Научная статья / Research Article
УДК 621.316

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ КАНАЛОВ СВЯЗИ РЕКЛОУЗЕРОВ В РАСПРЕДЕЛИТЕЛЬНЫХ СЕТЯХ 10 кВ

С.С. Зарецкий[1] , С.С. Зарецкий [2]
[1]Красноярский государственный аграрный университет, Россия, 660049, Красноярск, пр. Мира, 90
[2]Сибирский федеральный университет, Россия, Красноярск, пр. Свободный, 79.

Аннотация. *Статья посвящена актуальной проблеме обеспечения кибербезопасности каналов связи реклоузеров в распределительных сетях 10 кВ. Осуществлен анализ современных подходов к протоколам МЭК 61850 и МЭК 60870-5-104, которые являются основой для диспетчеризации реклоузеров, обладают встроенными уязвимостями, связанными с отсутствием шифрования и недостаточной аутентификацией, что создаёт риски несанкционированного доступа и нарушения управления. Сделан обзор нормативных требований. Определен комплекс технических мер, который должен включать: организацию шифрованных VPN-туннелей (с применением TLS или MACsec для защиты канала «последний метр»); внедрение аутентификации на основе DNP3-SA v5 или цифровых сертификатов; сегментацию сети с использованием межсетевых экранов; создание системы управления криптографическими ключами и регулярное проведение пенетрационного тестирования. Дальнейшие исследования в данной области целесообразно направить на разработку систем обнаружения вторжений, специализированных для протоколов МЭК 61850, а также на адаптацию требований постквантовой криптографии для оборудования реклоузеров.*

Ключевые слова: *реклоузер, канал связи, кибербезопасность, система управления.*

ENSURING CYBERSECURITY OF COMMUNICATION CHANNELS OF RECLOSERS IN 10 kV DISTRIBUTION NETWORKS

S.S. Zaretsky [1], S.S. Zaretsky[2]
[1]Krasnoyarsk agrarian university, Russia, 660049, Krasnoyarsk, av. Mira, 90
[2]Siberian Federal University, pr. Free, 79, Krasnoyarsk, Russia.

Инженерные системы и энергетика. 2026. № 2. С. 24–33.
Engineering systems and energy. 2026;(2):24-33.

Abstract. *The article is devoted to the urgent problem of ensuring cybersecurity of recloser communication channels in 10 kV distribution networks. An analysis of modern approaches to the IEC 61850 and IEC 60870-5-104 protocols was carried out, which are the basis for dispatching reclosers, have built-in vulnerabilities associated with the lack of encryption and insufficient authentication, which creates risks of unauthorized access and control violations. An overview of regulatory requirements was made. A set of technical measures has been defined, which should include: the organization of encrypted VPN tunnels (using TLS or MACsec to protect the "last meter" channel); Implement DNP3-SA v5 or digital certificate based authentication Network segmentation using firewalls creation of cryptographic key management system and regular penetration testing. Further research in this area is advisable to focus on the development of intrusion detection systems specialized for IEC 61850 protocols, as well as on adapting the requirements of post-quantum cryptography for equipment of reclausers.*

Key words: *recloser, communication channel, cybersecurity, control system.*

Введение. В процессе цифровой трансформации электроэнергетики одним из ключевых направлений повышения надёжности распределительных сетей 10 кВ является внедрение интеллектуальных коммутационных аппаратов - реклоузеров. Данные устройства обеспечивают автоматическое секционирование, локализацию повреждений и восстановление электроснабжения, а также дистанционное управление из диспетчерских центров. Переход от распределительных сетей как закрытых систем к высокоинтегрированной и взаимосвязанной среде неизбежно влечёт за собой расширение поверхности атак и появление новых уязвимостей, которые требуют должного внимания.

Полевые устройства (реклоузеры) работают в реальном времени и непосредственно влияют на выполнение коммутационных операций. Нарушение безопасности в таких системах способно привести не только к утечке данных, но и к некорректному поведению устройств, включая несанкционированные отключения или отказ в выполнении команд управления. В этой связи задача обеспечения безопасности каналов связи реклоузеров является критически важной для поддержания надёжности и устойчивости электроснабжения [1].

Целью работы был анализ угроз и уязвимостей каналов связи реклоузеров и обоснование комплекса технических мер по защите информационного обмена между реклоузерами и диспетчерскими пунктами.

