Второй блок – предотвращение атак. Внедрение шифрования каналов связи и строгой аутентификации пользователей снижает риск перехвата и подмены команд. Практика показывает, что даже внедрение простых механизмов TLS и VPN значительно повышает уровень защиты. Эффективным средством становится сегментация сети: выделение технологической части инфраструктуры и ограничение взаимодействия с внешними системами через строго контролируемые шлюзы. Здесь же находит применение концепция Zero Trust, при которой даже внутренние узлы не считаются априори доверенными, а каждый запрос проходит проверку.

Кроме того, в промышленной кибербезопасности применяются количественные методы оценки риска. Оценка риска определяется по формуле

$$R = PI,$$

где R – риск; P – вероятность реализации угрозы, I – потенциальный ущерб (Impact). Такой подход позволяет приоритизировать ресурсы, например атака с низкой вероятностью, но высоким ущербом (вывод из строя электростанции) будет иметь приоритет выше, чем частая, но малозначительная угроза.

Не менее важно внедрение средств реагирования и восстановления. Полностью предотвратить атаки невозможно, но можно минимизировать ущерб. Регулярные резервные копии конфигураций, заранее подготовленные планы реагирования и отработанные сценарии переключения на резервные каналы связи позволяют быстрее восстанавливаться после инцидента. Опыт многих компаний показывает, что именно готовность к инцидентам определяет реальные потери, а не только уровень применяемых защитных технологий.

Отдельно стоит подчеркнуть роль стандартизации. Международные документы, такие как IEC 62443, задают рамки по обеспечению безопасности для промышленных систем. Их требования включают управление уязвимостями, контроль доступа, управление изменениями, аудит действий операторов. Следование этим стандартам обеспечивает единый уровень безопасности на всех этапах жизненного цикла – от проектирования до эксплуатации.

Таким образом, методы обнаружения и предотвращения кибератак на системы телемеханики и SCADA должны представлять собой не набор разрозненных решений, а целостную стратегию. Она включает мониторинг и анализ трафика, применение аномалийных и сигнатурных детекторов, организацию защищённых каналов связи, сегментацию сетей и постоянную готовность к инцидентам. Только сочетание технических, организационных и нормативных мер способно обеспечить устойчивость систем, которые лежат в основе современной инфраструктуры. Безопасность SCADA – это не вопрос отдельного продукта или технологии, а непрерывный процесс, в котором должны участвовать как инженеры, так и специалисты по кибербезопасности.

Список литературы

1 **Bhamare, D.** Cybersecurity for Industrial Control Systems: A Survey / D. Bhamare, M. Zolanvari, A. Erbad [et al.] // Computers & Security. – 2020. – Vol. 89. – Article 101677. – DOI: 10.1016/j.cose.2019.101677.

2 **Аметов, Ф. Р**. Формализация защищённой коммуникации SCADA / Ф. Р. Аметов // eLIBRARY.RU. – 2021. – URL: https://www.elibrary.ru/item.asp?id=47462847 (дата обращения: 14.09.2025).

УДК 004.056:621.311.1

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ПРОЕКТА ВНЕДРЕНИЯ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

С. Ю. ВОРОБЬЁВ, Е. А. ХАНЧЕВСКИЙ

Научно-исследовательское и проектно-изыскательское республиканское унитарное предприятие «Белэнергосетьпроект», г. Минск, Республика Беларусь

Набором общепризнанных международным сообществом требований и лучших практик, предъявляемых к системам менеджмента информационной безопасности (далее – СМИБ), является серия стандартов ISO/IEC 270xx, принятая Международной организацией по стандартизации ISO

(International Organization for Standardization). После проведения мероприятий по переводу и терминологической адаптации Государственным комитетом по стандартизации Республики Беларусь данные технические нормативные правовые акты были введены в действие (по содержанию и смысловой нагрузке они полностью идентичны стандартам ISO). В национальной системе стандартизации действуют следующие из них:

– СТБ ISO/IEC 27000-2024 «Информационные технологии. Методы обеспечения безопасности. Общий обзор и словарь» – представляет собой обзор СМИБ, а также терминологическую базу связанных с ними терминов [1];

– СТБ ISO/IEC 27001-2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования» (далее – СТБ ISO/IEC 27001) – по сути является основным стандартом данной серии и устанавливает требования к разработке, внедрению, поддержанию и постоянному улучшению СМИБ [2];

– СТБ ISO/IEC 27002-2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью» – предназначен для использования при разработке руководства по менеджменту ИБ в конкретных отраслях и организациях с учетом их специфики [3];

– СТБ ISO/IEC 27003-2014 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности» – описывает процессный подход по определению и разработке СМИБ от начала до фактического завершения проекта [4];

– СТБ ISO/IEC 27004-2014 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения» – представляет собой руководство по разработке и применению мер измерения и проведению процесса измерения внедренной СМИБ [5];

– СТБ ISO/IEC 27005-2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по менеджменту рисков информационной безопасности» – описывает механизм реализации выполнении требований, касающихся действий по рассмотрению рисков ИБ и менеджмента рисков ИБ [6].

