2) проверка целостности и аутентичности данных выполняется в основном программно с использованием оптимизированных алгоритмов, что минимизирует задержки в цикле управления;

3) системы мониторинга ИБ интегрируются с подсистемами самодиагностики ФБ, формируя единое пространство управления рисками;

4) совместная реализация позволяет снизить интенсивность опасных отказов вида (технический отказ + кибервоздействие) до уровня порядка 10^{-9} 1/ч.

Автоматизированные системы управления ответственными технологическими процессами железнодорожного транспорта являются фундаментом безопасного функционирования всей отрасли. Их архитектура сочетает дублированные каналы управления, принципы fail-safe и механизмы киберзащиты.

Функциональная безопасность достигается дублированием, диагностикой и контролем целостности, а информационная – сегментацией, шифрованием, CRC-контролем и мониторингом событий. Современные тенденции направлены на интеграцию этих направлений в единую платформу управления безопасностью, обеспечивающую устойчивость железнодорожной автоматики к техническим отказам и киберугрозам.

Список литературы

1 **Бочков, К. А.** Оценка временных параметров функционирования микропроцессорных устройств связи с объектами систем железнодорожной автоматики и телемеханики / К. А. Бочков, С. Н. Харлап, Б. В. Сивко // Вестник БелГУТа: Наука и транспорт. – 2012. – № 2 (25). – С. 12–15.

УДК 004.056

ОЦЕНКА УЯЗВИМОСТИ ПЕРСОНАЛА К АТАКАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: НЕЧЕТКО-МНОЖЕСТВЕННЫЙ ПОДХОД

Д. В. ВЛАСЕНКО
Саратовский государственный технический университет им. Гагарина Ю. А., Российская Федерация

В условиях цифровой трансформации транспортной отрасли проблема защиты от кибератак с использованием социальной инженерии приобретает особую актуальность. До 74 % успешных кибератак связаны именно с человеческим фактором [1]. Транспортная инфраструктура относится к критически важным объектам, где он становится ключевым элементом системы безопасности. Успешность атак с использованием социальной инженерии на транспортные компании прежде всего связана с методами социальной инженерии, что обусловлено спецификой отрасли: высоким уровнем стресса, необходимостью оперативного принятия решений и сложными многоуровневыми коммуникациями. Вопреки всеобщему мнению эффективность этих атак зависит не только от уровня подготовки атакующего, но и от различных характеристик жертвы.

Американский психолог Роберт Чалдини в своей книге «Психология влияния» описывает шесть принципов влияния, которыми успешно пользуются мошенники во время своих атак. К ним относятся авторитет, привлекательность, срочность или дефицит, постоянство и последовательность, социальное доказательство, взаимность [2].

Современные подходы к обеспечению кибербезопасности в основном сосредоточены на технических средствах защиты. Эти методы зачастую не учитывают человеческий фактор, который остается наиболее уязвимым звеном в системе безопасности. Технические средства не могут полностью защитить от социальной инженерии, направленной на манипуляцию персоналом. Существующие системы обучения и тестирования сотрудников также имеют ограниченную эффективность, поскольку не учитывают индивидуальные особенности восприимчивости к манипуляциям.

Предложенная методология оценки уязвимости основана на аппарате теории нечетких множеств Заде. Математическая модель включает четыре ключевых компонента: возрастные характеристики, уровень образования, показатели цифровой грамотности и психологические особенности. Для каждого параметра разработаны функции принадлежности μ, отражающие степень уязвимости сотрудника:

– для возрастного фактора: μ_1 = 0,7 (18–30 лет), 0,4 (31–50 лет), 0,8 (50+ лет);

– для образовательного критерия: μ_2 = 0,3 (техническое образование), 0,6 (гуманитарное), 0,8 (среднее);

– для цифровой грамотности: μ_3 = 0,1 (90–100 % правильных ответов), 0,4 (60–89 % правильных ответов), 0,9 (<60 % правильных ответов);

– для психологической устойчивости: μ_4 = 0,3 (высокая), 0,6 (средняя), 0,9 (низкая).

Общий показатель уязвимости рассчитывается по формуле взвешенной суммы:

$$\mu = \sum_{i=1}^{n} \omega_i \mu_i, \quad (1)$$

где μ – общий показатель уязвимости; μ_i – нечеткий элемент со степенью принадлежности; ω_i – удельный вес элемента.

Удельный вес – это мера относительной важности каждого фактора в формировании общего уровня уязвимости сотрудника. Если говорить проще – насколько сильно каждый фактор влияет на итоговый риск.

Для данной модели было принято решение использовать следующий вес:

– 0,2 для возраста;

– 0,1 для образования;

– 0,3 для цифровой осведомленности;

– 0,4 для психологического фактора.

Это означает, что возраст вносит 20 % общего вклада в оценку пользователя. Этот фактор считается более значимым, чем образование (10 %), но меньшим, чем результат тестов (30 %). Самым весовым фактором для нашей модели является психологический фактор, ведь атаки с помощью социальной инженерии учитывают именно внутренние качества человека.

Выбор данных весовых коэффициентов основан на анализе статистики успешных атак и экспертных оценках специалистов по информационной безопасности. Особое внимание уделяется учету отраслевой специфики: для транспортных работников критически важными являются способность сохранять концентрацию в условиях стресса, умение быстро распознавать подозрительные ситуации и соблюдение установленных регламентов безопасности.

Для оценки психологического фактора в данной модели предлагается использование укороченного пятифакторного опросника личности (Большой пятерки). В рамках подхода учитываются четыре фактора из пяти: нейротизм, добросовестность, сотрудничество и открытость новому. Вклад экстраверсии же на фоне предыдущих особенностей является незначительным и не приводит к повышению точности, однако увеличивает сложность расчётов.

Итоговый показатель уязвимости рассчитывается по следующей формуле:

$$\mu_п = 0{,}4Н + 0{,}3(1 – Д) + 0{,}2(1 – С) + 0{,}1 – (1 – О), \quad (2)$$

где Н – значение нейротизма (чем выше показатель, тем больше уязвимость); Д – нормализованное значение добросовестности; С – нормализованное значение сотрудничества; О – нормализованное значение открытости новому.

Значения сотрудничества (1 – С), добросовестности (1 – Д) и открытости новому (1 – О) считаем обратными, поскольку высокие значения снижают показатель уязвимости. Весовые коэффициенты (0,4 для нейротизма, 0,3 для добросовестности, 0,2 для сотрудничества и 0,1 для открытости новому) отражают вклад каждого фактора в итоговую уязвимости.

Особенностью методологии является ее адаптивность: система позволяет настраивать весовые коэффициенты в зависимости от конкретной специализации и особенностей ее работы.

Тонкость данного метода также подтверждается тем, что возможно использование практически любого набора критериев, так или иначе подходящего под уязвимости человека атакам с использованием социальной инженерии.

Главными же преимуществами метода можно считать возможность тонкой настройки коэффициентов, наглядное представление результатов, простую интеграцию с корпоративными системами, простоту вычислений и внедрения.

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:

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