1. Анализ уязвимостей протоколов связи реклоузеров. Основу информационного обмена в системах диспетчеризации реклоузеров составляют промышленные протоколы передачи данных, среди которых наиболее широкое распространение получили протоколы МЭК 60870-5-104 и МЭК 61850, а также в ряде случаев Modbus. Указанные протоколы были разработаны с акцентом на надёжность и оперативность передачи

данных, однако вопросы кибербезопасности на начальных этапах их создания не были в полной мере учтены.

Уязвимости протокола МЭК 61850. Стандарт МЭК 61850 определяет профили протоколов, модели данных и абстрактные сервисные определения для связи между интеллектуальными электронными устройствами (IED), поддерживая их взаимодействие в единой Ethernet-среде [1-2]. Однако исследователями идентифицирован ряд уязвимостей данного стандарта, включая отсутствие шифрования в GOOSE-сообщениях, недостаточную реализацию систем обнаружения вторжений и отсутствие встраиваемых межсетевых экранов внутри сети подстанции. Используя эксплойты этих уязвимостей, злоумышленники могут осуществлять как атаки «отказ в обслуживании» (DoS), так и атаки с учётом особенностей мультикастной рассылки сообщений GOOSE. Потенциальные последствия - от нецелевых срабатываний автоматики до полного нарушения управления распределительной сетью. Существенным недостатком является также то, что любые управляющие команды могут быть скомпрометированы через открытые каналы, что подразумевает необходимость их независимой проверки корректности IED [2].

Уязвимости протоколов МЭК 60870-5-104 и Modbus. Протокол МЭК 60870-5-104, широко применяемый для обмена телеметрическими данными между диспетчерскими пунктами и полевыми устройствами, также не содержит встроенных механизмов аутентификации и шифрования. При передаче данных по открытым сетям (включая сети общего пользования с использованием GPRS/4G) возникает риск перехвата и подмены сообщений [3].

Критически значимым является тот факт, что аутентификация является значительно более эффективной стратегией снижения рисков по сравнению с шифрованием: при атаке повторного воспроизведения (replay attack) злоумышленнику не требуется знать содержимое зашифрованного сообщения, чтобы вызвать нежелательное переключение. Реализация надёжной аутентификации на основе механизмов «запрос-ответ» и цифровых подписей закрывает один из главных векторов атак.

Векторы атак на канальном уровне (последний метр). Особую проблему представляет защита каналов связи на участке между реклоузером и маршрутизатором, так называемого «последнего фута». Типовой шкаф управления реклоузером содержит, помимо самого контроллера, сотовый маршрутизатор и короткий (около 30 см) Ethernet-кабель, соединяющий два устройства. В большинстве существующих реализаций трафик на этом участке передаётся в открытом виде (plain text). Физический взлом шкафа даёт злоумышленнику доступ к незащищённому сетевому трафику с возможностью его анализа, подмены или повторного воспроизведения. Данная уязвимость известна в индустрии как проблема «последнего фута (last foot)»[3-4].

2. Нормативно-правовая база обеспечения кибербезопасности в электроэнергетике Российской Федерации

В Российской Федерации сформирована система нормативного регулирования в области защиты критической информационной инфраструктуры (КИИ), к которой относятся объекты электроэнергетики.

Базовые требования: приказ ФСТЭК России № 239. Приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 года № 239 утверждены «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Документ регламентирует весь жизненный цикл защиты - от проектирования до вывода из эксплуатации - для значимых объектов КИИ, к которым относятся системы управления технологическими процессами в электроэнергетике. Сбой или разрушение таких объектов влечёт за собой тяжёлые потери, угрозы жизни и здоровью граждан, экономические риски.

Приказ устанавливает, что разработка мер защиты значимого объекта КИИ должна включать анализ угроз и разработку модели угроз, а внедряемые меры защиты не должны оказывать негативного влияния на функционирование самого объекта [5].

Дополнительные требования для электроэнергетики: приказ Минэнерго России № 1215. Приказом Министерства энергетики Российской Федерации от 26 декабря 2023 года № 1215 утверждены дополнительные требования по обеспечению безопасности значимых объектов КИИ, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием из диспетчерских центров.

