IT-форум с «бородой»

В 2016 году 70% населения Татарстана воспользовались государственными услугами в электронной форме. 1,9 млн личных кабинетов, 240 доступных сервисов и 86 фактов их оказания. Не удивительно, что в таком контексте 11-я Всероссийская конференция IT&SECURITY FORUM–2017 собрала в Казани более 800 экспертов по информационным технологиям. Свыше 300 компаний прислали своих делегатов на форум. А журнал РУБЕЖ традиционно выступил информационным партнером мероприятия.

Текст: Станислав Тарасов

К своему 11-му году существования форум IT&SECURITY FORUM 2017 (ITSF 2017) продемонстрировал отточенную технологию организации. Как рассказала Ксения Халилова, руководитель отдела маркетинга «ICL Системные технологии», форум изначально был задуман как небольшое региональное мероприятие, посвященное теме информационной безопасности. Затем добавились информационные технологии и бизнес-решения. Число участников стало расти, и, в конце концов, конференция вышла на всероссийский уровень.

«Мы никогда не старались искусственно нарастить популярность. Входные билеты мы не продаем и не зарабатываем на этом. Для посетителей участие в форуме бесплатное. О нем компании, как правило, узнают от своих коллег, которые делятся впечатлениями. Это работает лучше любой внешней рекламы», — поделилась Халилова.

Отдельным поводом для гордости организаторы называют обеспечение безопасности. На площадке присутствует специальная группа, задача которой — исключить нахождение на мероприятии посторонних. Идентификация проводится по бейджам. Пожалуй, ITSF — одно из немногих мероприятий, где это не пустая формальность.

В 2017 году за внимание к ITSF организаторам пришлось побороться. Параллельно с форумом в Иннополисе проходила «Цифровая индустрия промышленной России 2017» (ЦИПР). И если глава Республики Татарстан Рустам Минниханов ITSF 2017 не посетил (все же год не юбилейный), то в целом власти не обошли вниманием мероприятие даже при наличии конкурента в деловом расписании. На пленарной сессии выступили первый заместитель премьер-министра республики Рустам Нигматуллин и министр информатизации и связи Роман Шайхутдинов.

Следом подтянулись и участники ЦИПР. Например, Илья Сычев, руководитель компании GROUP-IB, после выступления в Иннополисе был замечен гуляющим по экспозиции ITSF.

ИНТЕРАКТИВНОЕ РЕГУЛИРОВАНИЕ

Внимание к безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) для казанского ITSF — традиционная часть программы.

Якорным спикером здесь по-прежнему остается государственный регулятор — Федеральная служба по техническому и экспортному контролю (ФСТЭК) России. В 2017 году актуальные тренды рынка озвучила заместитель начальника 2-го управления ФСТЭК Елена Торбенко. На секции «Индустриальные технологии информатизации» она представила обзор изменений в нормативной базе. В частности, теперь операторы государственных информационных систем (ГИС) обязаны не только докладывать во ФСТЭК и ФСБ о возникших инцидентах (149-ФЗ «Об информации, информационных технологиях и защите информации»), но и согласовывать с каждым из ведомств тех-

Well-Worn IT-Forum. Report. Kazan. ITSF 2017 / By Stanislav Tarasov

IT&SECURITY Forum 2017 collected more than 800 experts in the field of cybersecurity and IT-technologies. More than 300 companies sent their representatives to discuss industry's problems and find needed solutions.

Фото: itsecurityforum.ru

нические задания на построение ГИС (Постановление Правительства РФ от 11 мая 2017 г. № 555).

Еще одна новация: приказ ФСТЭК № 27 от 15 февраля 2017 года актуализировал требования о защите информации, обрабатываемой в ГИС. Приказ изменил классы средств защиты информации, применяемых для информационных систем (ИС) различных классов, упразднил 4-й класс защищенности, расставил все точки над «i» в вопросе проверок при аттестационных испытаниях инфраструктуры для ИС. С момента вступления приказа в силу (документ был зарегистрирован в Минюсте 14 марта 2017 года) лица, которые проектируют и внедряют системы защиты информации, не могут самостоятельно проводить аттестацию своих ИС. Теперь ФСТЭК требует, чтобы компании-разработчики обращались в специализированные организации.

Кроме того, с 1 июня 2017 года ФСТЭК предъявляет более строгие требования к безопасности информации в операционных системах. Но дальше — больше. До 2019 года служба сформулирует 12 новых критериев информационной безопасности — от систем управления базами данных и средств управления потоками информации до средств виртуализации.

Елена Торбенко провозгласила от имени ФСТЭК «Эру обратной связи»: служба планирует обзавестись аккаунтом в Твиттере и запустит RSS-рассылки с обновлениями банка данных угроз. Как выяснилось, свои намерения быть в контакте ФСТЭК уже подкрепляла реальными действиями. «Были случаи оперативного реагирования службы на уязвимости. ФСТЭК рассылала рекомендации установить определенный патч и разрешала в виде исключения поставить его до инспекционного контроля», — поделился Дмитрий Кузнецов, директор по методологии Positive Technologies.

Впрочем, в зале, где собрались представители Dell, CheckPoint, Лаборатории Касперского, HPE и т. д., нашлись и те, кто отнесся к усилиям службы со скепсисом: рамочный отраслевой закон нужен, говорили они. Благо новшества теперь можно будет обсуждать прямо в комментах в аккаунте ФСТЭК.

ЭФФЕКТ ЗАИМСТВОВАНИЯ

Накопленную от доклада представителей ФСТЭК энергию слушатели выплеснули на тематических секциях. Самым оживленным местом диалога докладчика и аудитории стал «круглый стол» по правовым аспектам кибербезопасности АСУ ТП.

Тон дискуссии задал Ефим Розенберг, первый заместитель генерального директора ОАО «НИИАС» РЖД. Он рассказал про

«чудеса автоматизации» производственных процессов на станции Усть-Луга в Ленинградской области; доклад с интересом выслушали даже представители энергетических и промышленных предприятий (их в зале было чуть ли не большинство).

Для непрофильной, казалось бы, аудитории как нельзя кстати пришелся опыт разработки отраслевых стандартов, которым охотно делился докладчик от ОАО «РЖД». Слушатели подавали идеи с мест: работу над безопасностью необходимо начинать на стадии внедрения системы, «заточенной» под конкретный объект, массовые подходы в современных условиях не работают и чреваты большим количеством ошибок.

Участники так увлеклись беседой, что времени, отведенного для «круглого стола», не хватило. От организаторов стали требовать учесть это на будущее и выделить отдельный день для разбора информационной безопасности АСУ ТП.

ТЕМНЫЙ РЫЦАРЬ

«Mustbe»-атрибутом ITSF уже многие годы остается еще один докладчик — эксперт по инфобезопасности Алексей Лукацкий. Фанаты этой сферы знают его в качестве бизнес-консультанта по кибербезопасности компании Cisco. А широкой публике он известен как «человек с бородой и в шляпе» на рекламных баннерах форумов «Технологии безопасности» и All-over-IP.

На этот раз в рамках секции «Индустриальные технологии информатизации» Алексей представил анализ законопроекта по безопасности критической информационной инфраструктуры (КИИ). Документ предусматривает интеграцию объектов в государственные системы защиты информации и выполнение требований ФСБ по реагированию на инциденты.

В соответствии с этим проектом затраты на категорирование и оценку защищенности, выполнение требований по ИБ, присоединение к ГосСОПКе (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак), приобретение сертифицированных средств защиты информации, выстраивание процесса реагирования на компьютерные атаки по документам ФСБ, обязательное уведомление об инцидентах, сбор и хранение информации об атаках, обучение персонала и т. д. — все это возложено, как нетрудно догадаться, на плечи самих собственников объектов и инфраструктуры.

По мнению Лукацкого, ситуация напоминает «кипучее нормотворчество» на тему безопасности АСУ ТП, тогда как до сих пор нет элементарного единства в терминах, а документы ФСТЭК, Минэнерго и МЧС не согласованы между собой. Даже ключевой регулятор в вопросе КИИ окончательно не определен, эту роль не могут поделить между собой ФСТЭК и ФСБ России. Правда, точный и подробный анализ ситуации повис в воздухе —мнение специалиста американской корпорации представители российских госструктур тактично оставили без комментариев.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СЕРВИС

«Что же такое SOC и как его готовить» — эта тема стала центральной в рамках секции Security Operation Center (SOC). Свой Центр мониторинга и реагирования на компьютерные инциденты компания «ICL Системные технологии» открыла в Иннополисе 24 мая 2017 года. 25 мая его презентовал журналистам на ITSF руководитель проекта Владимир Дмитриев.

«Классический подход предусматривает покупку средств защиты, их установку и последующее использование. Но этого недостаточно, поскольку у заказчиков нет ресурсов, чтобы правильно эксплуатировать систему, нет обученного персонала. Для решения этих проблем мы вывели на рынок новый продукт, который предлагает информационную безопасность как сервис», — рассказал Дмитриев.

SOC обеспечивает непрерывный мониторинг информационной безопасности, защиту от таргетированных атак и несанкционированных вторжений в АСУ ТП. В центре SOC при компании ICL в режиме 24/7 работают 10 специалистов, а штат подразделения информационной безопасности в целом достигает 200 человек. Дмитриев пообещал, что использование SOC позволит оптимизировать расходы благодаря переводу капитальных вложений в операционные.

Центр будет использовать сервисную модель MSSP (Managed Security Service Provider), по которой «ICL Системные технологии» достигли договоренностей с компанией HPE Security Russia. Эксперт HPE Артем Медведев так прокомментировал это сотрудничество: «Партнеру не приходится инвестировать большие средства в покупку софта, а потом пытаться получить эти деньги с заказчика. Сколько партнер платит нам — зависит от объема услуг, потребляемых клиентом». Стоимость услуг может составлять и 50 тысяч рублей, и несколько миллионов».

Центр мониторинга и реагирования на компьютерные инциденты компании «ICL Системные технологии», как заверили журналистов спикеры ICL, не первый в России, но первый в Поволжье. Здесь услуги «безопасность как сервис» будут предложены клиентам с учетом региональной специфики.

По словам Алексея Лукацкого, ажиотаж вокруг темы SOC на форуме 2017 года связан с изменениями в конъюнктуре отрасли. Раньше можно было обеспечить безопасность с помощью разрозненных решений, сейчас требуется консолидация всех усилий в одних «руках», пояснил эксперт. И сделал прогноз на будущее: «SOC понимают поразному, одни как деятельность, другие как подразделение, кто-то видит в нем только мониторинг, а кто-то добавляет реагирование. Каждый по-своему прав, ведь тема SOC и в мире не устоялась. Наверное, концентрация усилий будет идти вокруг bestpractice — выработки передового опыта. Компании будут делиться тем, как они выстроили мониторинг, реагирование и обнаружение сложных угроз, как они работают с персоналом и т. д.».

БАНКОВСКАЯ НЕГАРАНТИЯ

Год от года IT&SECURITY FORUM выводит в тренд ту или иную тему по мере ее востребованности отраслевым сообществом (организаторы следят за этим еще на ранних этапах подготовки к каждому мероприятию).

На ITSF 2017 популярной стала банковская секция. Программным стало выступление начальника Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России Артема Калашникова.

В докладе ФинЦЕРТ была представлена любопытная и даже уникальная статистика о главных направлениях атак в сегменте финансовых организаций за 2016-2017 годы.

Представитель ФинЦЕРТа также поделился цифрами по мошенникам, действующим в Сети: в 2016 году в «черные списки» был направлен 1601 сайт, а в 2017 году только за первые четыре месяца зарегистрировано 9895 фишинговых страниц. Самыми распространенными нарушениями стали фейковые страницы банков, компаний по продаже авиабилетов, несуществующих онлайн-магазинов. «Для кибермошенников существует благоприятная почва в условиях отсутствия единого компьютерного центра блокировки мошеннических ресурсов, а также сложностей, связанных с проведением расследования правоохранительными органами», — объяснил криминальную статистику Артем Калашников. При этом слушатели в зале опасливо стали посматривать на экраны своих мобильныхустройств.

Специалисты ФинЦЕРТа предлагают интернет-пользователям несколько инструментов борьбы с кибермошенниками: усиление технической экспертизы, развитие антифрод (фрод-мониторинг — система оценки финансовых транзакций в интернете), а также введение системы личных кабинетов на сайте Банка России.

Подытожил свой доклад Артем Калашников сообщением о том, что в Госдуму внесен проект закона, который в случае принятия обяжет банки делиться информацией об инцидентах с Банком России. Таким образом, доклад Калашникова организовал повестку последующей работы ИБ-специалистов в банковском и финансовом сегментах.

