется набор организационных мер, таких как запрет проноса на территорию и использования различных устройств и внешних носителей, физическое ограничение возможности использования портов оборудования, а также введение строгого контроля доступа и ограничения доступа к системе на основе ролей и обязанностей [3].

Следует отметить, что организация системы защиты автоматизированной системы управления технологическими процессами требует тщательного и многогранного подхода. Точная настройка, глубокое понимание тонкостей системы, активное использование специальных функциональных возможностей, плавная интеграция в единую систему кибербезопасности и всестороннее внедрение в инфраструктуру являются ключевыми элементами. Кроме того, целостная интеграция инструментов безопасности не только для управления, но и для извлечения событий безопасности и последующего анализа подчеркивает необходимость постоянного совершенствования и адаптации. Соблюдение этих принципов обеспечивает не только безопасность, но и устойчивость и оперативность реагирования автоматизированной системы управления на меняющийся ландшафт киберугроз.

ЗАКЛЮЧЕНИЕ

Всестороннее изучение основных задач, уровней и компонентов автоматизированных систем управления технологическими процессами позволяет определить отличительные особенности этих систем и принципы, учитывающие необходимость индивидуального и адаптивного подхода к организации системы обеспечения информационной безопасности.

По мере исследования уровней АСУ ТП от полевых устройств, таких как датчики и исполнительные механизмы, до систем диспетчерского

управления и сбора данных (SCADA) важность обеспечения безопасности каждого компонента становится очевидной. Компоненты нижнего и среднего уровней связаны между собой проводными линиями связи в единую распределенную систему управления, работающую в режиме реального времени. Доступ к датчикам осуществляется по протоколам и полевым шинам, также зачастую в таких системах используют специализированные и специально разработанные протоколы связи, влекущие за собой как ряд преимуществ, так и ряд сложностей и проблем. Контроллеры и диспетчерское управление зачастую территориально изолированы друг от друга и осуществляют связь посредством организации выделенных каналов связи, что также вносит свои коррективы в систему защиты. Взаимосвязанный характер этих систем требует целостного подхода, при котором безопасность отдельных элементов способствует устойчивости работы всей системы.

Отличительные особенности АСУ ТП, включая обработку данных в режиме реального времени, необходимость незамедлительного принятия важных решений и непрерывный мониторинг, требуют сложной системы защиты, не влияющей на работу системы.

Также при проектировании системы защиты основной упор необходимо делать на целостность и доступность информации, это обусловлено критичностью времени реакции для корректного функционирования системы. Контроль в режиме реального времени и принятие решений зависит от немедленного доступа к точным данным, а нарушение целостности и доступности передаваемой информации может привести к принятию неверных решений и сбоям в работе объекта автоматизации или его остановки

В статье рассмотрены такие особенности АСУ ТП, как длительный жизненный цикл системы, использование специализированных и специально разработанных протоколов, территориальная удаленность компонентов АСУ ТП. Рассмотрены возможные проблемы, связанные с этими особенностями.

На основе рассмотренных особенностей системы приведены важнейшие принципы, необходимые для построения эффективной системы защиты и включающие точную настройку средств защиты с учетом критической важности автоматизированной системы управления, использование специализированных средств, разработанных для применения в промышленной автоматизации, интеграцию мер кибербезопасности в инфраструктуру без остановки и влияния на работу компонентов, контроль ресурсоемкости средств защиты и учет физической среды функционирования защищаемого комплекса автоматизации.

В заключение необходимо отметить, что методы и принципы защиты, рассмотренные в статье, составляют лишь часть необходимых комплексных мер. Решение проблем в области защиты автоматизированных систем требует целостного подхода, который охватывает более широкий спектр методов обеспечения безопасности и постоянную адаптацию к возникающим угрозам. Каждая информационная система АСУ ТП специфична. Даже если системы функционируют в одной сфере, они могут быть построены на базе средств различных производителей, иметь разную архитектуру, разные протоколы, разные датчики и разные параметры контроля технологического процесса. Поэтому важно подходить к проектированию системы защиты каждой системы с индивидуальным и всеохватывающим подходом.

СПИСОК ЛИТЕРАТУРЫ

1. Моделирование угроз информационной безопасности в автоматизированных системах управления предприятиями топливно-энергетического комплекса / В.Г. Лим, Ю.А. Арбузов, В.Н. Химич, С.К. Дзиоев // Вопросы защиты информации. – 2010. – № 3 (90). – С. 23–27.

2. Введение в безопасность систем ICS/SCADA / SecurityLab.ru. – URL: https://www.securitylab.ru/analytics/487977.php?R=1 (дата обращения: 06.03.2024).

3. *Яковенко Я., Каменева Е.* Особенности прогнозирования и оценки эффективности средств антивирусной защиты и межсетевого экранирования в АСУ ТП на предприятии нефтегазовой отрасли // Инновационные научные исследования: теория, методология, практика: сборник статей XV Международной научно-практической конференции. – Пенза, 2018. – С. 73–82.

4. *Пищик Б.* Безопасность АСУ ТП // Вычислительные технологии. – 2013. – Т. 18, спец. вып. – С. 170–175.

5. Безопасность промышленных систем в цифрах v2.1 / Г. Грицай, А. Тиморин, Ю. Гольцев, Р. Ильин, С. Гордейчик. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/SCADA-analytics-rus.pdf (дата обращения: 06.03.2024).

