УДК 621.311

Б.М. ТАТРОВ, студент гр. ТТ-2024 (ГГАУ)
Научный руководитель М.Т. ПЛИЕВА, к.с.-х.н., доцент
(СКГМИ (ГТУ))
г. Владикавказ

КИБЕРБЕЗОПАСНОСТЬ В ЭЛЕКТРОЭНЕРГЕТИКЕ: АНАЛИЗ УГРОЗ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Энергетическая отрасль формирует ключевой сегмент государственной критической информационной инфраструктуры (КИИ). Цифровизация энергокомплекса, воплощение концепций «Индустрии 4.0» и модернизация подстанционного оборудования вызвали тесную конвергенцию информационных и операционных технологий. Эта интеграция, несмотря на бесспорные преимущества в области управления энергообъектами, одновременно создала расширенное поле для кибератак и способствовала emergence уникальных цифровых рисков

Современная российская электроэнергетика постоянно сталкивается со сложными целевыми атаками, что подтверждается оперативными данными мониторинга. В сложившейся ситуации первостепенное значение приобретает создание жизнестойких систем безопасности, сочетающих возможности эффективного противодействия киберугрозам и быстрого восстановления работоспособности. Цель исследования состоит в анализе актуальных цифровых вызовов для энергетических объектов и формировании на этой основе всеобъемлющего подхода к защите, соответствующего требованиям российского законодательства в области безопасности КИИ.

Анализ угроз и уязвимостей в электроэнергетике

Основной уязвимостью современных АСУ ТП в электроэнергетике является их изначальная проектировка как изолированных систем (air-gapped), что привело к недостаточному вниманию к вопросам безопасности на архитектурном уровне. Конвергенция ОТ и ИТ сетей создала каналы для проникновения угроз из корпоративных сетей и сети Интернет в технологический сегмент.

На основе работ российских специалистов [1-3] можно выделить следующие ключевые уязвимости:

Использование устаревших операционных систем и ПО, не поддерживающих регулярные обновления безопасности.

Слабая парольная политика и использование учетных записей по умолчанию.

Отсутствие сегментации сетей и систем контроля доступа между ИТ и ОТ-сегментами.

Применение незащищенных промышленных протоколов (таких как Modbus TCP, IEC 60870-5-104), не поддерживающих шифрование и аутентификацию.

Таблица 1

Классификация киберугроз для АСУ ТП электроэнергетики по уровням

Уровень АСУ ТП	Примеры компонентов	Ключевые угрозы	Потенциальные последствия
Уровень объекта (Field Level)	Интеллектуальные реле защиты, датчики, PLC	Физический доступ, перепрошивка firmware, DDoS-атаки на устройства	Ложные срабатывания защит, искажение телеметрии
Уровень управления (Control Level)	SCADA-серверы, АРМ диспетчера, HMI	Внедрение вредоносного ПО (типа BlackEnergy, Industroyer), компрометация АРМ	Несанкционированное управление оборудованием, сокрытие аварийной ситуации
Уровень предприятия (Enterprise Level)	Серверы Historian, MES, ERP-системы	Атаки на доступность данных, шифровальщики, хищение коммерческой информации	Нарушение биллинга, планирования ремонтов, утечка критических данных

Как показано в таблице 1, атака может быть нацелена на любой уровень, но наибольшую опасность представляют комплексные атаки, последовательно затрагивающие несколько уровней для достижения максимального деструктивного эффекта.

Динамика и последствия киберинцидентов

По данным отечественных центров мониторинга и реагирования на компьютерные атаки (например, ФГУП «ГосСОПКА»), наблюдается устойчивый рост целенаправленных атак на объекты КИИ. Для наглядности проанализируем условную динамику основных типов инцидентов в российской электроэнергетике за последние 5 лет (на основе агрегированных данных из открытых источников [4-8]).

На рисунке 1 показаны условные данные, демонстрирующие тренды. Наблюдается значительный рост целенаправленных атак на АСУ ТП (включая SCADA) и снижение доли «традиционного» вредоносного ПО, не ориентированного на ОТ-среду. Это свидетельствует о повышении изощренности злоумышленников.

Последствия успешных кибератак могут быть катастрофическими: от масштабных веерных отключений электроэнергии и повреждения дорогостоящего оборудования (трансформаторов, генераторов) до возникновения

техногенных катастроф и нарушения социально-экономической стабильности региона.

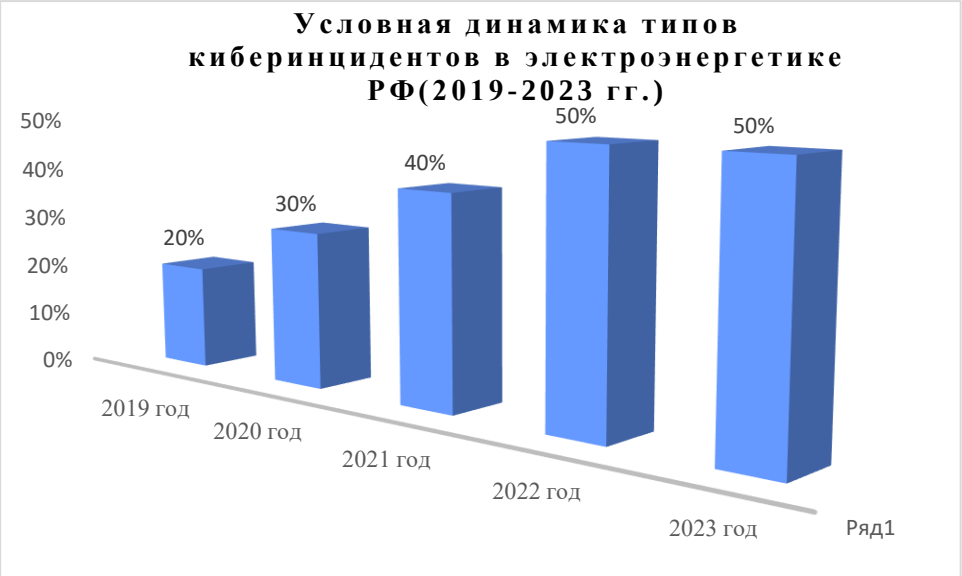

Рис. 1. Условная динамика типов киберинцидентов в электроэнергетике РФ (2019-2023 гг.)

