ОАО «НИИАС»

Пресс-служба

Тел. +7 495 967-77-02
Эл. почта: info@vniias.ru
www.vniias.ru

Positive Technologies

Пресс-служба

Тел. + 7 495 744-01-44
Эл. почта: pr@ptsecurity.com
ptsecurity.ru
facebook.com/PositiveTechnologies
facebook.com/PHDays
twitter.com/ptsecurity

ООО «Бомбардье Транспортейшн (Сигнал)»

Елена Алешина

Тел. + 7 495 925-53-70
Эл. почта:
elena.alechina@rail.bombardier.com

Пресс-релиз

5 июля 2016 г., Москва

Positive Technologies и «Бомбардье Транспортейшн (Сигнал)» повышают киберзащищенность российских железных дорог

Компании Positive Technologies, «Бомбардье Транспортейшн (Сигнал)» и Научно-исследовательский и проектно-конструкторский институт информатизации и связи на железнодорожном транспорте (ОАО «НИИАС») сообщают о разработке комплексной системы повышения киберзащищенности микропроцессорных систем управления движением поездов. Продукт включает в себя сенсор анализа сетевого трафика на базе системы управления инцидентами кибербезопасности Positive Technologies Industrial Security Incident Manager (PT ISIM)[1], а также устройство кибербезопасного мониторинга CyberSafeMon. Разработанная система — это первый опыт промышленного внедрения подобных устройств в транспортной отрасли не только на территории России, но и в мире.

«Основная задача микропроцессорных систем управления движением поездов (МПСУ) — обеспечение эффективного и безопасного движения поездов, в том числе и за счет минимизации роли человеческого фактора в возникновении аварийных ситуаций, — рассказывает о предпосылках проекта ***Борис Макаров, руководитель центра кибербезопасности ОАО "НИИАС".*** *— Однако широкое внедрение информационных технологий в транспортную систему и активный рост хакерских атак переводят задачу повышения уровня защищенности систем, использующих ИТ, в число наиболее приоритетных. Поиск решения этой задачи потребовал, чтобы мы как головная организация в области кибербезопасности на сети российских железных дорог сформировали тандем из разработчиков таких систем и специалистов в области информационной безопасности. Наиболее активно среди разработчиков МПСУ выступила компания "Бомбардье Транспортейшн (Сигнал)". В качестве экспертов в области ИБ была привлечена компания Positive Technologies — лидер рынка в области противодействия кибератакам, на счету которого обнаружение более 250 уязвимостей нулевого дня в АСУ ТП».*

Эксперты Positive Technologies совместно со специалистами ОАО «НИИАС», работающими над проблемами кибербезопасности микропроцессорных систем, применяемых на сети дорог ОАО «РЖД», при сотрудничестве с разработчиком проанализировали защищенность

[1] **Positive Technologies Industrial Security Incident Manager (PT ISIM)** — система, предназначенная для защиты автоматизированных систем управления технологическим процессом (АСУ ТП). PT ISIM позволяет обнаруживать уязвимости и хакерские атаки на технологические сети предприятия, а также расследовать инциденты (в том числе ретроспективно) на критически важных объектах; помогает бороться с внутренними и внешними угрозами безопасности, включая несанкционированное подключение, подбор пароля, неправомерные управляющие команды, подмену прошивки промышленного оборудования, потенциально опасные действия персонала, ошибки конфигурации.

натурного макета одной из систем управления движением поездов — МПЦ EBILock 950[2]. На основании результатов анализа были сформированы требования по обеспечению кибербезопасности таких систем и начаты работы по повышению их устойчивости к кибератакам.

В рамках этих работ специалисты компании Positive Technologies совместно с «Бомбардье Транспортейшн (Сигнал)» и ОАО «НИИАС» адаптировали сенсор анализа сетевого трафика, предназначенного для противодействия инцидентам кибербезопасности (PT ISIM). В решении обеспечены поддержка специализированных промышленных протоколов, выявление кибератак и инцидентов безопасности с оперативным оповещением ответственных служб. Мониторинг сетевой активности МПЦ EBILock 950 производится в пассивном режиме. Сенсор позволяет подробно визуализировать развитие и распространение атаки в пространстве и времени, а дополнительно разработанный интерфейс позволяет отслеживать все стадии инцидента на технологической карте локальной сети объекта в удобном для пользователя виде.

