Следует особо подчеркнуть, что метод сохраняет свою актуальность даже при изменении тактик социальной инженерии, так как позволяет оперативно адаптировать весовые коэффициенты и параметры оценки. Это делает его универсальным инструментом для обеспечения корпоративной безопасности в условиях постоянно эволюционирующих угроз.

Список литературы

1 Verizon. 2023 Data Breach Investigations Report – 2023. – 95 p. – URL: https://www.researchgate.net/publication/371445421_DBIR_2023_Data_Breach_Investigations_Report_10K_20K_30K_About_the_cover (date of access: 27.12 2024).

2 **Чалдини, Р.** Психология влияния / Р. Чалдини ; пер. с англ. А. Миронова. – 5-е изд. – СПб. : Питер, 2021. – 336 с.

УДК 51-7

МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК НА СИСТЕМЫ ТЕЛЕМЕХАНИКИ И SCADA

Д. Н. ВОЛОДИН
Саратовский государственный технический университет им. Гагарина Ю. А., Российская Федерация

Современные системы телемеханики и SCADA являются ключевыми элементами инфраструктуры в энергетике, транспорте, промышленности и других критически важных отраслях. Их главная задача – управление технологическими процессами в реальном времени, что предполагает высокие требования к надёжности и отказоустойчивости. Но именно эти системы в последние годы всё чаще становятся объектом целенаправленных кибератак. Причины понятны: вывод из строя такой системы способен вызвать не только экономический ущерб, но и серьёзные социальные и экологические последствия.

Уязвимость SCADA-систем во многом связана с их историческим наследием. Первые поколения таких решений проектировались в условиях изолированных сетей, без учёта современных требований к информационной безопасности. Используемые протоколы – Modbus, DNP3, IEC 60870-5-104 – изначально не предполагали встроенную аутентификацию или шифрование. При подключении этих систем к корпоративным и внешним сетям возникла новая поверхность атаки, которой активно пользуются злоумышленники. Известные примеры, такие как Stuxnet или BlackEnergy, когда вредоносное ПО прямо воздействовало на оборудование автоматики, показали классические средства защиты корпоративных ИТ-сетей не всегда применимы к телемеханике, где главная ценность – непрерывность технологического процесса.

Для повышения безопасности критически важно использовать комплексный подход. Первый блок – это методы обнаружения атак. На практике применяются два основных направления: сигнатурные и поведенческие. Сигнатурные системы базируются на базе известных образцов атак и позволяют быстро выявлять повторяющиеся сценарии. Их слабость – невозможность противостоять новым, ещё не описанным угрозам. Поведенческие методы опираются на анализ аномалий в трафике и работе устройств. Например, внезапное увеличение числа команд на включение или резкое отклонение телеметрии от статистических норм могут быть сигналом о вторжении.

Для формализации подобных методов часто применяется энтропия Шеннона, которая измеряет уровень неопределённости в сетевом трафике:

$$H(X) = \sum_{i=1}^{n} p(x_i)\log_2 p(x_i),$$

где $p(x_i)$ – вероятность появления события x_i (например, определённого типа пакета). При резких изменениях энтропии сетевого трафика система может зафиксировать подозрительное поведение.

Современные подходы используют и машинное обучение: строятся модели нормальной работы устройств, после чего вычисляется ошибка прогноза. Если она превышает заданный порог ε, генерируется тревога:

$$\left| y_{\text{real}} - y_{\text{pred}} \right| > \varepsilon.$$

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