УДК 054.056.53

РЕАЛИЗАЦИЯ КОНЦЕПЦИИ SECURE BY DESIGN В ЦЕЛЯХ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ АСУ ТП ЭЛЕКТРИЧЕСКИХ ПОДСТАНЦИЙ

канд. физ.-мат. наук О. К. БАРАНОВСКИЙ, Е. П. ЛАДОХО
(Открытое акционерное общество «АГАТ – системы управления» – управляющая компания холдинга «Геоинформационные системы управления», г. Минск, Беларусь)

Аннотация. *Предложена архитектура локальной вычислительной сети электрической подстанции, реализация которой позволит повысить защищенность АСУ ТП от кибератак.*

Ключевые слова: *автоматизированная система управления технологическим процессом, электрическая подстанция, кибербезопасность, сегментация сети.*

Согласно Стратегии информатизации и цифровой трансформации ГПО «Белэнерго» на период 2021–2025 гг. (утверждена приказом ГПО «Белэнерго» от 09.04.2021 № 7) одной из задач цифровой трансформации является создание, модернизация и развитие автоматизированных систем управления технологическим процессом (далее – АСУ ТП), при этом особое внимание акцентировано на обеспечении информационной безопасности (далее – ИБ), включая создание и модернизацию систем ИБ (далее – СИБ) критически важных объектов информатизации (далее – КВОИ).

При определении требований к процедурам проектирования, создания и проверки соответствия реализованных мер обеспечения ИБ в АСУ ТП электрических подстанций (далее – ПС) руководствуются приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря г. № 449» (далее – приказ № 66), который устанавливает требования по защите информации (далее – ЗИ), распространение и (или) предоставление которой ограничено, а также меры ИБ КВОИ.

Вместе с тем, цифровая трансформация энергетики все более реализуется в виде взаимного проникновения информационных потоков информационных систем (далее – ИС) различного назначения, вследствие чего АСУ ТП ПС уже не могут считаться изолированными объектами информатизации. В этой связи планирование мер ИБ непосредственно в процессе документирования проектных решений сетевой инфраструктуры АСУ ТП позволяет существенно повысить уровень кибербезопасности за счет учета информационных факторов, влияющих на безопасность объекта.

Принято считать, что для успешной реализации угрозы ИБ необходимо наличие некой характеристики (уязвимости или недостатка) в объекте защиты. Для ИС выделяют следующие типы уязвимостей в зависимости от области происхождения [1]:

– уязвимости, появившиеся в процессе разработки программного обеспечения (далее – ПО);

– уязвимости, появившиеся в результате конфигурации ПО и технических средств;

– уязвимости архитектуры, появившиеся в процессе проектирования ИС;

– организационные уязвимости, появившиеся в результате отсутствия или несоблюдения правил эксплуатации ИС, требований локальных правовых актов по ЗИ и обеспечению ИБ;

– многофакторные уязвимости, появившиеся в результате наличия совокупности уязвимостей нескольких типов.

В [2] описан процесс обнаружения и устранения уязвимостей ИС. При этом предложено подразделять уязвимости на: уязвимости технических средств, уязвимости программных средств, уязвимости средств и систем ЗИ (далее – СЗИ), а также уязвимости, вызванные конфликтом взаимодействия средств ЗИ и СЗИ. Соответственно, предлагаются следующие меры устранения уязвимостей: устранение обновлениями, устранение патчами безопасности, устранение СЗИ, устранение средствами ЗИ, устранение настройками/политиками безопасности.

Сведения об обнаруженных уязвимостях можно получить из интернет-ресурсов со свободным доступом. Например, банк данных угроз безопасности информации ФСТЭК России [3] в качестве уязвимостей архитектуры содержит, главным образом, сведения об уязвимостях встроенного ПО. Вместе с тем, разработчики СЗИ сталкиваются с уязвимостями архитектуры масштаба объекта защиты – АСУ ТП (как системы из составляющей ее объектов), – связанными с недостатками организации сетевой инфраструктуры, на базе которой строится АСУ ТП, и которые появляются на этапе ее проектирования (строительства). Очевидно, что такого рода уязвимости могут быть устранены с применением дополнительных средств ЗИ или проектируемой СЗИ, что, в свою очередь, может оказывать влияние на показатели функциональной безопасности ПС. Внедрение дополнительных средств ЗИ приводит к тому, что строится «забор» не только вокруг объекта защиты, но и внутри его, а не изначально выстраиваются безопасные информационные структура и взаимодействия.

