Методы и средства защиты информации автоматизированной системы учета товарной продукции нефтегазодобывающего предприятия

С.О. Школьников, Т.В. Хоменко, Е.Л. Медянкина

Астраханский государственный технический университет, Астрахань, Россия

Аннотация **– Исследование касается проектирования и обеспечения информационной безопасности для автоматизированной системы учета товарной продукции нефтегазодобывающего предприятия. В товарную продукцию входят различные углеводороды, такие как газ, газовый конденсат, а также сера и другие продукты их переработки. Описаны основные принципы информационной безопасности для системы мониторинга технологических процессов, связанных с добычей, хранением, транспортировкой и переработкой углеводородов, а также отгрузкой товарной продукции. Планируется выявление узких мест в производственном цикле. Определены требования к серверному и вспомогательному оборудованию для трех уровней системы.**

Ключевые слова **– автоматизированная система, мониторинг технологических процессов, информационная безопасность, средства измерений, дистанционный сбор информации, автоматический контроль, оперативное управление, контролируемый объект, серверное оборудование, структурная схема.**

I. ВВЕДЕНИЕ

Автоматизированная система (АС) – это комплекс программного и аппаратного обеспечения, который может выполнять определенные задачи и функции без непосредственного участия человека. Она выполняет автоматическую обработку данных, управлением процессами, принятие решений и выполнение действий в соответствии с заранее определенными алгоритмами и правилами. Так, например, «Система автоматизированного учета сырья, полупродуктов и товарной продукции» [1] (САУ СП и ТП) на нефтегазоперерабатывающем предприятии играет важную роль в контроле и оптимизации производственных процессов.

Одним из основных преимуществ АС является возможность оперативного мониторинга процессов добычи, транспортировки и хранения газа. Эта система позволяет быстро обнаруживать и устранять проблемы, связанные с утечками, аппаратными сбоями или несоответствиями в производственной среде. Поэтому для обеспечения работоспособности данной системы необходимо обеспечивать информационную безопасность.

II. ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ

Структура комплекса технических средств САУ СП и ТП должна быть основана на следующих основных принципах современной концепции построения автоматизированных систем управления [2]:

- централизованный иерархический контроль и управление средствами автоматизации;
- открытая архитектура информационного взаимодействия компонентов системы;
- распределенная структура сбора и обработки информации;
- простота обслуживания и высокая доступность программного и аппаратного обеспечения, внедрение самодиагностики.

Автоматизированная система управления технологическими процессами (САУ ТП) на нефтегазодобывающем предприятии (НГДП), организованная по иерархическому принципу, должна включать следующие уровни (Рис.1):

- нижний уровень: узлы измерения на технологических установках;
- средний уровень: вычислительные системы и автоматизированные рабочие места работников в операторных;
- верхний уровень: серверы, размещенные в серверных помещениях НГДП.

Целью обеспечения защиты информации является повышение стабильности функционирования и реализации внедряемых технологических процессов путем предотвращения и уменьшения возможного ущерба от несанкционированного воздействия на объекты защиты САУ СП и ТП [2].

Обеспечение информационной безопасности для САУ СП и ТП должно быть основано на следующих принципах:

- обязательная идентификация и классификация объектов охраны;
- выбор мер и средств защиты с учетом модели частных угроз;

• оценка рисков, связанных с реализацией угроз информационной безопасности;
• регулирование доступа к охраняемым объектам.

