РАЗВИТИЕ СОВРЕМЕННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ С УЧЕТОМ ТРЕБОВАНИЙ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БОЧКОВ К.А. д.т.н., профессор
БУЙ П.М. к.т.н., доцент
КОМНАТНЫЙ Д.В. к.т.н., доцент
Белорусский государственный университет транспорта, Гомель, Республика Беларусь

Рабочее место дежурного по станции системы электрической релейной централизации

Релейное помещение системы электрической централизации

Центр управления перевозками (ЦУП)

на ж.д. транспорте

Согласно нормативным документов ФСТЭК микроэлектронные и микропроцессорные СЖАТ относятся к критическим системам информационной инфраструктуры (КСИИ, в РБ- КВОИ), также , как и практически во всех западных странах.

Вопросы информационной безопасности таких систем регламентируются различными техническими нормативно-правовыми актами (ТНПА). К основным нормативным документам для анализа защищённости информационных технологий (ИТ) относятся стандарты ГОСТ Р ИСО-МЭК 15408 (3 части) и ГОСТ Р ИСО-МЭК 18045 2012 и 2013 годов (в Республике Беларусь это стандарты СТБ с номерами 1, 2 и 3 серии 34.101 2014 года .

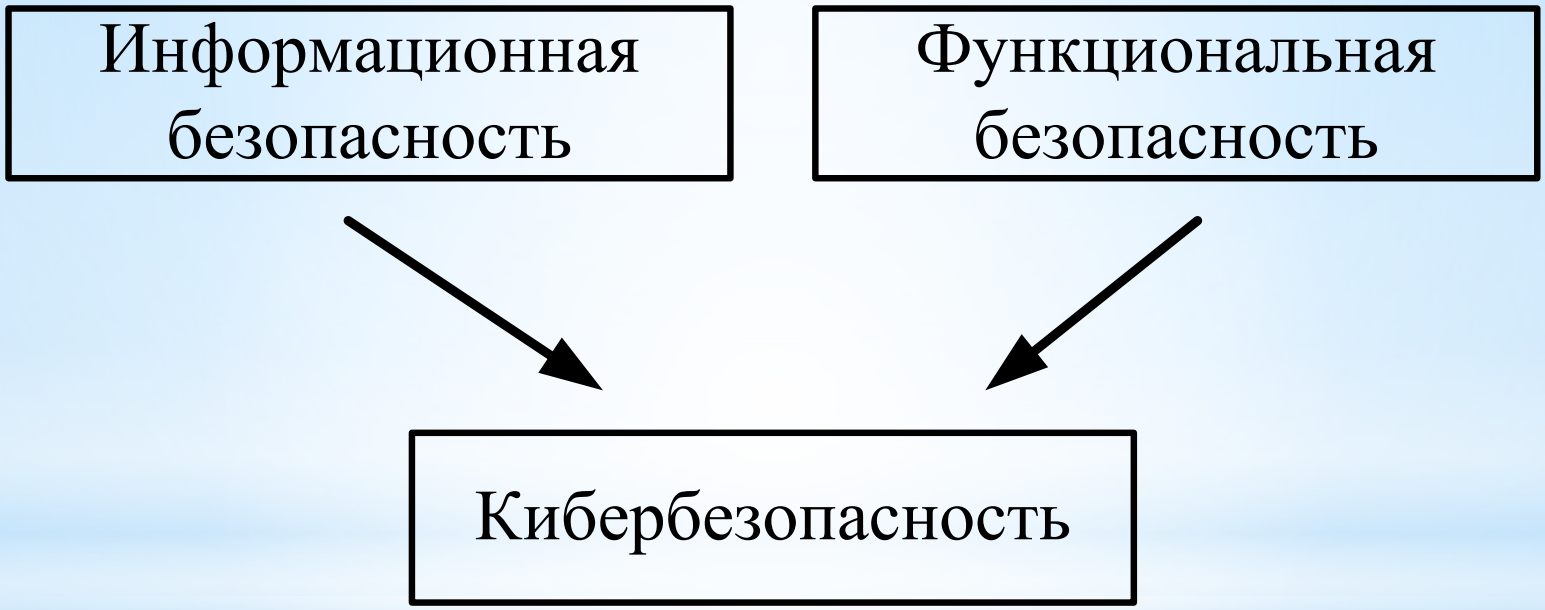
Отдельные аспекты особенностей КСИИ (КВОИ) учтены в стандарте США NIST 800-82 (2011) и стандарте EEC 62279 (2012) *Railway applications. Communications, signaling and processing systems. Software for rail way control and protection systems* (Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах).

Эти стандарты ограничены рамками программно-технического уровня информационной безопасности, что вполне достаточно для оценки продуктов информационных технологий. Однако их не достаточно для микропроцессорных СЖАТ.

* Микропроцессорные СЖАТ относятся к нижнему уровню информационной инфраструктуры управления железнодорожным транспортом. К таким системам, в первую очередь, предъявляются повышенные требования к обеспечению безопасности движения поездов, то есть определяющие их функциональную безопасность, при отказах, ошибках ПО и внешних воздействий, в том числе и кибератаках.
* Комплексный подход к оценке соответствия программного обеспечения (ПО) СЖАТ, учитывающий требования к функциональной и информационной безопасности, отражен в СТО РЖД 02.049-2014г. «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. *Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия*»

Совокупность таких условий функционирования системы управления, при которых обеспечивается конфиденциальность целостность и доступность содержащейся в ней информации.

Совокупность таких условий функционирования системы управления, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных воздействий, приводящих к нарушению процесса штатного функционирования системы.