Указанные требования:

- распространяются на дистанционное управление выключателями, разъединителями и устройствами релейной защиты и автоматики, что напрямую относится к системам диспетчеризации реклоузеров;
- предусматривают обеспечение защиты трафика команд дистанционного управления с использованием средств криптографической защиты информации;
- устанавливают необходимость организации взаимодействия технологических сетей связи с внешними сетями через межсетевой экран [5-6].

3. Международные стандарты кибербезопасности для реклоузеров. На международном уровне в области кибербезопасности энергетических систем ключевую роль играет серия стандартов IEC 62351, разработанная для повышения безопасности протоколов ТК 57 МЭК.

IEC 62351-3: обеспечение безопасности TCP/IP. Стандарт IEC 62351-3 (актуальная редакция 2023 года) определяет способы обеспечения конфиденциальности, целостности и аутентификации сообщений для протоколов, использующих TCP/IP в качестве транспортного уровня. В от-

личие от предыдущих редакций, настоящая версия является самодостаточной и полностью определяет профиль TLS, включая обязательные шифровальные наборы для TLSv1.2 и профиль TLSv1.3, применимый для энергетического сектора. Стандарт может применяться непосредственно для защиты каналов связи между реклоузерами и SCADA-системами [7].

IEC 62351-6: защита протоколов МЭК 61850. IEC 62351-6 устанавливает требования кибербезопасности для протокола МЭК 61850, включая защиту мультикастных сообщений GOOSE и SV, которые наиболее уязвимы в силу отсутствия в них встроенных механизмов безопасности.

IEC 62351-9: управление криптографическими ключами. IEC 62351-9:2023 (вторая редакция) определяет управление криптографическими ключами, преимущественно долгосрочными асимметричными ключами (публичные сертификаты и соответствующие закрытые ключи), а также симметричными ключами для групповой связи. Принципиальным отличием редакции 2023 года от предыдущей является введение компонентов сертификатов, верификации компонентов и поддержки постквантовой криптографии. Реализация управления ключами на основе IEC 62351-9 на объектах с реклоузерами позволяет создать инфраструктуру открытых ключей, обеспечивающую безопасную смену и отзыв ключей, что критически важно при большом количестве полевых устройств.

Стандарты IEC 62210 и NISTIR 7628. Помимо серии IEC 62351, важную роль играют технические отчёты (TR) серии IEC 62210, носящие в основном ознакомительный характер, однако требующие безусловного применения на практике. Ключевой ориентир для интегрированной оценки рисков - документ «Guidelines for Smart Grid Cybersecurity» (NISTIR 7628 Rev. 1), который представляет аналитическую основу для разработки эффективных стратегий кибербезопасности, учитывающих трансформацию энергосистемы от относительно закрытой к сложной и высокоинтегрированной среде [7-8].

4. Комплекс технических решений по защите каналов связи реклоузеров. На основе анализа угроз и нормативных требований может быть предложен комплекс организационно-технических мер.

Построение защищённых VPN-туннелей и сегментация сети. Базовым решением для защиты каналов связи реклоузеров при использовании сотовых сетей общего пользования является организация VPN-туннелей с шифрованием на базе протоколов TLS в соответствии с IEC 62351-3. Каждый реклоузер должен получать статический IP-адрес в корпоративной сети, а маршрутизатор на стороне поля должен устанавливать VPN-соединение с концентратором в диспетчерском центре. Для повышения отказоустойчивости в некоторых реализациях, например на оборудовании Cisco и SEL, совместно используемом в проектах распределённой автоматизации, применяется стандарт MACsec (IEEE 802.1AE) для шифрования трафика между контроллером реклоузера и маршрутизатором, что полностью закрывает уязвимость «последнего фута».

Взаимодействие технологических сетей связи с внешними сетями должно осуществляться через промышленные межсетевые экраны (Industrial Firewalls), обеспечивающие фильтрацию пакетов и реализующие функции DPI для контроля прикладных протоколов. Сегментация сети с помещением серверов сбора данных в защищённую DMZ-зону исключает прямой доступ к устройствам из внешних сетей [9].

Реализация аутентификации и обнаружение вторжений. Крайне важной мерой является внедрение полноценной аутентификации на протокольном уровне. Наиболее экономически эффективным на сегодняшний день представляется применение протокола DNP3 Secure Authentication версии 5 (DNP3-SA v5), который позволяет реализовать криптостойкую аутентификацию команд управления даже на устаревших системах, использующих последовательные интерфейсы связи. При такой архитектуре удалённое устройство (реклоузер) способно отличить легитимную команду от поддельной, что кардинально повышает устойчивость сети к кибератакам. Для систем, работающих по протоколу МЭК 61850, необходима реализация аутентификации на основе цифровых сертификатов в соответствии с IEC 62351-6 [10-11].

