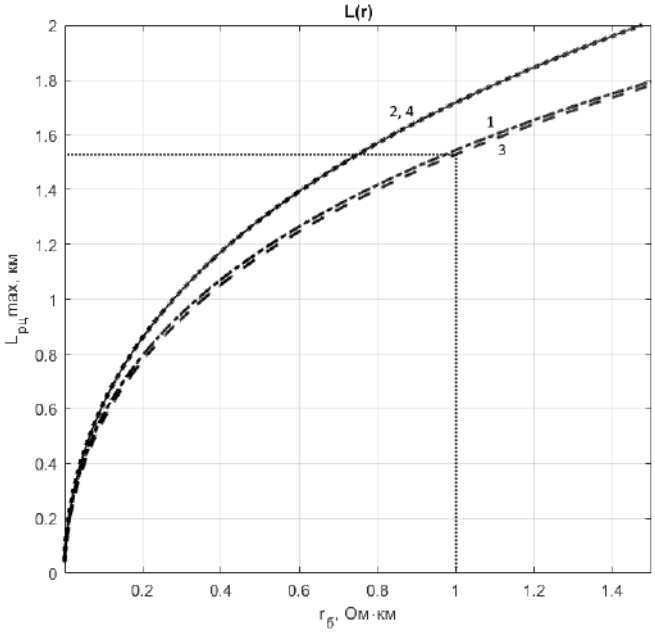

Рисунок 3 – Графики зависимости длины $l_{рл}$ от сопротивления изоляции $r_и$:
1 – $S_{пг(н)}$, *2* – $S_{пг(кз)}$, *3* – $k_н$, *4* – $k_{кз}$

Полученные графики дают возможность определить максимальную длину $l_{рл}$ при нормативном минимальном значении сопротивления изоляции $r_и$ = 1,0 Ом·км (при частоте несущих колебаний сигнала 420 Гц), которая составляет 1,529 км.

Список литературы

1 **Брылеев, А. М.** Теория, устройство и работа рельсовых цепей / А. М. Брылеев, Ю. А. Кравцов, А. В. Шишляков. – 2-е изд., перераб. и доп. – М. : Транспорт, 1978. – 344 с.

2 **Леушин, В. Б.** Определение максимальной длины рельсовой линии при нормативном минимальном значении величины сопротивления изоляции в функции частоты несущих колебаний сигнала рельсовой цепи / В. Б. Леушин, Л. Б. Смирнова, Р. Р. Юсупов // Автоматика на транспорте. – 2018. – Т. 4, № 4. – С. 505–519.

3 ТРЦ-ЭТ50 (АЛС 25,75)-С-96. Станционные рельсовые цепи тональной частоты с наложением АЛС 25 (75) Гц при электротяге переменного тока. – СПб. : ГТСС, 1996. – 57 с.

УДК 656.25

ОБЗОР АРХИТЕКТУРЫ, ОСОБЕННОСТЕЙ И МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ОТВЕТСТВЕННЫМИ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

К. А. БОЧКОВ, С. Н. ХАРЛАП, Е. П. ЛИТВИНОВ
Белорусский государственный университет транспорта, г. Гомель

Автоматизированные системы управления ответственными технологическими процессами (АСУ ОТП) на железнодорожном транспорте обеспечивают надёжное управление объектами инфраструктуры, от которых напрямую зависит безопасность движения поездов. К таким объектам относятся стрелочные переводы, светофоры и др.

АСУ ОТП относятся к классу систем повышенной ответственности, где основным критерием эффективности является функциональная безопасность (ФБ) – способность сохранять безопасное состояние при любых отказах оборудования или ошибках персонала. Наряду с этим, в условиях цифровизации возрастает роль информационной безопасности (ИБ), предотвращающей вмешательство в управляющие и диагностические каналы.