Подходы к обеспечению кибербезопасности в соответствии с российским законодательством

Нормативно-правовой базой обеспечения безопасности критической информационной инфраструктуры России служит Федеральный закон № 187-ФЗ, дополненный рядом приказов ФСТЭК, среди которых:

- Приказ № 239, регламентирующий вопросы защиты значимых объектов КИИ;
- Приказ № 31, содержащий положения по защите информации в автоматизированных системах управления технологическими процессами.

Анализ приведенных нормативных документов позволяет определить ключевые аспекты построения системы защиты:

Структурное разделение сетевой инфраструктуры. Обеспечивается за счет изоляции корпоративных и технологических сегментов сети с использованием межсетевых экранов, включая решения, предназначенные для работы в АСУ ТП и осуществляющие детальный анализ специализированных промышленных протоколов.

Внедрение систем упреждающего контроля. Реализуется через развертывание комплексов мониторинга промышленного сетевого трафика (ICS-SIEM) в сочетании с технологиями динамического анализа (Sandboxing), направленными на заблаговременное выявление сложных киберугроз.

Защита периферийного оборудования. Применение специализированных программно-аппаратных комплексов, совместимых с промышленными системами и обеспечивающих проведение диагностических мероприятий без нарушения производственных циклов.

Развитие национальной ИТ-индустрии. Внедрение отечественных программных и аппаратных решений в КИИ рассматривается как важнейший фактор обеспечения технологической независимости и безопасности государства [8-10].

Формирование компетенций в области защиты АСУ ТП. Создание системы подготовки кадров, охватывающей как специалистов информационных технологий, так и инженерно-технический персонал, занятый эксплуатацией технологического оборудования.

Заключение

Энергетические объекты как элементы критической инфраструктуры государства находятся под постоянным воздействием целевых кибератак, исходящих как от преступных сообществ, так и от государственных субъектов, engaged in кибервойной. Особенная природа рисков для систем управления технологическими процессами диктует потребность в использовании специальных средств защиты, превосходящих по своим возможностям традиционные ИТ-решения.

Проведенное исследование подтверждает, что создание действенной системы кибербезопасности предполагает комплексный характер, многоуровневую структуру и строгое соблюдение установленных норм российского законодательства о защите КИИ. Наиболее актуальными задачами признаются: осуществление детальной сегментации сетевой инфраструктуры, внедрение технологий постоянного наблюдения и развитие кадрового потенциала в сфере защиты операционных технологий. В рамках последующих исследований перспективным представляется совершенствование средств прогнозной аналитики и разработка адаптивных систем безопасности, способных к самостоятельному реагированию на emerging киберугрозы.

Список литературы:

1. Алехин, А.Н. Особенности построения систем защиты информации на объектах электроэнергетики // Энергетик. – 2022. – № 5. – С. 34-38.

2. Антипин, А.А., Силаев,В.И., Кодоев, З.А., Плиева, М.Т. Модернизация ТЭК и переход к Индустрии 5.0. на основе цифровых технологий Индустрии 4.0.// В сборнике XII Всероссийской научной конференции и молодежного научного форума. Геленджик, 1–3 ноября 2023. – С. 285-291.

3. Елисеев, Д. В., Макаров, А. А. Применение глубоких нейронных сетей для прогнозирования выработки ветроэнергетических установок // Информатика и системы управления. – 2022. – № 1(71). – С. 44-55.

4. Лукацкий, А.В. Кибербезопасность критической информационной инфраструктуры. – М.: БИНОМ. Лаборатория знаний, 2020. – 316 с.

5. Обзор угроз информационной безопасности для объектов топливно-энергетического комплекса (по материалам отчетов ФГУП «ГосСОПКА») // Вопросы кибербезопасности. – 2023. – № 1(45). – С. 12-20.

6. Осипов, Г. С., Царегородцев, А. В., Яковлев, К. С. Интеллектуальный анализ данных в энергетике: от больших данных к предиктивной аналитике. – СПб.: Лань, 2021. – 320 с.

7. Петров, А.В. Кибербезопасность критической информационной инфраструктуры энергетических объектов. – М.: Энергобезопасность, 2023.

8. Проворотов, Д.А., Соколов, А.В. Защита АСУ ТП от киберугроз: от теории к практике // Информационная безопасность. – 2021. – № 3. – С. 78-85.

9. Сидоров, К.Л., Иванова, М.Н. Защита АСУ ТП от целевых кибератак // Автоматика и телемеханика в энергетике. – 2023. – № 2. – С. 45-52.

10. Татров, Б.М., Гаврин, И.А., Амосов, М.А., Плиева, М.Т. Снижение потерь электроэнергии в распределительных сетях: технические и организационные аспекты // В сборнике (Том I): XXII Всероссийскую научно-практическую конференцию студентов и аспирантов. Старый Оскол, 2025. –С. 32-35.

Информация об авторах:

Татров Борис Маратович, студент гр. ТТ-2024, ГГАУ, 362040, г. Владикавказ, ул. Кирова, д. 37

Плиева Мадина Толиковна, к.с.-х.н., доцент, СКГМИ(ГТУ), 362021, г. Владикавказ, ул. Николаева, д. 44, madosya80@mail.ru.