На рисунке 1 приведен пример соответствующего требованиям приказа № 66 типового решения по обеспечению ЗИ в части управления информационными потоками в локальной вычислительной сети (далее – ЛВС) ПС. В соответствии с регламентирующими документами Министерства энергетики Республики Беларусь ЛВС должна состоять из двух сегментов: технологического сегмента (далее –

ТС), в котором развертываются АСУ ТП, автоматизированная система контроля и учёта энергоресурсов (далее – АСКУЭ), автоматизированная система диспетчерского управления (далее – АСДУ), система контроля, защиты и управления (далее – СКЗУ), релейная защита и автоматика (далее – РЗА) и т.п., и корпоративного сегмента (далее – КС), в котором развертываются системы управления деятельностью предприятия.

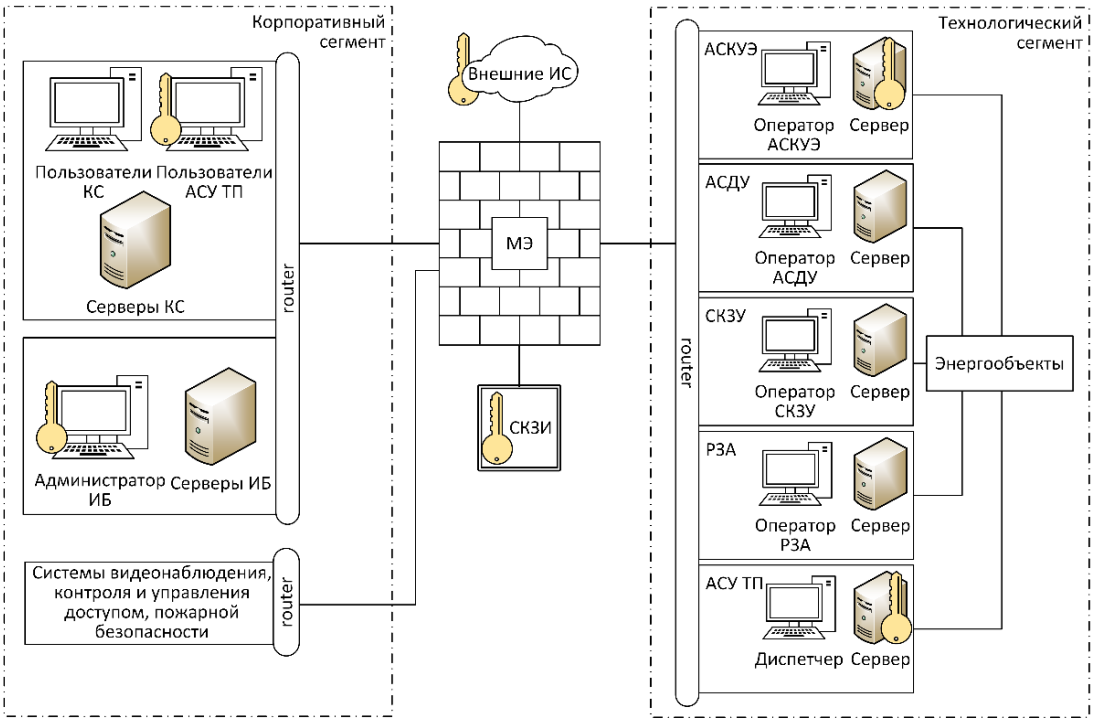

Рисунок 1. – Применение средств защиты информации для управления информационными потоками в ЛВС ПС