Архитектура АСУ ОТП систем железнодорожной автоматики и телемеханики (СЖАТ) построена по иерархическому принципу и включает три уровня:

1 Нижний (полевой) уровень. Представлен датчиками и исполнительными устройствами: стрелочными электроприводами, рельсовыми цепями, счётчиками осей, контактными датчиками и блоками ввода-вывода. Эти элементы работают в реальном времени и передают телеметрию в объектные контроллеры.

Обмен данными осуществляется по промышленным протоколам, использующим физические интерфейсы RS-485/422 (скорость 9,6–115 кбит/с, расстояние до 1,2 км), например Modbus RTU, CAN, IEC 60870-5-101/104. Для отказоустойчивости применяются дублированные каналы связи (до 2 независимых линий) и кольцевые топологии, позволяющие восстановить обмен менее чем за 50 мс при обрыве одного сегмента.

2 Средний (управляющий) уровень. Основной функциональный уровень, реализующий логику управления и диагностики. Он включает микропроцессорные системы централизации (МПЦ), автоблокировки (САБ), системы линейной телемеханики (СЛТ), а также устройства энергоуправления. Здесь формируются маршруты, выполняются взаимные блокировки, контролируется занятость участков пути, осуществляется самодиагностика и обработка сигналов.

Управляющие контроллеры реализуют архитектуры типа 1oo2 (один из двух) или 2oo3 (два из трёх), что обеспечивает допустимую интенсивность опасного отказа на уровне 10^{-8}–10^{-9} 1/ч – менее одного опасного сбоя за 10000 лет непрерывной работы. Для всех компонентов обязательна сертификация по уровням УПБ 3, УПБ 4 (EN 50129, МЭК 61508).

3 Верхний (диспетчерский и серверный) уровень. Отвечает за визуализацию технологических процессов, архивирование данных и обмен информацией с системами управления движением поездов и технической диагностики. На данном уровне функционируют автоматизированные рабочие места (АРМ) операторов, дежурных по станции и инженерно-технического персонала, обеспечивающие взаимодействие человека с системой управления.

Через АРМ осуществляются мониторинг состояния оборудования, отображение предупреждений, анализ архивных данных и формирование отчётности. Управляющие воздействия формируются и исполняются на уровне объектных контроллеров, сертифицированных на соответствие требованиям функциональной безопасности (УПБ), тогда как верхний уровень выполняет функции наблюдения, анализа и поддержки принятия решений.

Передача данных между уровнями осуществляется по выделенным оптоволоконным линиям (скорость 100 Мбит/с–1 Гбит/с), радиорелейным или VPN-каналам с криптографической защитой.

АСУ ОТП железнодорожного транспорта характеризуются:

1) работой в реальном времени – задержка реакции не превышает 1 с;

2) принципом fail-safe – любой отказ приводит к безопасному состоянию (например, закрытию сигналов);

3) долговечностью оборудования – срок службы до 10–15 лет, наработка на отказ более 10^6 часов;

4) распределённой структурой – станции и перегонные блоки соединены линиями длиной до 10–20 км;

5) жёсткой нормативной регламентацией – EN 50126/50129, МЭК 61508, отраслевые требования ЖД.

Эти особенности диктуют необходимость комплексного обеспечения функциональной и информационной безопасности, согласованного на всех уровнях системы.

Функциональная безопасность направлена на предотвращение перехода системы в опасное состояние при возникновении отказов оборудования, сбоев связи или ошибок оператора.

Основные методы:

1 Принцип fail-safe. При потере связи с контроллером все светофоры устанавливаются в запрещающее положение, маршруты фиксируются, стрелки блокируются. Вероятность того, что отказ не приведёт к безопасному состоянию, – не более 10^{-9} 1/ч.

2 Архитектуры дублирования. Используются схемы 1oo2 и 2oo3, при этом вероятность ошибочного решения снижается на 99 %, а вероятность скрытого отказа не превышает 10^{-7}. Модули часто выполняются аппаратно- и программно-разнородными (разные микроконтроллеры, компиляторы, логика).

