# Кибербезопасность АСУТП 2016: время действовать вместе

Т.В. Девятков (Институт перспективных исследований АН РТ)

*Рассмотрены основные события, которыми запомнилась IV конференция по кибербезопасности, организованная компанией «Лаборатория Касперского».*

*Ключевые слова: кибербезопасность, операционная система, АСУТП.*

11–12 октября 2016 г. в новом городе России Иннополис (Республика Татарстан) прошла IV конференция — «Кибербезопасность АСУТП 2016: время действовать вместе». В церемонии открытия конференции участвовали: генеральный директор «Лаборатории Касперского» Евгений Касперский; руководитель управления перспективных технологий «Лаборатории Касперского» Андрей Духвалов; вице-президент ПАО «Ростелеком» Александр Маслов; заместитель Премьер-министра Республики Татарстан — министр информатизации и связи Республики Татарстан Роман Шайхутдинов; премьер министр Республики Татарстан Ильдар Халиков.

Основной акцент конференции был сделан на практические вопросы применения киберзащиты индустриальных объектов.

## Безопасная ОС KasperskyOS

Специалисты компании «Лаборатории Касперского» представили собравшимся ОС KaspersyOS, которая разрабатывалась с нуля в течение последних 10 лет для защиты микроконтроллеров. Решение предполагается поставлять в качестве предустановленного программного обеспечения на различных типах оборудования, применяемого в индустриальных и корпоративных сетях. В настоящее время безопасная ОС «Лаборатории Касперского» внедрена в маршрутизирующий коммутатор уровня L3, разработанный компанией Kraftway.

В силу своей архитектуры и предназначения KasperskyOS гарантирует высокий уровень информационной безопасности. Основной принцип работы безопасной ОС сводится к правилу «запрещено все, что не разрешено». Это помогает исключить возможность эксплуатирования как уже известных уязвимостей, так и тех, что будут обнаружены в будущем. При этом система крайне гибкая, и все политики безопасности, в том числе запреты на выполнение определенных процессов и действий, настраиваются в соответствии с потребностями организации.

К преимуществам ОС можно отнести и небольшой размер дистрибутива (1,5 Мб), что обеспечивает значительную производительность и мобильность для использования в самых слабых микроконтроллерах с небольшим объемом памяти.

Безопасная ОС KasperskyOS не является заменой уже существующих ОС широкого применения, используемых на пользовательских компьютерах или серверах. У нее другие задачи и другой принцип работы. Так, если во всех ОС легитимность и безопасность приложений определяется на основе их цифровой подписи, то в безопасной ОС «Лаборатории Касперского» верификация программ осуществляется путем проверки и утверждения их поведения. Любые коммуникации между программными модулями KasperskyOS гарантированно проходят через системное микроядро, которое содержит средства вычисления вердиктов безопасности в соответствии с заданной политикой безопасности, разрешающими или запрещающими каждое конкретное действие со стороны приложения.

В настоящее время компания рассматривает возможность использования KasperskyOS в промышленных системах, в частности, в АСУТП, в телекоммуникационном оборудовании, в медицинских аппаратах, в автомобилях и прочих гаджетах из мира «Internet вещей», например, в видеокамерах, которые не просто осуществляют запись, но также отвечают за распознавание объектов и лиц, хранение и классификацию информации.

В конференции с докладами выступили не только разработчики «Лаборатории Касперского», но и представители других крупных компаний, специализирующихся на информационной безопасности — EnLab, Digital security, ICL КПО ВС, Jet Infosystems, Softline, Диалог-наука, ИнфоТеКС, а также лидеры рынка средств и систем автоматизации: Emerson, SAP CIS, Schneider Electric, Siemens.

В соответствии с темой конференции: «Время работать вместе» в большинстве выступлений демонстрировались формы кооперации с «Лабораторией Касперского» и примеры применения их программного обеспечения. Также были представлены доклады, раскрывающие некоторые приемы злоумышленников, направленные на кражу материальных ресурсов.

В фойе работала выставка, демонстрирующая решения по информационной безопасности от различных компаний — участниц конференции.