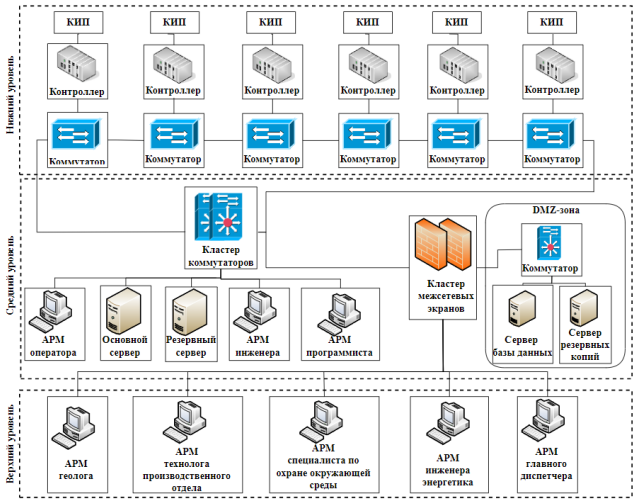

Рис. 1. Структурная схема САУ ТП

Объектами защиты САУ СП и ТП могут являться:
• серверное оборудование (серверные системы SCADA, архивные, коммуникационные и другие серверы);
• локальные системы автоматизации (системы автоматического управления, узлы, контроллеры, пункты управления технологическими объектами);
• устройства связи с объектами (сенсорное оборудование и программируемые логические контроллеры);
• рабочие станции операторов и специалистов;
• сетевые устройства (коммутаторы, маршрутизаторы, интерфейсные процессоры, интегрирующие контроллеры, контроллеры объектной связи);
• каналы передачи данных;
• программное обеспечение;
• информация о процессах производства (включая сигналы, управляющие команды, данные параметров (состояния) объекта (процесса) управляемого процесса).

САУ СП и ТП должна включать в себя систему управления, построенную в виде локальной компьютерной сети (ЛВС), изолированной от внешних сетей путем фильтрации информационных потоков [3]. Информационное взаимодействие с информационно-управляющей системой (ИУС) заключается в передаче технологической информации САУ СП и ТП в ИУС и получении из ИУС необходимой информации, связанной с управлением САУ СП и ТП, обновлением ПО, конфигураций элементов САУ СП и ТП и входящих в ее состав средств защиты.

Информационная безопасность САУ СП и ТП должна обеспечиваться в следующих направлениях (Рис.2):

1) Защита обработки, хранения и передачи информации: является критически важным аспектом для обеспечения безопасности данных и предотвращения возможных утечек или несанкционированного доступа к информации. Это достигается различными путями. Так, системные и сетевые администраторы могут вносить изменения в конфигурацию средств обработки и хранения данных, а также в сетевую инфраструктуру и конфигурацию сетевого оборудования. Администраторы информационной безопасности также могут вносить изменения в конфигурацию безопасности. Все изменения должны регистрироваться в соответствующих журналах. Также необходимо запретить изменять конфигурацию обработки, хранения и распространения информации самими пользователями САУ СП и ТП. Использование съемных носителей в САУ СП и ТП также должно быть запрещено [4].

2) Защита от вредоносного программного обеспечения: для предотвращения проникновения, обнаружения и нейтрализации вредоносного программного обеспечения (ПО) должны применяться меры защиты от вредоносного программного обеспечения, направленные на предотвращение, обнаружение и нейтрализацию проникновения вредоносного программного обеспечения. Антивирусное программное обеспечение следует установить на серверное оборудование и рабочие станции операторов и специалистов. Если установка антивредоносного программного обеспечения на определенные серверы и рабочие станции технически невозможна, принимаются дополнительные организационные и технические меры защиты. Средства защиты от вредоносных программ должны управляться и обновляться централизованно. Можно использовать только антивредоносное программное обеспечение, сертифицированное на соответствие требованиям информационной безопасности. Средства защиты от вредоносных программ должны управляться и настраиваться системным администратором информационной безопасности [4].

3) Резервирование серверов, сетевого оборудования и каналов передачи данных автоматизированной системы управления технологическими процессами: для обеспечения бесперебойной работы САУ СП и ТП должна обеспечиваться безопасность важных серверов и рабочих станций, сетевого оборудования, функций безопасности и каналов передачи данных. Перечень важнейших средств защиты, обработки, хранения и передачи информации следует формировать в результате идентификации и классификации объектов САУ СП и ТП [4].