Совокупность политик и действий, которые должны быть предприняты для защиты критически важных объектов от деструктивных информационных воздействий (несанкционированный доступ, компьютерная атака, программно-аппаратные закладки, недекларированные возможности, искажение, кража, уничтожение информации), направленных на нарушение штатного функционирования этих систем.

Микропроцессорные СЖАТ, имеют следующие дополнительные особенности с позиций обеспечения киберзащищенности по сравнению с массовым «промышленным» АСУ ТП:

- главной целью кибератаки на микропроцессорные СЖАТ является не информация сама по себе, а возможность воздействия на исполнительные объекты;
- возможная атака будет направлена на вывод из строя микропроцессорной СЖАТ (в том числе, и методами электромагнитного терроризма) или нарушения функциональной безопасности, а, следовательно, и нарушения безопасности движения поездов;
- атака может быть направлена на конкретные (наиболее опасные по последствиям), объекты СЖАТ (контроллеры управления исполнительными объектами) с помощью специально разработанных средств, поэтому традиционные (шаблонные), средства защиты могут быть неэффективными;

Эти отличия затрудняют применение в микропроцессорных СЖАТ традиционных подходов в обеспечении информационной безопасности бизнес-систем и обычных промышленных АСУ ТП.

Особенность систем управления нижнего уровня на железнодорожном транспорте

В них практически отсутствует конфиденциальная информация.

Поэтому обеспечение конфиденциальности информации приобретает второстепенное значение, а наиболее важными становятся целостность и доступность информации.

Целостность предполагает надежное и безопасное управление за счет сохранения контроля над структурой управляющих воздействий, а доступность – над их авторизацией и временем появления.

Все эти вопросы касаются безопасности функционирования системы управления.

Системы управления на нижнем уровне в первую очередь должны отвечать требованиям, предъявляемым с точки зрения функциональной безопасности!

Рекомендации по обнаружению закладок, возможных ошибок ПО и минимизации числа уязвимостей при обеспечении кибербезопасности микропроцессорных систем управления на железнодорожном транспорте:

1. Закладки в прикладном ПО можно обнаружить при наличии исходного кода и собственноручной его компиляции.

2. Закладки в системном ПО в первую очередь необходимо искать в операционной системе, в драйверах для промышленных микроконтроллеров.

3. Закладки часто встречаются в аппаратном обеспечении (USB, RS232, RS485, мышь, клавиатура и пр.), а также в нестандартном аппаратном обеспечении (разрабатываемые производителем нестандартизированные платы сопряжения).

4. При минимизации уязвимостей прикладного ПО в первую очередь анализируются:

- уязвимости протокола TCP/IP – здесь должен использоваться контроль целостности и принадлежность пакета, IP адресов и MAC адресов;
- уязвимости прикладного протокола – сообщения должны быть подписаны или зашифрованы каждым отправителем и проверяться на принимающей стороне, также должно быть исключено дублирование пакетов, подключение промежуточного сетевого оборудования (концентраторов), и вклинивание в сеть Ethernet;
- уязвимости в графическом интерфейсе – должна быть предусмотрена обязательная аутентификация пользователя, а также невозможность выполнения недекларированных функций.

5. Подключение к внешним сетям должно быть организовано только через DMZ (демилитаризованную зону, отдельный компьютер с Firewall).

6. При минимизации уязвимостей системного ПО рекомендуется:

- не устанавливать драйверы для BlueTooth, Wi-Fi, USB и пр., а установленные удалить;
- отключить или заблокировать Firewall неиспользуемые сетевые порты (например FTP и пр).

7. При минимизации аппаратных уязвимостей следует:

- запретить аппаратное подключение дополнительных устройств – USB/COM порты должны быть физически отключены, PnP устройства должны быть отключены в BIOS;
- опломбировать или закрыть на ключ корпус (статив);
- физически отключить устройства накопителей на CD, DVD, Floppy и пр.

Одним из новых видов угроз микропроцессорным СЖАТ является «электромагнитный терроризм», суть которого заключается в преднамеренном воздействии сверхширокополосным импульсом высокой энергии.

Воздействие сверхширокополосных импульсных помех (СШИП) различной энергии на микроэлектронные СЖАТ могут приводить к сбоям в работе объектных контроллеров как наиболее ответственных узлов, влияющих на возможное появление опасных отказов, так и к физическому разрушению элементной базы.

Отличительной особенностью СШИП является также соизмеримость длительности воздействия импульсов с длительностью рабочих и тактовых импульсов АПК СЖАТ, что делает их значительно опаснее чем воздействие электромагнитного импульса высотного ядерного взрыва микросекундной длительности с шириной спектра от единиц кГц до сотен МГц.

В начале 2000-х годов на международных симпозиумах по электромагнитной совместимости угроза «электромагнитного терроризма» стала отдельным разделом, а в справочнике «Оружие мира» описаны типы электромагнитного оружия.

При проведении испытаний на устойчивость к воздействию СШИП обычно используют специальные генераторы с излучателями на основе антенной решетки из ТЕМ-рупоров или излучателей на основе параболических рефлекторов.

Рупорные излучатели образуют сферические, сравнительно слабонаправленные волны, а параболические рефлекторы формируют плоскую остронаправленную волну с шириной диаграммы в несколько градусов.

В условиях прямой видимости объекта поражения можно использовать выражения для поля указанных типов волн во временной области:

плоская волна

$$E(R,t) = \frac{1}{2} E_m f\left(t - \frac{R}{c}\right) e^{-\frac{\gamma}{2}R}$$

сферическая волна

$$E(R,t) = \frac{1}{R} E_m f\left(t - \frac{R}{c}\right) e^{-\gamma R}$$


iПУТЬ
СПАСИБО ЗА ВНИМАНИЕ
БелГУТ