Внедрение СМИБ в деятельность предприятия, структурно входящего в ГПО «Белэнерго» Министерства энергетики Республики Беларусь (далее – Предприятие), имело под собой следующие основания:

– укрепление деловой репутации как высоконадежной организации, применяющей в своей деятельности наилучшие общепризнанные практики ИБ;

– выполнение требований законодательства в сфере лицензирования для получения лицензии на осуществление деятельности в сфере технической и криптографической защиты информации по проектированию, созданию и аудиту систем ИБ критически важных объектов информатизации [7].

По результату реализации проекта внедрения СМИБ в деятельность Предприятия представилось возможным сформулировать следующие выводы.

1 Следование методологии СТБ ISO/IEC 27001 позволило определить цели внедрения СМИБ в деятельность Предприятия, заинтересованные стороны, участников проекта и сроки реализации.

2 В реализацию проекта был вовлечен весь персонал Предприятия: от директора до специалиста, что способствовало выделению необходимых материальных ресурсов в достаточном количестве, своевременной и качественной актуализации локальной правовой базы, внесению изменений и дополнений в должностные инструкции работников, повышению осведомленности последних по вопросам ИБ.

3 В соответствии с требованиями нормативных актов Президента Республики Беларусь [8, 9] на базе РУП «Национальный центр обмена трафиком» и Национального центра защиты персональных данных Республики Беларусь кроме специалистов, обеспечивающих ИБ, было осуществлено повышение квалификации персонала по вопросам технической и криптографической защиты информации от заместителя директора Предприятия до специалистов структурных подразделений.

4 При осуществлении работы по подбору и изучению соискателей на вакантные должности Предприятия осуществляется тщательное изучение профессиональных, этических качеств, а также гражданской ответственности и законопослушности кандидатов.

5 Парадигма применения в СМИБ законодательных, нормативных и договорных требований позволяет гибко и адаптивно выстраивать локальную правовую базу, регулирующую вопросы ИБ, в том числе путем имплементации требований национального законодательства.

6 Реализацией проекта внедрения СМИБ процесс поддержания надлежащего уровня ИБ в организации не заканчивается (методологией СМИБ предусмотрены систематические мероприятия по переоценке рисков ИБ и проведения внутренних аудитов на соответствие требованиям СТБ ISO/IEC 27001).

7 Подтверждение соответствия требованиям СТБ ISO/IEC 27001 в Национальной системе соответствия Республики Беларусь СМИБ, внедренной в деятельность Предприятия, позволит получить лицензию на право выполнения работ по проектированию, созданию и аудиту систем ИБ критически важных объектов информатизации, а также укрепить деловую репутацию и инвестиционную привлекательность.

Список литературы

1 Информационные технологии. Методы обеспечения безопасности. Общий обзор и словарь : СТБ ISO/IEC 27000-2024. – Введ. 25.10.2024 (с отменой на территории РБ СТБ ISO/IEC 27000-2012). – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. – 23 с.

2 Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования : СТБ ISO/IEC 27001-2024. – Введ. 25.10.2024 (с отменой на территории РБ СТБ ISO/IEC 27001-2016). – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. – 19 с.

3 Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью : СТБ ISO/IEC 27002-2024. – Введ. 25.10.2024 (с отменой на территории РБ СТБ ISO/IEC 27002-2012). – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. – 132 с.

4 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности : СТБ ISO/IEC 27003-2014. – Введ. 14.08.2014. – Минск : Науч.-исслед. ин-т техн. защиты информации. – 59 с.

5 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения : СТБ ISO/IEC 27004-2014. – Введ. 14.08.2014. – Минск : Науч.-исслед. ин-т техн. защиты информации. – 53 с.

6 Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по менеджменту рисков информационной безопасности : СТБ ISO/IEC 27005-2024. – Введ. 25.10.2024 (с отменой на территории РБ СТБ ISO/IEC 27005-2012). – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. – 56 с.

7 О лицензировании : Закон Респ. Беларусь от 14 окт. 2022 г. № 213-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 10.09.2025).

8 О киберобезопасности : Указ Президента Респ. Беларусь, 14 февр. 2023 г., № 40 // ЭТАЛОН : информ.-поисковая система (дата обращения: 10.09.2025).

9 О некоторых мерах по совершенствованию защиты информации : Указ Президента Респ. Беларусь, 16 апр. 2013 г., № 196 : в ред. Указа Президента Респ. Беларусь от 09.12.2019 г. // ЭТАЛОН : информ.-поисковая система (дата обращения: 10.09.2025).

УДК 621.314

ДИАГНОСТИКА ПРЕДОТКАЗНОГО СОСТОЯНИЯ ТРАНСФОРМАТОРОВ НА ОСНОВЕ ЧАСТОТНОГО АНАЛИЗА

И. Л. ГРОМЫКО
Белорусский государственный университет транспорта, г. Гомель

Для диагностики неисправностей трансформаторов в настоящее время существует много различных методов. В качестве информативных параметров используются частичные разряды, анализ растворенного газа, спектроскопия, индекс поляризации, коэффициент диэлектрической проницаемости [1], сопротивление изоляции, измерение напряжения восстановления, ток поляризации и деполяризации, анализ частотных характеристик (*frequency response analysis* – FRA) и др. В последнее время FRA привлекают всё больше внимания для обнаружения механических повреждений из-за его высокой чувствительности к деформациям обмоток трехфазных трансформаторов [2].

Для проведения частотного анализа использован метод трех вольтметров. Схемы подключения задающего генератора сигналов и вольтметров для опытов холостого хода и короткого замыкания приведены на рисунке 1.