«Любой наш проект по защите АСУ ТП имеет несколько составляющих, благодаря которым итоговое решение максимально адаптировано к специфике объекта защиты, с его протоколами, бизнес-логикой, технологическими процессами и характерными угрозами безопасности, — поясняет **Борис Симис, директор по развитию бизнеса компании Positive Technologies.** *— Это качественный аудит и выявление возможных векторов развития атаки на систему на всех уровнях, выбор и внедрение компенсационных мер, адаптация PT ISIM под конкретную систему. Только такой экспертный подход — трудозатратный и индивидуальный — может обеспечить реальную защиту, которую не в состоянии дать решения "из коробки"».*

Интеграция PT ISIM и МПЦ EBILock 950 выполнена по схеме, исключающей какое-либо влияние на технологический процесс. Применена специальная схема подключения, обеспечивающая выполнение требований к безопасности движения поездов, которая является главным приоритетом для систем управления.

Специалисты компании «Бомбардье Транспортейшн (Сигнал)» разработали устройство мониторинга CyberSafeMon для безопасного подключения внутренней сети систем управления движением к внешним недоверенным сетям передачи данных. Это решение позволяет эффективно и безопасно передавать информацию о состоянии процесса движения поездов в единые центры по управлению перевозками для целых железнодорожных участков. Разработанное устройство сертифицировано ФСТЭК России как средство защиты информации.

На сегодняшний день сенсор PT ISIM и устройство CyberSafeMon успешно прошли предварительные испытания и введены в опытную эксплуатацию на одной из станций центрального региона, оборудованной системой управления МПЦ EBILock 950. Результаты работ обсуждались на экспертном совете по кибербезопасности ОАО «РЖД» с участием международных экспертов, в частности Марка Антони, директора департамента железнодорожных систем международного союза железных дорог. По итогам опытной эксплуатации будет принято решение о применении разработанной системы на объектах инфраструктуры ОАО «РЖД», оснащенных микропроцессорными системами управления различных производителей.

«Это первый в мире практический опыт обеспечения киберзащищенности микропроцессорных систем управления движением поездов. Мы благодарны ОАО "РЖД" за участие нашей компании в таком важном проекте. Достигнутые результаты могут быть использованы для различных систем с учетом их особенностей, а наработанный опыт будет востребован нашими зарубежными коллегами. Тем не менее мы понимаем, что обеспечение кибербезопасности — непрерывный процесс, и не останавливаемся на достигнутом. Совместно с центром кибербезопасности ОАО "НИИАС" мы продолжаем

[2] **Система микропроцессорной централизации EBILock 950** — микропроцессорная система управления движением поездов последнего поколения производства ООО «Бомбардье Транспортейшн (Сигнал)». В России ею оснащены 157 станций на 15 железных дорогах от Калининграда до Дальнего Востока, за рубежом — еще 131 станция. МПЦ EBILock 950 установлена на высокоскоростных магистралях Москва — Санкт-Петербург и Москва — Нижний Новгород, а также на одной из ключевых транспортных артерий страны — Транссибирской магистрали.

отслеживать новые векторы угроз и непрерывно совершенствовать наши продукты. Только такой проактивный подход позволяет нам оставаться лидером рынка железнодорожных систем управления движением поездов», — комментирует ***Вадим Гросс, исполнительный директор ООО «Бомбардье Транспортейшн (Сигнал)»****.*

ОАО «НИИАС» — дочернее общество ОАО «РЖД», является головным институтом российской отрасли железнодорожного транспорта в создании комплексов и систем обеспечения безопасности движения (в том числе высокоскоростного), управления движением поездов, геоинформационных и спутниковых технологий мониторинга состояния подвижного состава и инфраструктуры железных дорог.
Подробнее: vniias.ru

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована ФСТЭК и «Газпромом». Более 3000 организаций из 30 стран мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями. В 2015 году Gartner назвал Positive Technologies «визионером» в рейтинге Magic Quadrant for Web Application Firewalls.
Подробнее: ptsecurity.ru, facebook.com/PositiveTechnologies, facebook.com/PHDays, twitter.com/ptsecurity

ООО «Бомбардье Транспортейшн (Сигнал)» — первое в истории ОАО «РЖД» совместное предприятие, созданное с компанией Bombardier Transportation, крупнейшим в мире производителем железнодорожной техники. Bombardier Transportation производит весь спектр подвижного состава, включая высокоскоростные поезда и локомотивы, а также интеллектуальные системы управления движением поездов. Первоначально совместное предприятие было образовано для внедрения таких систем управления на российском рынке. Однако затем успех удалось повторить в Узбекистане, Казахстане, странах Балтии, в Словакии и Турции.
Подробнее: ru.bombardier.com/