Для резервирования серверов и рабочих станций стоит использовать отказоустойчивые схемотехнические решения (использование кластерных конфигураций серверов; двойное подключение сервера к локальной сети через два сетевых интерфейса, подключенных к разным коммутаторам локальной сети или разным модулям одного и того же коммутатора и т.д.). Для обеспечения избыточности сетевого оборудования, средств защиты и каналов передачи данных необходимо внедрить:

• применение отказоустойчивых схемотехнических решений;
• дублирование проводных каналов передачи данных с беспроводными каналами;
• дублирование сетевого оборудования и средств защиты.

Для быстрого восстановления конфигурации серверов, сетевого оборудования и безопасности в случае физического или логического сбоя необходимо выполнять резервное копирование конфигураций и образов системных дисков сервера, а также сохранять файлы конфигураций сетевого оборудования и безопасности.

4) Защита сетевой инфраструктуры: для обеспечения непрерывной и стабильной работы САУ СП и ТП необходима защита сетевой инфраструктуры. Она должна осуществляться следующими способами:
• физическая защита сетевого оборудования и средств безопасности;
• контроль логического доступа к сетевому оборудованию;
• шифрование каналов управления;
• мониторинг сетевых подключений;
• обнаружение и предотвращение вторжений;
• мониторинг сетевых устройств, подключенных к локальной сети САУ СП и ТП;
• использование встроенной защиты сетевого оборудования от смены адресов (защита от подмены);
• защита ограниченной информации, если она передается за пределы контролируемых зон;
• использование инструментов для мониторинга и регистрации событий.

Управление входящими и исходящими информационными потоками в локальной вычислительной сети САУ СП и ТП должно осуществляться сертифицированными средствами межсетевого экранирования, размещенных на входе в ЛВС САУ СП и ТП. Сетевые соединения между локальной сетью САУ СП и ТП и подключенными к ней беспроводными сетями также контролируются с помощью брандмауэра [5].

5) Защита программного обеспечения: для поддержания функциональности программного обеспечения необходимо принимать меры по устранению уязвимостей в программном обеспечении, а также другие меры защиты. Устранение уязвимостей программного обеспечения достигается за счет регулярного централизованного поиска и установки обновлений, предоставляемых разработчиками программного обеспечения. Системные администраторы и администраторы приложений должны обновлять операционную систему (ОС) и другое общесистемное и прикладное программное обеспечение. Серверы обновлений должны доставлять обновления для программного обеспечения САУ СП и ТП [5].

6) Регистрация и учёт событий информационной безопасности: для своевременного выявления нарушений информационной безопасности необходимо осуществлять отслеживание событий в операционных и прикладных системах, системах управления базами данных (СУБД), сетевом оборудовании и средствах безопасности. В САУ СП и ТП должны регистрироваться события, которые могут возникнуть в результате нарушений безопасности, и они регистрируются в журналах событий операционных и прикладных систем, СУБД, сетевого оборудования и функций безопасности. В САУ СП и ТП должна происходить регистрация следующих событий [6]:
• действия пользователя для доступа к операционным и прикладным системам;
• действия администраторов по изменению настроек обработки, хранения и передачи информации, конфиденциальности и прав доступа пользователей;
• попытки несанкционированного подключения к сетевой инфраструктуре и замены адресов сетевых устройств;
• попытка получить доступ к журналам событий.

7) Контроль защищённости: чтобы своевременно и эффективно реагировать на выявленные уязвимости средств защиты информации в САУ СП и ТП необходимо принимать меры для мониторинга безопасности оборудования обработки, хранения и передачи [7]. Проверки безопасности должны проводиться специалистами отдела информационной безопасности и выполняться следующими способами:
• регулярный инструментальный анализ безопасности с помощью сканеров безопасности;
• анализ конфигурационных файлов для обработки, хранения и передачи информации.