### Центр реагирования на компьютерные инциденты

В ходе конференции «Лаборатория Касперского» объявила об открытии первого в России центра реагирования на компьютерные инциденты на индустриальных и критически важных объектах — Kaspersky Lab ICS-CERT. Основная цель ICS-CERT– координировать действия производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей в области информационной безопасности. CERT будет собирать информацию о найденных уязвимостях, имевших место инцидентах и актуальных угрозах и на основе этих данных предоставлять рекомендации по защите индустриальных и критически важных инфраструктурных объектов. Все данные, за исключением конфиденциальных, будут доступны публично в обезличенном виде. Сведения об уязвимостях индустриального ПО и оборудования будут публиковаться при взаимодействии с производителями.

Помимо этого, ICS-CERT планирует проводить консультации по требованиям государственных и отраслевых регуляторов в области обеспечения информационной безопасности индустриальных объектов. Также специалисты центра смогут оценить уровень защищенности промышленных систем автоматизации и провести расследование инцидентов информационной безопасности.

Данные и услуги ICS-CERT будут доступны бесплатно заинтересованным организациям по всему миру. Ожидается, что основными клиентами центра станут производители компонентов АСУТП, национальные CERT и промышленные предприятия, работающие в самых разных отраслях: в энергетике, машиностроении, нефтегазовом секторе, металлургии, производстве строительных материалов, транспорте и пр. Также ISC-CERT «Лаборатории Касперского» готов сотрудничать со сторонними исследователями информационной безопасности, государственными органами и международными правоохранительными организациями.

Одним из первых партнеров проекта стало дочернее предприятие ПАО "Татнефть" — АО " ТАНЕКО". НПЗ «ТАНЕКО» (г. Нижнекамск) — новый завод, построенный с нуля. В Компании «Татнефть» большое внимание уделяется информационной безопасности и обеспечению эффективной защиты АСУ. При строительстве завода были предусмотрены системы информационной безопасности разного уровня, включая и уровень АСУТП. Комплексный подход к вопросу информационной безопасности способствовал расширению сотрудничества с «Лабораторией Касперского». Ранее «Лаборатория Касперского» совместно с ТАНЕКО завершила пилотный проект по обеспечению кибербезопасности железнодорожной платформы по сливу вакуумного газойля.

Стартует проект в Татарстане, но в планах — выход на российский рынок, а затем и на зарубежный.

### Конкурс «белых хакеров»

В рамках конференции «Кибербезопасность АСУ ТП 2016: время действовать вместе» проходил финал конкурса CTF-турнира по индустриальной Кибербезопасности. На площадке конференции был сформирован стенд, моделирующий в реальном времени работу распределительной станции. К стенду подключалось реально используемое для этих целей оборудование с высоким уровнем защиты. Во время работы конференции четыре команды специалистов по кибербезопасности пытались сломать систему защиты и нарушить работу этого стенда. Показателем их деятельности был маленький макет города, освещенный электрическим светом, который должен был погрузиться во тьму.

За главный приз сражались четыре команды из г.г. Долгопрудного (Московская обл.), Екатеринбурга, Новосибирска и Саратова, победившие в предварительных отборочных этапах.

Всего для участия в CTF-турнире зарегистрировалось 154 команды, преимущественно из России. Однако попытать свои силы во взломе энергосистемы на основе архитектуры microgrid также стремились участники из Белоруссии, Украины, Казахстана, Турции, Швеции, Румынии, Индии и Китая.

В рамках финала соревнующиеся команды в режиме реального времени атаковали и проверяли на прочность как отдельные компоненты энергосистемы, так и архитектуру в целом. Победила команда Filthy Thr33 из Екатеринбурга, которая первой (менее чем за 1 сут.) добилась успеха, то есть нарушила работу энергосистемы, устроила короткое замыкание, смоделировала локальное повреждение оборудования и лишила таким образом потребителей источника энергии.

В целом конференция прошла на позитивной волне. Общий настрой с самого начала задал Евгений Касперский, который постоянно шутил, несмотря на серьезность вопросов, затронутых в докладах.

Мероприятие получилось информативным и живым, дало возможность участникам не только познакомиться с продуктами компаний из области кибер-защиты, но и понять общие векторы развития данной области.

***Девятков Тимур Владимирович*** *– канд. техн наук, старший научный сотрудник Института перспективных исследований АН РТ.*
*E-mail: The-9th@yandex.ru*