SOC обеспечивает непрерывный мониторинг информационной безопасности, защиту от таргетированных атак и несанкционированных вторжений в АСУ ТП

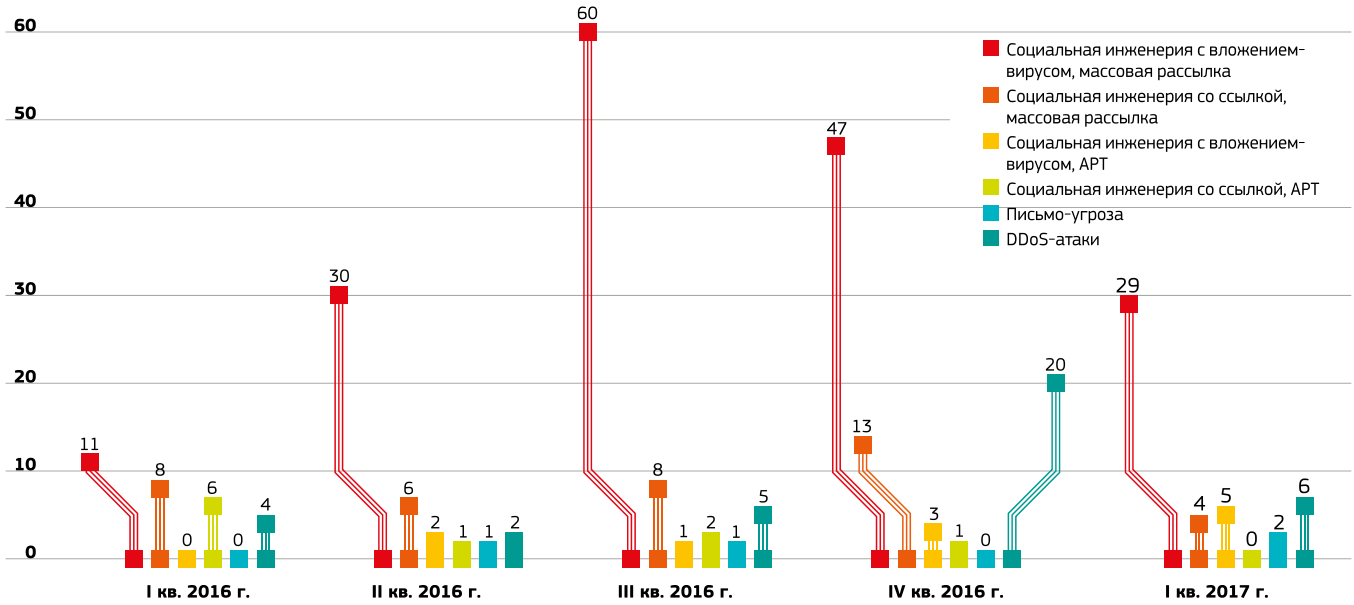
ФОРУМ НА ВЫРОСТ

С момента основания ITSF проводится на базе ГТРК «Корстон», одного из самых крупных в Казани бизнес-центров. Но в 2017 году организаторы признали — площадка стала маловата. Пора присмотреться к новым, более масштабным локациям. Например, активно строится большой международный конгрессно-выставочный центр «Казань Экспо». Ксения Халилова пообещала: «С его появлением станет проще. Мы обязательно к нему присмотримся».

Примечательно, что аудитория ITSF каждый год не только обрастает новыми участниками и слушателями, но и сохраняет «костяк» форума. Во многом это достигается заботой организаторов о каждом партнере практически в индивидуальном режиме. Поддержание семейной атмосферы работает на руку форуму — даже после 8 часов работы все участники с удовольствием и в полном составе отправляются на неформальные мероприятия. За торжественными ужинами продолжается не только деловое общение — эксперты рынка информационной безопасности показывают друг другу, как правильно оттягиваться после напряженного и продуктивного дня.

11-й ITSF не стал исключением. В первый день ИТ-профи поехали в ресторан «Эрмитаж», где под аккомпанемент группы «Несчастный случай» продолжили общение и уничтожили бочку виски. Группа Mgzavrebi стала хедлайнером второго вечера, на этот раз — в ресторане «ПАШМИР». Если интригой 2016 года было «сбреет ли бороду Лукацкий», то в 2017 собравшихся больше волновало, кому Гиги Дедаламазишвили (фронтмен Mgzavrebi) вручит свою пластинку. Кстати, борода пока все еще при Лукацком.

Число кампаний (типов атак), направленных на организацию кредитно-финансовой сферы
(по статистике FinCERT)



Отзывы об ITSF 2017

Алексей Лукацкий

бизнес-консультант по информационной безопасности, Cisco

Несколько лет назад форум задал уже довольно высокую планку, поэтому каких-либо изменений в организации не наблюдаю. Однако каждый год выделяются те или иные ключевые темы. В этом году продолжилась и усилилась тема безопасности АСУ ТП, что связано с увеличением числа атак на критически важные объекты, а также с изменением правового поля.