Базы данных об уязвимостях регулярно должны обновляться веб-сайтами производителей используемых СЗИ.

8) Криптографическая защита: для обеспечения безопасности автоматизированной системы учёта продукции нефтегазодобывающего предприятия необходимо использовать криптографические методы защиты данных. Криптографическая защита обеспечивает конфиденциальность, целостность и аутентификацию информации, передаваемой и хранящейся в системе [7]. В САУ СП и ТП должен использоваться сильный алгоритм шифрования для защиты конфиденциальности данных. Для передачи данных между устройствами также должно использоваться шифрование, которое обеспечивает защищенное соединение. Также, для обеспечения целостности данных в системе могут использоваться хэш-функции, которые позволяют проверить, были ли данные изменены в процессе передачи или хранения.

9) Физическая защита: для предотвращения несанкционированного доступа и утечки информации, кражи технических средств обработки и хранения информации, а также простоев в процессе обработки данных должны быть предусмотрена физическая защита технических средств. Серверное оборудование и критически важное сетевое оборудование необходимо разместить в запираемых шкафах, установить сигнализации в специальных помещениях (серверных). Перед утилизацией или передачей технического оборудования на ремонт информация

должна гарантированно стираться. Кабельные сети необходимо проложить таким образом, чтобы максимально ограничить несанкционированный доступ.

Таким образом, информационная безопасность САУ СП и ТП должна обеспечивается в следующих направлениях (Рис.2):

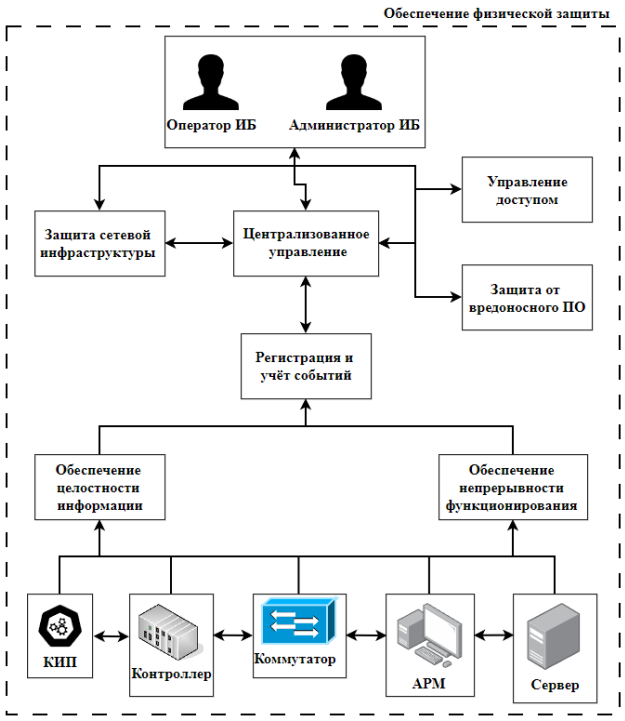

Рис. 2. Функциональная схема системы информационной безопасности

III. ЗАКЛЮЧЕНИЕ

Автоматизированные системы играют ключевую роль в современных производственных процессах, особенно в нефтегазовой отрасли. Структура САУ должна быть организована по иерархическому принципу, что обеспечивает централизованный контроль и управление, а также распределенную обработку информации. Принципы построения таких систем включают открытость архитектуры, простоту обслуживания и внедрение самодиагностики.

Обеспечение информационной безопасности автоматизированных систем в нефтегазовой отрасли включает в себя защиту серверного оборудования, локальных систем автоматизации, сетевых устройств и программного обеспечения от несанкционированного доступа и вредоносного ПО. Рекомендуется применять многоуровневую защиту, включая физическую защиту, криптографические методы, резервирование оборудования и регулярный мониторинг событий информационной безопасности.