6. *Мухаметшин А.* Как защитить АСУ ТП: экспертиза Innostage // СТА: Современные технологии автоматизации. – 2023. – № 3. – С. 66–72.

7. *Акименко В.* Где кроются реальные проблемы защиты АСУ ТП? // Информационная безопасность. – 2017. – № 6. – URL: https://lib.itsec.ru/articles2/import/gde-kroyutsya-realnye-problemy-zaschity-asu-tp (дата обращения: 06.03.2024).

8. Insights on the security and dependability of industrial control systems / F. Kargl, R.W. van der Heijden, H. König, A. Valdes, M.C. Dacier // IEEE Security & Privacy. – 2014. – Vol. 12 (6). – P. 75–78. – DOI: 10.1109/MSP.2014.120.

9. *Jazdi N.* Cyber physical systems in the context of Industry 4.0 // 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania. – IEEE, 2014. – P. 1–4. – DOI: 10.1109/AQTR.2014.6857843.

Бычкова Екатерина Игоревна, лаборант кафедры защиты информации Новосибирского государственного технического университета. E-mail: e.bychkova.2018@stud.nstu.ru

Лысенко Марина Валерьевна, ассистент кафедры защиты информации Новосибирского государственного технического университета. E-mail: m.v.lysenko@corp.nstu.ru

DOI: 10.17212/2782-2230-2024-1-9-22

Overview of the main components, features and security solutions of automated process control systems*

E.I. Bychkova[1], M.V. Lysenko[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: e.bychkova.2018@stud.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, assistant of the Department of Information Security. E-mail: m.v.lysenko@corp.nstu.ru*

The structure, main components and tasks of typical automated process control systems (ACS) are described. The main distinctive features of automated systems and their impact on the design of an information security system (ISMS) are determined. A brief overview of the problems of information security of automated process control systems is given. The basic principles that must be taken into account when creating.

Keywords: automated process control system, automated control system, automation, technological systems, protection system, information protection, information system, information security systems

* *Received 10 February 2024.*

REFERENCES

1. Lim V.G., Arbuzov J.A., Himich V.N., Dzioev S.K. Modelirovanie ugroz informatsionnoi bezopasnosti v avtomatizirovannykh sistemakh upravleniya predpriyatiyami toplivno-energeticheskogo kompleksa [Modelling of threats of information safety in the automated control systems of the enterprises of a fuel and energy complex]. *Voprosy zashchity informatsii = Information security questions*, 2010, no. 3 (90), pp. 23–27.

2. SecurityLab.ru. *Vvedenie v bezopasnost' sistem ICS/SCADA* [Introduction to the security of ICS/SCADA systems]. Available at: https://www.securitylab.ru/analytics/487977.php?R=1 (accessed 06.03.2024).

3. Yakovenko Y., Kameneva E. [Features of forecasting and evaluating the effectiveness of anti-virus protection and firewall in the automated process control system in the oil and gas industry]. *Innovatsionnye nauchnye issledovaniya: teoriya, metodologiya, praktika* [Innovative scientific research: theory, methodology, practice]. Collection of articles of the XV International Scientific and Practical Conference. Penza, 2018, pp. 73–82. (In Russian).

4. Pishchik B. Bezopasnost' ASU TP [Safety of automated control systems]. *Vychislitel'nye tekhnologii = Computational Technologies*, 2013, vol. 18, Spec. iss., pp. 170–175.

5. Gritsai G., Timorin A., Gol'tsev Y., Il'in R., Gordeichik S. *Bezopasnost' promyshlennykh sistem v tsifrakh v2.1* [Safety of industrial systems in numbers v2.1]. Available at: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (accessed 06.03.2024).

6. Mukhametshin A. Kak zashchitit' ASU TP: ekspertiza Innostage [How to protect the automated control system: Innostage expertise]. *STA: Sovremennye tekhnologii avtomatizatsii*, 2023, no. 3, pp. 66–72. (In Russian).

7. Akimenko V. Gde kroyutsya real'nye problemy zashchity ASU TP? [Where are the real problems of automated process control system protection?]. *Informatsionnaya bezopasnost' = Information Security*, 2017, no. 6. Available at: https://lib.itsec.ru/articles2/import/gde-kroyutsya-realnye-problemy-zaschity-asu-tp (accessed 06.03.2024).

8. Kargl F., Heijden R.W. van der, Konig H., Valdes A., Dacier M.C. Insights on the security and dependability of industrial control systems. *IEEE Security & Privacy*, 2014, vol. 12 (6), pp. 75–78. DOI: 10.1109/MSP.2014.120.

9. Jazdi N. Cyber physical systems in the context of Industry 4.0. *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, Cluj-Napoca, Romania, 2014, pp. 1–4. DOI: 10.1109/AQTR.2014.6857843.

Для цитирования:

Бычкова Е.И., *Лысенко М.В.* Обзор основных компонентов, особенностей и решений безопасности автоматизированных систем управления технологическими процессами // Безопасность цифровых технологий. – 2024. – № 1 (112). – С. 9–22. – DOI: 10.17212/2782-2230-2024-1-9-22.

For citation:

Bychkova E.I., Lysenko M.V. Obzor osnovnykh komponentov, osobennostei i reshenii bezopasnosti avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami [Overview of the main components, features and security solutions of automated process control systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 1 (112), pp. 9–22. DOI: 10.17212/2782-2230-2024-1-9-22.