Сейчас активно меняется нормативная база, принята «Доктрина информационной безопасности», сформирована «Стратегия развития информационного общества», готовится ряд новых приказов со стороны регуляторов, в Госдуме находится проект закона о безопасности критической информационной инфраструктуры. Поэтому эта тема сейчас находится в центре внимания.

Артем Медведев

руководитель направления, HPE Security Russia

Я посещаю форум последние пять лет и могу сказать, что ITSF достиг определенной планки качества. HPE как вендор часто принимает участие в подобных мероприятиях, но форум от «ICL Системные технологии» выделяется невероятным уровнем организации. Сделать лучше, пожалуй, сложно. С точки зрения спикеров — все авторитеты рынка присутствуют, поэтому недостатка в общении, информации и заказчиках нет. Несмотря на то что «ICL Системные технологии» — региональная компания, форум, безусловно, имеет федеральный масштаб. Нам, как компании-партнеру ITSF, очень хорошо видно, во что мы вкладываем деньги. Всегда есть польза, результат и новые идеи.

Форум 2017 года сконцентрировал большое внимание на регуляторах, и это правильно. За последний год ФСТЭК, Минкомсвязи и ЦБ выпустили ряд документов, которые, с одной стороны, сильно повлияют на отрасль, а с другой — слабо информационно освещены. Очень полезными стали выступления ФСТЭК, а также обсуждение нормативов для защиты АСУ ТП.

Если говорить о недостатках, то хотелось бы видеть больше экспертных докладов, практических кейсов использования продуктов заказчиками.

Антон Шипулин

менеджер по развитию решений по безопасности критической инфраструктуры, Лаборатория Касперского

Я участвую в ITSF второй раз, но знаю, что мероприятие проводится уже 11 лет. Это солидный возраст для конференции. За эти годы форум успел завоевать уважение благодаря отличной организации. На площадке ITSF собирается действительно много профессионалов в области информационной безопасности.

Я занимаюсь защитой критических инфраструктур, промышленных систем автоматизации, поэтому в основном уделил свое время именно этой тематике. Приятно отметить, что мои интересы совпали с намерениями организаторов и интересами аудитории. Удалось встретить здесь и заказчиков из нефтегазовой сферы и других рынков. Видно, что заинтересованные лица готовы к диалогу, но не всегда получают достаточное количество нужной информации. Например, на «круглом столе» по безопасности АСУ ТП было озвучено желание выделить целый день на обсуждение этой темы.

Сергей Лачугин

начальник отдела продаж, «Газинформсервис»

Стоит сказать, что мы регулярно принимаем участие в ITSF — это статусное мероприятие. От коллег и заказчиков получаем только хорошие отзывы. Если сравнивать форум 2017 года с предшествующими, то заметен рост числа посетителей. Деловая программа форума вызывает большой интерес участников. Достоинство форума заключается в актуальной повестке, с которой мы стараемся синхронизировать представленные на стенде нашей компании продукты. Сегодня в тренде криптография, защита ИТ-инфраструктуры, конфигурационный менеджмент, а также автоматизация пропускного режима на объектах и защита ERP на базе SAP.

Сергей Касаев

руководитель IBM в Поволжье, Центральной и Южной России

Я посетил форум впервые. Однако много раз слышал очень хорошие отзывы от коллег. И нужно сказать, что мои ожидания оправдались. Это, безусловно, одно из лучших региональных мероприятий. Здесь отличная организация, правильно подобранные спикеры, а также большое количество посетителей.

Василий Широков

заместитель генерального директора по развитию бизнеса в России, Check Point Software Technologies

В новое десятилетие своего успешного существования конференция ITSF предстала перед нами еще более масштабной и, что самое главное, стремящейся к поиску новых форм и методов работы с аудиторией и с деловой программой. Безусловно, это является залогом того, что мы еще не один раз с успехом и огромным удовольствием встретимся на этом уникальном мероприятии. Что же касается неформальной программы конференции — она как всегда на высоте, подхватив тенденцию на развитие. В результате вечерняя программа второго дня ни в чем не уступала первому, а в чем-то и превосходила его. Так держать, ITSF! И отдельно хотелось бы выразить огромное уважение людям, которые вложили все свои силы и душу в организацию конференции. Вы лучшие!