Для обеспечения эффективной работы автоматизированных систем управления в нефтегазовой отрасли важно не только внедрять передовые технологии, но и обеспечивать кибербезопасность и защиту инфраструктуры. Это поможет снизить риски, повысить стабильность и адаптивность производства, что особенно актуально в условиях быстроменяющегося технологического и геополитического ландшафта для достижения долгосрочной устойчивости и развития предприятий.

ЛИТЕРАТУРА

[1] Газпром информ: официальный сайт. – Астрахань. – URL: http://www.gazprominfo.ru/terms/gpz/ (дата обращения: 01.05.2025). – Текст: электронный.
[2] Гусев, А. И., Смирнов, П. В. Современные подходы к защите информации в автоматизированных системах управления. Вестник информационных технологий – М.: Наука, 2020. – 45с.
[3] В. А. Морозов. «Технологии защиты информации в системах учета товарной продукции». Журнал безопасности информации, 2022 –19с.
[4] Кузнецов, С. А., Защита информации в автоматизированных системах: Учебное пособие. Санкт-Петербург: Питер, 2019.
[5] Галушко А.И., Защита информации в автоматизированных системах. — М.: Издательство "Эксмо", 2019. — 250 с.
[6] Петров И.С., Риски и угрозы информационной безопасности в нефтегазовой отрасли. — М.: Наука, 2020. — 240 с.
[7] Широков А.А., Автоматизация учёта товарной продукции: современные подходы и технологии. — М.: Инфра-М, 2020. — 220 с.

Информация об авторах

Хоменко Татьяна Владимировна – д.т.н., профессор, заведующий кафедрой «Автоматизированные системы обработки информации и управления» Астраханского государственного технического университета, Астрахань, Россия, Астрахань, Россия, e-mail: t_v_khomenko_stud@mail.ru

Медянкина Елена Львовна – к.п.н, доцент кафедры «Автоматика и управление» Астраханского государственного технического университета, Астрахань, Россия, e-mail: mel292016@mail.ru

Школьников Сергей Олегович – магистрант по направлению «Информатика и вычислительная техника» Астраханского государственного технического университета, Астрахань, e-mail: shkolnikov3210@mail.ru

Methods and means of information protection of an automated accounting system for commercial products of an oil and gas producing enterprise

S.O. Shkolnikov, T.V. Khomenko, E.L. Medyankina

Astrakhan State Technical University, Astrakhan, Russia

***Abstract* – The research concerns the design and provision of information security for an automated accounting system for commercial products of an oil and gas producing enterprise. Commercial products include various hydrocarbons such as gas, gas condensate, as well as sulfur and other processed products. The basic principles of information security for the monitoring system of technological processes related to the extraction, storage, transportation and processing of**

hydrocarbons, as well as the shipment of marketable products, are described. It is planned to identify bottlenecks in the production cycle. The requirements for server and auxiliary equipment for three levels of the system are defined.

Keywords **– automated system, monitoring of technological processes, information security, measuring instruments, remote information collection, automatic control, operational management, controlled facility, server equipment, block diagram.**

References

[1] Gazprom inform: official website. – Astrakhan. – URL: http://www.gazprominfo.ru/terms/gpz / – Text: electronic.
[2] Gusev, A. I., Smirnov, P. V., Modern approaches to information protection in automated control systems. Bulletin of Information Technologies– Moscow: Nauka Publ., 2020– 45 pp.
[3] Morozov, V. A. Information security technologies in commodity accounting systems. Information Security Journal, 2022-19c.
[4] Kuznetsov, S. A., Information protection in automated systems: A textbook. St. Petersburg: Peter, 2019.
[5] Galushko A.I., Information protection in automated systems. Moscow: Eksmo Publishing House, 2019. 250 p.
[6] Petrov I.S., Risks and threats to information security in the oil and gas industry, Moscow: Nauka Publ., 2020, 240 p.
[7] Shirokov A.A., Automation of accounting for commercial products: modern approaches and technologies, Moscow: Infra-M, 2020, 220 p.