3 Непрерывная самодиагностика. Каждый модуль выполняет проверку исправности памяти, интерфейсов и логики выполнения программы с периодичностью 10–500 мс. Для этого могут быть использованы следующие методы:

– «бегущего нуля» и «бегущей единицы» – позволяют выявить до 95–98 % аппаратных неисправностей памяти (залипания битов, деградацию ОЗУ);

– CRC-контроля кода и данных – обеспечивают вероятность недетектирования случайных искажений порядка 10^{-7};

– сравнения контрольных сумм программ с эталоном при старте (проверка выполняется за 50–100 мс), и фоновой самопроверки (background check) – позволяют выявлять «мягкие» ошибки ПЗУ и ОЗУ с вероятностью до 99 %;

4 Многоканальная обработка информации в нескольких вычислительных модулях. Несоответствие результатов между дублируемыми контроллерами обнаруживается за время менее 10 мс. При этом активируется диагностический режим и формируется сообщение в вышестоящую систему.

5 Журналирование событий. Каждое изменение состояния, отказ или ручное вмешательство фиксируются во внутренней энергонезависимой памяти.

6 Верификация и валидация ПО. Программное обеспечение проходит многоступенчатую проверку: формальная спецификация требований, моделирование логики, анализ временных задержек, имитация отказов и сертификация.

Таким образом, ФБ реализуется как комплексная система диагностики, контроля и многоканальной обработки информации, обеспечивающая гарантированное безопасное состояние при любых нарушениях нормальной работы.

Переход на цифровые протоколы и IP-сети в телемеханике создал новые векторы угроз. Нарушение целостности телесигналов или подмена управляющих команд может привести к сбоям с тяжёлыми последствиями. Поэтому ИБ стала неотъемлемой частью проектирования АСУ ОТП.

Основные направления защиты:

1 Сегментация сетей и изоляция контуров. Технологическая сеть управления изолируется от корпоративной. Взаимодействие между сегментами разрешено только через шлюзы с межсетевыми экранами и демилитаризованными зонами (DMZ). Наличие DMZ позволяет снизить риск несанкционированного доступа.

2 Аутентификация и управление доступом. Реализуются ролевое разграничение прав (3–5 уровней доступа), двухфакторная авторизация операторов, централизованное ведение учётных записей. Использование аппаратных ключей снижает вероятность возникновения компрометации.

3 Криптографическая защита каналов. Передача данных между станциями и диспетчерскими пунктами осуществляется с использованием алгоритмов шифрования. Нагрузка на процессор при шифровании практически отсутствует, что не влияет на реальное время управления.

4 Контроль целостности и самопроверка данных. Для обнаружения случайных или злонамеренных изменений пакетов используется CRC-контроль каждого сообщения, обеспечивающий вероятность необнаружения ошибки порядка 10^{-7}. Обмен тестовыми «сердечными» пакетами (heartbeat) выполняется каждые 1–2 с для подтверждения активности узлов; отсутствие определенного количества сигналов подряд инициирует аварийный режим.

5 Мониторинг и реагирование. Системы сбора событий безопасности способны анализировать большое количество событий за короткий промежуток времени и оповещать персонал при аномалиях трафика.

6 Физическая защита. Шкафы телемеханики, серверные помещения и кабельные каналы оборудуются средствами контроля доступа и сигнализацией вскрытия.

7 Аудит и тестирование. Проводимые проверки целостности ПО и анализа уязвимостей снижают риск эксплуатации уязвимостей.

Комплексное применение этих мер позволяет свести к минимуму вероятность несанкционированного вмешательства и нарушения целостности данных.

Функциональная и информационная безопасность взаимосвязаны: нарушение целостности данных способно спровоцировать опасное состояние, а чрезмерное усложнение защиты может нарушить временные параметры управления.

В современных АСУ ОТП реализуется координированный подход, при котором:

1) критические команды передаются по изолированным каналам с задержкой не более 5 мс [1];

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: