УДК 004.056, 658.382, 681.3

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА РОИЗВОДСТВЕННЫХ УЧАСТКАХ

Массалиев Темирлан Алексеевич

студент, факультет «Цифровые технологии и искусство», кафедра Высшая школа компьютерной инженерии,
Университет «Туран», г.Алматы, Казахстан

Научный руководитель: Нурымова Сауле Кенесовна

В статье рассматриваются современные подходы к обеспечению информационной безопасности на производственных участках. Основное внимание уделено сегментации сети с использованием изолированных подсетей и туннелей VPN, внедрению централизованного логирования событий с помощью SIEM-систем, а также применению специализированных устройств для физического размыкания сетевых соединений. Приводятся ключевые принципы маршрутизации трафика, обеспечивающие передачу данных только между устройствами, участвующими в рабочих процессах, и ограничивающие доступ инженерного состава через файрволл. Рассматриваются этапы практической реализации решений, включая настройку сетевой инфраструктуры, интеграцию систем мониторинга и внедрение механизмов физической защиты. Предложенные меры направлены на минимизацию рисков кибератак и утечек данных, что способствует повышению уровня безопасности и надёжности автоматизированных систем управления технологическими процессами (АСУТП).

Ключевые слова: Информационная безопасность (ИБ), Автоматизация систем управления технологическим процессом (АСУТП), SIEM система, VPN, Firewall, Автоматизированная Система Контроля и Учета Электроэнергии (АСКУЭ), Программируемый логический контроллер (ПЛК), Human Machine Interface (HMI)- человеко-машинный интерфейс.

Введение

Информационная безопасность (ИБ) на производственных участках является одним из ключевых аспектов обеспечения бесперебойной и безопасной работы автоматизированных систем управления технологическими процессами (АСУТП). Современные киберугрозы, такие как атаки на промышленное оборудование, компрометация сетевых устройств и утечка данных, требуют разработки комплексного подхода к защите

производственных сетей. В данной статье рассмотрены методы сегментации сети, логирования событий и физической защиты сетевой инфраструктуры с помощью специальных устройств.

Обоснование выбора архитектуры сети

Эффективная защита производственных участков начинается с проектирования архитектуры сети, обеспечивающей минимизацию точек взаимодействия и контроль трафика. В основе лежат следующие принципы:

1. ***Сегментация сети на изолированные подсети****:*

- *Подсеть процессного участка****:*** включает контроллеры ПЛК (PLC), промышленные компьютеры HMI/SCADA и исполнительные устройства. Взаимодействие внутри подсети ограничивается рабочими процессами, исключая несанкционированный доступ извне.
- *Подсеть АСКУЭ:* предназначена для сбора и обработки данных энергоэффективности. Доступ к данным осуществляется только через контролируемую точку.
- *Подсеть инженерного состава:* обеспечивает работу персонала, занимающегося обслуживанием и настройкой оборудования. Доступ возможен только через файрволл и VPN.

2. ***Использование VPN-туннелей****:*

- Все взаимодействия между подсетями проходят через туннели VPN, исключая прямое соединение.
- VPN-серверы размещены в демилитаризованной зоне (DMZ), что позволяет контролировать доступ и минимизировать риск компрометации.

3. ***Маршрутизация пакетов****:*

- Файрволлы на границе каждой подсети обеспечивают передачу данных только между устройствами, участвующими в рабочем процессе (например, ПЛК и HMI).

Логирование и мониторинг событий

Для своевременного обнаружения и реагирования на инциденты в сети необходимо внедрение системы централизованного логирования и анализа событий. Основные этапы:

1. ***Внедрение SIEM-системы****:*

- Сбор логов со всех ключевых устройств сети: файрволлов, VPN-серверов, коммутаторов и серверов.
- Анализ событий в реальном времени с использованием корреляции данных.
- Примеры логируемых событий:
  - Попытки подключения к запрещённым узлам.
  - Изменение конфигурации сетевых устройств.
  - Необычная активность в VPN-туннелях.

2. ***Создание централизованного сервера логов****:*

- Логи передаются на защищённый сервер с разграничением доступа.
- Настройка уведомлений на подозрительные события, такие как превышение лимитов трафика или многократные попытки аутентификации.

3. ***Ретенция данных****:*

- Установление сроков хранения логов в соответствии с политиками безопасности.
- Регулярное резервное копирование логов.

Использование устройств для физического размыкания сети

Для повышения уровня защиты производственной сети предлагается использование специализированных устройств, обеспечивающих физическое размыкание соединений. Эти устройства работают на основе механических ключей и обеспечивают абсолютную изоляцию сетевых компонентов.

1. ***Преимущества физического размыкания****:*

- Исключение несанкционированного доступа даже при компрометации сетевых устройств.
- Высокий уровень отказоустойчивости и надёжности.

2. ***Этапы внедрения устройств****:*

- *На входе в систему****:***
  - Установка устройства между сетью инженерного состава и производственной сетью.
  - Применение ключа для размыкания соединения в случае необходимости проведения технических работ или при обнаружении угрозы.
- *Между туннелями внешней сети и производственной сетью****:***
  - Размещение устройства на границе VPN-туннеля для предотвращения утечек данных и атак со стороны внешних подключений.

3. ***Пример реализации****:*

- Устройство устанавливается в шкаф управления сети.
- Ключ для активации соединения находится только у уполномоченного персонала. В случае угрозы соединение размыкается мгновенно.