Видно, что объединение объектов АСУ ТП, АСКУЭ, АСДУ, СКЗУ, РЗА может быть реализовано посредством одного (или нескольких) неуправляемого сетевого оборудования (router). В этом случае для решения задач управления внешними и внутренними информационными потоками используется один (реже два дублирующих друг друга) сертифицированный по требованиям ЗИ межсетевой экран (далее – МЭ), который потенциально является единой точкой отказа при кибератаках. При этом, впоследствии в рамках реконструкции возникает необходимость создания информационных потоков между автоматизированными рабочими местами (далее – АРМ), подключаемыми дистанционно из КС к объектам ТС. Соответственно, появляются дополнительные угрозы ИБ вследствие изначального выбора подхода к проектированию структуры ИС без учета фактора ИБ. Наличие таких АРМ в КС ЛВС, реализованной по приведенной на рисунке 1 архитектуре, несет риски реализации угроз информации телеуправления. В таких случаях для устранения уязвимостей архитектуры, а также для выполнения требования сегментации сети

на КС и ТС используется средство криптографической ЗИ (далее – СКЗИ, на схеме обозначены как объект «ключ»). Вместе с тем, применение СКЗИ снижает эффективность систем обнаружения и предотвращения вторжений (IDS/IPS) и может повышать нагрузку на МЭ.

В этой связи необходимы практики по уменьшению количества автоматически появляющихся уязвимостей по результатам проектирования (строительства) АСУ ТП, что позволит снизить издержки внедрения и эксплуатации СЗИ и СИБ за счет верных проектных решений. Такие практики должны содержать минимальные наборы требований к созданию безопасных архитектур ЛВС, на базе которых будет функционировать АСУ ТП (например, в виде шаблонов) и требований по реализации встроенных механизмов безопасности (требования к обеспечению конфиденциальности, целостности, доступности, сохранности и подлинности обрабатываемой информации) при разработке прикладного ПО. Описанному безопасному подходу эксперты в области ИБ дали название «Secure by design» и трактуют как интеграцию свойств безопасности в будущий продукт (ИС) наравне с функциональными требованиями, основные шаблоны подхода изложены в [4]. Вопросам стандартизации безопасных архитектур посвящено руководство «Кибербезопасность для систем промышленной автоматизации и контроля» [5], рекомендованное для использования при автоматизации ПС.

На рисунке 2 приведена более безопасная к угрозам ИБ архитектура ЛВС ПС. Объекты каждой системы ТС объединены посредством отдельного сетевого оборудования. Для целей снижения угроз несанкционированного воздействия на механизмы безопасности и ЛВС, ТС и КС имеют собственные МЭ и серверы ИБ, а политики разграничения доступа настраиваются из двух центров принятия решений. Для взаимодействия между ТС и КС используется демилитаризованная зона (DMZ), что позволяет уменьшить количество угроз, связанных с эксплуатацией уязвимостей прикладного ПО АСУ ТП. Инспекция пропускаемого трафика осуществляется на МЭ прозрачным способом, так как не используются СКЗИ внутри ЛВС. Предложенный подход к сегментации ЛВС позволяет обеспечить приемлемую взаимную изоляцию ТС и КС в условиях кибератак на информационную инфраструктуру ПС.

Согласно регламентирующих документов Министерства энергетики Республики Беларусь, информация телеуправления АСУ ТП относится к информации, распространение и (или) предоставление которой ограничено, соответственно, необходимо выполнение требований приказа № 66. Помимо применения сертифицированных средств ЗИ, целесообразно встраивать механизмы безопасности в прикладное ПО АСУ ТП: идентификация и аутентификация пользователей, реализация политик управления доступом к активам АСУ ТП, обеспечение конфиденциальности сигналов телеуправления, контроль целостности информации, информационных процессов и прикладного ПО АСУ ТП.