Управление криптографическими ключами и техническое обслуживание. Эффективность всех криптографических мер напрямую зависит от системы управления ключами, построенной в соответствии с IEC 62351-9:2023. Требуется внедрение централизованной PKI для генерации, распределения и отзыва сертификатов, используемых для аутентификации устройств и шифрования каналов. Каждый реклоузер должен быть оснащён аппаратным модулем безопасного хранения ключей.

Критически важным является требование непрерывного тестирования систем в течение всего жизненного цикла из-за постоянного развития киберугроз. Это подразумевает регулярное проведение пенетрационного тестирования каналов связи реклоузеров и анализа защищённости конфигураций. Все изменения в настройках устройств безопасности должны производиться только через авторизованные защищённые каналы с многофакторной аутентификацией персонала.

Заключение.

Проведённый анализ позволяет сделать следующие выводы:

1. Протоколы МЭК 61850 и МЭК 60870-5-104, являющиеся основой для диспетчеризации реклоузеров, обладают встроенными уязвимостями, связанными с отсутствием шифрования и недостаточной аутентификацией, что создаёт риски несанкционированного доступа и нарушения управления.

2. Российская нормативно-правовая база (приказы ФСТЭК № 239 и Минэнерго № 1215) устанавливает обязательные требования к защите каналов связи значимых объектов КИИ электроэнергетики, включая шифрование трафика команд дистанционного управления и применение межсетевых экранов.

3. Международные стандарты серии IEC 62351, в частности IEC 62351-3 для защиты TCP/IP, IEC 62351-6 для защиты МЭК 61850 и IEC 62351-9 для управления криптографическими ключами, обеспечивают методологическую основу для реализации комплексной защиты каналов связи реклоузеров.

4. Комплекс технических мер должен включать: организацию шифрованных VPN-туннелей (с применением TLS или MACsec для защиты канала «последний метр»); внедрение аутентификации на основе DNP3-SA v5 или цифровых сертификатов; сегментацию сети с использованием межсетевых экранов; создание системы управления криптографическими ключами и регулярное проведение пенетрационного тестирования.

5. Дальнейшие исследования в данной области целесообразно направить на разработку систем обнаружения вторжений, специализированных для протоколов МЭК 61850, а также на адаптацию требований постквантовой криптографии для оборудования реклоузеров.

Список литературы

1. Moyer M. Cybersecurity Analysis for Grid Edge Devices / Tampa Electric Company. - Режим доступа: https://electricityforum.com/ai/cybersecurity/cybersecurity-analysis (дата обращения: 06.05.2026).
2. A review of security attacks on IEC61850 substation automation system network / 2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA). - Режим доступа: https://ieeexplore.ieee.org/document/7066594 (дата обращения: 06.05.2026).
3. Addressing Cybersecurity in Distribution Network SCADA Systems // NOJA Power. - November 2019. - Режим доступа: https://www.nojapower.com.au/expertise/2019/addressing-cybersecurity-in-distribution-network-SCADA-systems (дата обращения: 06.05.2026).
4. NISTIR 7628 Rev. 1. Guidelines for Smart Grid Cybersecurity // National Institute of Standards and Technology. - September 2014. - Режим доступа: https://csrc.nist.rip/publications/detail/nistir/7628/rev-1/final (дата обращения: 06.05.2026).
5. Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «Гарант». - Режим доступа: https://base.garant.ru/71825540/ (дата обращения: 06.05.2026).
6. Стандарты IEC в сфере кибербезопасности энергетических систем // БелГИСС. - 03.10.2023. - Режим доступа: https://belgiss.by/standarty-iec-v-sfere-kiberbezopasnosti-energeticheskikh-sistem (дата обращения: 06.05.2026).
7. Приказ Министерства энергетики Российской Федерации от 26 декабря 2023 г. № 1215 «Об утверждении дополнительных требований по

обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике» // СПС «Гарант». - Режим доступа: https://base.garant.ru/409030964/ (дата обращения: 06.05.2026).
8. IEC 61850: Technology standards and cyber-threats / 2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST). - Режим доступа: https://www.infona.pl/resource/bwmeta1.element.ieee-art-000007555647 (дата обращения: 06.05.2026).
9. DIN EN IEC 62351-3:2024-10. Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP (IEC 62351-3:2023). - Режим доступа: https://www.din.de/en/wdc-beuth:din21:381948876 (дата обращения: 06.05.2026).
10. BAS EN IEC 62351-9:2025. Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment (IEC 62351-9:2023). - Режим доступа: https://ftp.isbih.gov.ba/sr/standard/342800 (дата обращения: 06.05.2026).
11. Secure the ‘last foot’ in distribution automation / Cisco Blogs. - 25.10.2022. - Режим доступа: https://blogs.cisco.com/industrial-iot/secure-the-last-foot-in-distribution-automation (дата обращения: 06.05.2026).

References

1. Moyer M. Cybersecurity Analysis for Grid Edge Devices / Tampa Electric Company. - Режим доступа: https://electricityforum.com/ai/cybersecurity/cybersecurity-analysis (дата обращения: 06.05.2026).
2. A review of security attacks on IEC61850 substation automation system network / 2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA). - Режим доступа: https://ieeexplore.ieee.org/document/7066594 (дата обращения: 06.05.2026).
3. Addressing Cybersecurity in Distribution Network SCADA Systems // NOJA Power. - November 2019. - Режим доступа: https://www.nojapower.com.au/expertise/2019/addressing-cybersecurity-in-distribution-network-SCADA-systems (дата обращения: 06.05.2026).

4. NISTIR 7628 Rev. 1. Guidelines for Smart Grid Cybersecurity // National Institute of Standards and Technology. - September 2014. - Режим доступа: https://csrc.nist.rip/publications/detail/nistir/7628/rev-1/final (дата обращения: 06.05.2026).
5. Order of the Federal Service for Technical and Export Control of December 25, 2017
No. 239 "On approval of the Requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation "//SPS" Garant. " - Access mode: https://base.garant.ru/71825540/ (access date: 06.05.2026).
6. IEC standards in the field of cybersecurity of energy systems//BelGISS. - 03.10.2023. - Access mode: https://belgiss.by/standarty-iec-v-sfere-kiberbezopasnosti-energeticheskikh-sistem (access date: 06.05.2026).
7. Order of the Ministry of Energy of the Russian Federation of December 26, 2023 No. 1215 "On approval of additional requirements for ensuring the safety of significant critical information infrastructure facilities operating in the electric power industry when organizing and implementing remote control of technological modes of operation and operational status of electric power facilities from dispatch centers of the subject of operational dispatch management in the electric power industry "//SPS" Garant. " - Access mode: https://base.garant.ru/409030964/ (access date: 06.05.2026).
8. IEC 61850: Technology standards and cyber-threats / 2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST). - Режим доступа: https://www.infona.pl/resource/bwmeta1.element.ieee-art-000007555647 (дата обращения: 06.05.2026).
9. DIN EN IEC 62351-3:2024-10. Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP (IEC 62351-3:2023). - Режим доступа: https://www.din.de/en/wdc-beuth:din21:381948876 (дата обращения: 06.05.2026).
10. BAS EN IEC 62351-9:2025. Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment (IEC 62351-9:2023). - Режим доступа: https://ftp.isbih.gov.ba/sr/standard/342800 (дата обращения: 06.05.2026).
11. Secure the 'last foot' in distribution automation / Cisco Blogs. - 25.10.2022. - Режим доступа: https://blogs.cisco.com/industrial-iot/secure-the-last-foot-in-distribution-automation (дата обращения: 06.05.2026).

Сведения об авторах.

Зарецкий Сергей Сергеевич, магистрант Красноярского государственного аграрного университета, электромонтер по обслуживанию подстанций

Филиала ПАО «Россети», Красноярского предприятия магистральных электрических сетей. E-mail: golda777@list.ru
Зарецкий Семен Сергеевич, студент политехнического университета ФГАОУ ВО «Сибирский федеральный университет»

Information about the authors
Zaretsky Sergey Sergeevich, master's student of the Krasnoyarsk State Agrarian University, electrician for servicing substations of the Branch of PJSC Rosseti, Krasnoyarsk enterprise of main electric networks. E-mail: golda777@list.ru
Zaretsky Semyon Sergeevich, student of the Polytechnic University of the Siberian Federal University