Практическая реализация

На практике внедрение предложенных мер включает следующие шаги:

1. ***Настройка маршрутизации****:*

- Файрволлы конфигурируются для передачи пакетов только между устройствами, которые участвуют в рабочих процессах (например, ПЛК и HMI).
- Пример правила на файрволле:
  - Разрешить трафик Modbus TCP с IP-адреса ПЛК на IP-адрес HMI.
  - Запретить весь остальной трафик.

2. ***Интеграция SIEM-системы****:*

- Установка агентов на ключевые узлы для сбора логов.
- Настройка дашбордов для мониторинга активности в реальном времени.

*3. **Размещение устройств физического размыкания**:*

- Устройства подключаются к критическим точкам сети.
- Инженеры проходят обучение по использованию данных устройств.

Заключение

Предложенная архитектура сети обеспечивает высокий уровень информационной безопасности на производственных участках. Сегментация сети, логирование событий и использование устройств физического размыкания минимизируют риски утечек данных и кибератак. Внедрение данных решений позволит не только защитить производственные процессы, но и повысить общую устойчивость системы к внешним угрозам. На следующем этапе возможно дальнейшее развитие системы за счёт применения современных технологий, таких как искусственный интеллект для анализа угроз, и расширение автоматизации процессов управления ИБ.

Список использованной литературы

1. Weiss, J., Industrial Control System Cybersecurity: Fundamentals and Applications. Wiley, 2020.
2. Stouffer, K., Falco, J., & Scarfone, K., Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, Revision 2, 2015.
3. He, X., Zhang, Y., & Xie, L., Cybersecurity in Industrial Automation and Control Systems: Roadmap for Future Research. Springer, 2021.
4. European Union Agency for Cybersecurity (ENISA), Good Practices for Security of Internet of Things in Industry 4.0. ENISA Report, 2022.
5. Langner, R., Robust Industrial Control System Networks. Momentum Press, 2017.

ӨНДІРІСТІК УЧАСКЕЛЕРДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК

Массалиев Темирлан Алексеевич

Ғылыми жетекші: Нурымова Сауле Кенесовна

Бұл мақалада өндірістік учаскелерде ақпараттық қауіпсіздікті қамтамасыз етудің заманауи тәсілдері қарастырылады. Негізгі назар оқшауланған ішкі желілер мен VPN туннельдерді пайдалану арқылы желіні сегментациялауға, оқиғаларды орталықтандырылған тіркеу үшін SIEM жүйелерін енгізуге, сондай-ақ желілік қосылыстарды физикалық ажыратуға арналған арнайы құрылғыларды қолдануға аударылады. Деректер алмасуды тек жұмыс процестеріне қатысатын құрылғылар арасында қамтамасыз ететін және

инженерлік құрамның файрволл арқылы қол жеткізуін шектейтін негізгі трафикті маршрутизациялау қағидаттары ұсынылады. Желілік инфрақұрылымды баптау, мониторинг жүйелерін интеграциялау және физикалық қорғаныс механизмдерін енгізуді қоса алғанда, шешімдерді практикалық жүзеге асыру кезеңдері қарастырылады. Ұсынылған шаралар кибершабуылдар мен деректердің сыртқа шығу қаупін азайтуға бағытталған, бұл өз кезегінде технологиялық процестерді басқарудың автоматтандырылған жүйелерінің (АСУТП) қауіпсіздігі мен сенімділік деңгейін арттыруға ықпал етеді.

Кілт сіздер: Ақпараттық қауіпсіздік (АҚ), Технологиялық процестерді басқарудың автоматтандырылған жүйесі (АСУТП), SIEM жүйесі, VPN, Firewall, Электр энергиясын бақылау және есепке алудың автоматтандырылған жүйесі (АСКУЭ), Бағдарламаланатын логикалық контроллер (ПЛК), Human Machine Interface (HMI) – адам-машина интерфейсі.

INFORMATION SECURITY AT INDUSTRIAL SITES

Massaliev T.A.

Scientific Supervisor: Nurymova S.K.

This article examines modern approaches to ensuring information security at industrial sites. The main focus is on network segmentation using isolated subnets and VPN tunnels, the implementation of centralized event logging through SIEM systems, and the application of specialized devices for physically disconnecting network connections. Key principles of traffic routing are provided, ensuring data transmission only between devices involved in work processes and restricting engineering personnel access through a firewall. The stages of practical implementation are considered, including network infrastructure configuration, integration of monitoring systems, and the introduction of physical security mechanisms. The proposed measures aim to minimize the risks of cyberattacks and data leaks, thereby enhancing the security and reliability of automated process control systems (APCS).

Keywords: Information Security (IS), Automated Process Control System (APCS), SIEM system, VPN, Firewall, Automated System for Electricity Control and Accounting (ASECA), Programmable Logic Controller (PLC), Human Machine Interface (HMI).

REFERENCES

1. Weiss, J., Industrial Control System Cybersecurity: Fundamentals and Applications. Wiley, 2020.
2. Stouffer, K., Falco, J., & Scarfone, K., Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, Revision 2, 2015.
3. He, X., Zhang, Y., & Xie, L., Cybersecurity in Industrial Automation and Control Systems: Roadmap for Future Research. Springer, 2021.
4. European Union Agency for Cybersecurity (ENISA), Good Practices for Security of Internet of Things in Industry 4.0. ENISA Report, 2022.
5. Langner, R., Robust Industrial Control System Networks. Momentum Press, 2017.