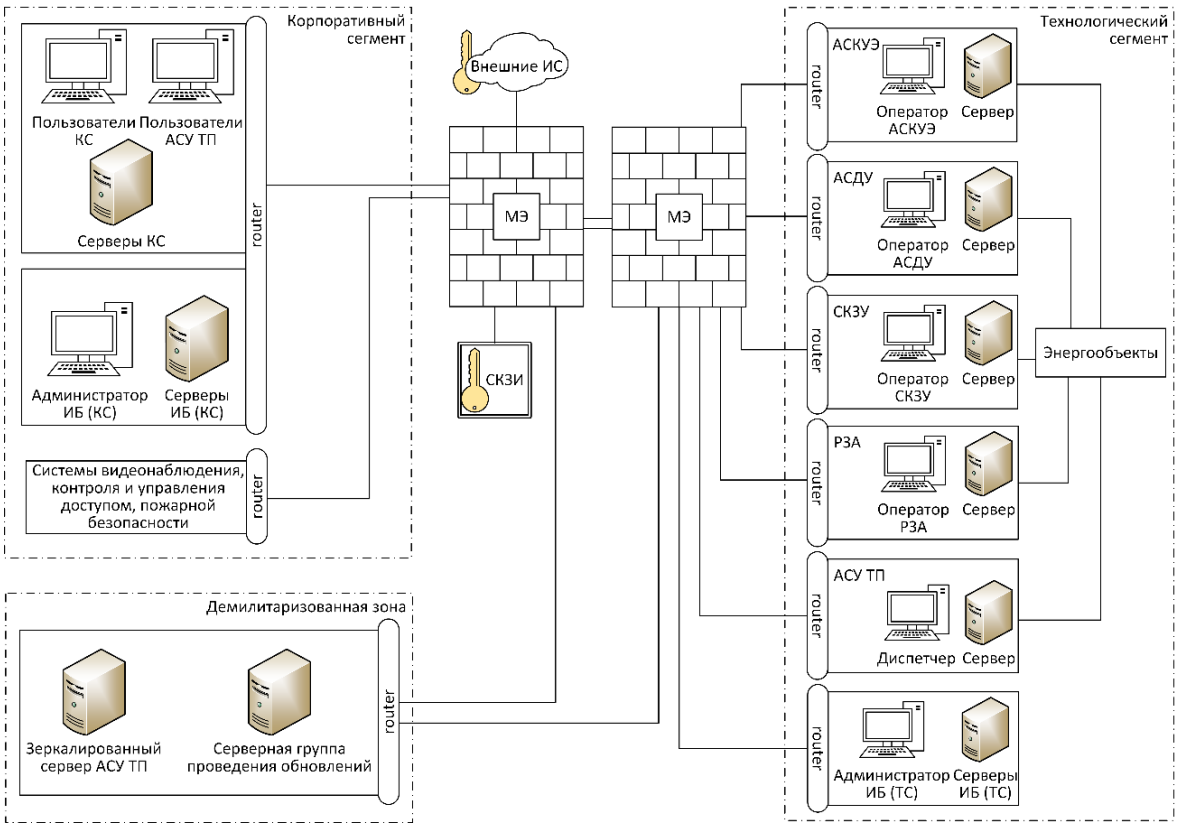

Рисунок 2. – Безопасная архитектура ЛВС ПС

Использование концепции Secure by design для проектирования безопасной архитектуры ЛВС и встроенных механизмов ЗИ в промышленных системах автоматизации представляется наиболее перспективно с позиции соблюдения баланса между обеспечением функциональной надежности и безопасности ПС и кибербезопасностью ее информационной инфраструктуры, а также позволяет поддерживать на необходимом уровне показатели пропускной способности ЛВС, быстродействия сетевых протоколов и доступности информационных процессов (сервисов).

ЛИТЕРАТУРА

1. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем: ГОСТ Р 56546-2015. – Введ. 01.04.2016. – М.: Стандартинформ, 2018. – 12 с.
2. Концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости / А. О. Ефимов [и др.] // Безопасность информационных технологий. – 2023. – Т. 30, № 2. – С. 63–79.
3. Федеральная служба по техническому и экспортному контролю России [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/vul. – Дата доступа: 20.02.2024.
4. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems / H. Adkins [et al.]. – O'Reilly Media, 2020. – 555 p.
5. Cyber Security for Industrial Automation and Control Systems (IACS) [Electronic resource]. – Mode of access: https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf. – Date of access: 20.02.2024.