IX КОНФЕРЕНЦИЯ

«Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов»

Категорирование завершено. Да здравствует защита!

17–18 марта в Москве состоялась IX конференция «Информационная безопасность АСУ ТП критически важных объектов», на которой традиционно обсуждались наиболее актуальные вопросы обеспечения защиты промышленных объектов и критической инфраструктуры от киберугроз.

Мероприятие прошло при поддержке ФСТЭК России. В конференции приняли участие 382 представителя государственных и коммерческих промышленных холдингов, производителей решений для защиты АСУ ТП и разработчиков продуктов для промышленной автоматизации, научных центров и учебных заведений. Партнерами конференции стали компании «АйТи БАСТИОН», «СайберЛимфа», InfoWatch, Positive Technologies, «Лаборатория Касперского», «Ростелеком-Солар», АМТ-ГРУП, «ДиалогНаука», «ИнфоТеКС», «Доктор Веб», R-Vision, УЦСБ, «НОРСИ-ТРАНС», «Гарда Технологии», «Газинформсервис», «КСБ-СОФТ» и RuSIEM. Организатор мероприятия – Издательский дом «КОННЕКТ». Именно с напутственного слова заместителя генерального директора ИД «КОННЕКТ» Дмитрия Корешкова и началась программа мероприятия. Модератором программы был главный научный сотрудник Федерального исследовательского центра «Информатика и управление» РАН Виктор Гаврилов.

От категорирования к СУИБ

Первый день конференции был посвящен обсуждению текущей ситуации с реализацией Федерального закона № 187-ФЗ «О безопасности КИИ», современных технологий обеспечения

Президиум (слева направо): Елена Торбенко, ФСТЭК России, Дмитрий Корешков, Connect, Виктор Гаврилов, ФИЦ ИУ РАН, Сергей Бочкарев, АйТи БАСТИОН, Георгий Петросюк, НИЦ «Институт им. Н.Е. Жуковского»

Елена ТОРБЕНКО,
заместитель начальника Управления ФСТЭК России

Алексей АНАСТАСЬЕВ,
Positive Technologies

Азат ШАЙХУТДИНОВ,
Kaspersky ICS

защиты промышленных объектов, научного подхода к моделированию кибератак и расчету рисков. С ключевым докладом первого дня выступила **заместитель начальника Управления ФСТЭК России Елена Торбенко**, которая рассказала о последних разработках регулятора в части регулирования защиты промышленных АСУ – «Рекомендациях по оценке показателей критериев экономической значимости объектов КИИ РФ». В ближайшее время ведомство планирует разработать аналогичные рекомендации и для социальных и экологических показателей.

Елена Торбенко сообщила о проблемах, которые возникают при категорировании объектов КИИ. В частности, она отметила, что авторы документов уже научились строить модели нарушителя и прогнозировать угрозы, но почему-то не могут подсчитать ущерб. Причем базовая модель для подобных расчетов существует – декларация промышленной безопасности. Кроме того, часто различные виды ущерба не согласуются между собой: если есть экологический ущерб, то должен быть и социальный. Аналогично, если есть экономический ущерб для предприятий, работающих с гособоронзаказом, то есть ущерб и для безопасности страны – опасность невыполнения ГОЗ в срок. Подобные рассогласования вызывают вопросы со стороны специалистов ФСТЭК и приводят к отклонениям присланной заявки.

Руководителей обучили, а линейный персонал – гениальные самоучки?
Елена Торбенко

К недостаткам документов, подаваемых на регистрацию объектов КИИ, Елена Торбенко отнесла и отсутствие планов по приведению систем защиты в соответствие с требованиями регуляторов или слишком длительные сроки, обозначенные в этих планах. В некоторых случаях рабочие места администраторов АСУ ТП не включаются в состав объекта КИИ, хотя именно через них хакеры могут воздействовать на все элементы информационных систем объекта. Иногда причиной для отказа в регистрации объекта КИИ могут быть слишком сложные трудовые обязанности сотрудников служб ИБ (например, вручную проанализировать 10 тыс. событий в день). С 2021 г. вступили в действие требования по обучению персонала, который работает в службе ИБ. К тому же в проверках, которые ФСТЭК собирается проводить в текущем

Игорь ДУША,
InfoWatch ARMA, выступил онлайн

В случае удаленной работы все внутренние пользователи стали внешними.

Сергей Бочкарев

году, соблюдение этих требований будут контролировать.

Комплексная защита предприятия

В докладах участников рынка были рассмотрены вопросы комплексной защиты промышленных сегментов сетей и интеграции промышленных средств защиты различных классов, что говорит о зрелости российского рынка средств защиты АСУ ТП.

Технический директор InfoWatch ARMA Игорь Душа дистанционно рассказал о возможностях современных индустриальных межсетевых экранов, которые обеспечивают сегментацию и микросегментацию промышленных сетей, управление доступом к промышленным сегментам и обнаружение атак с подробным разбором промышленных сетевых протоколов. Компания также разработала систему для защиты рабочих станций, установленных в промышленной сети, и единую систему управления защитой, которая позволяет взаимодействовать с различными защитными продуктами.

Стенд компании «АйТи БАСТИОН»

Тему комплексной защиты индустриальных сетей продолжил **руководитель направления по развитию бизнеса компании Positive Technologies Алексей Анастасьев**. Он рассказал о современных вызовах при построении промышленных систем автоматизации, в частности, речь шла о сложности обновления программного обеспечения в промышленных сегментах и процедуры внедрения средств обеспечения защиты промышленных сетей.

Менеджер по развитию бизнеса Kaspersky ICS Азат Шайхутдинов подробно рассказал о возможностях современных средств обнаружения вторжений (СОВ), которые могут быть установлены в промышленные сегменты. «Лаборатория Касперского» в этом году планирует выпустить новую версию своей СОВ KICS for Networks 3.1, в которой будут реализованы интеграция со средствами защиты рабочих станций (KICS for Nodes), централизованное управление средствами защиты промышленной сети и даже оперативное вычисление рисков.

Еще одно, на этот раз совместное решение компаний Dr.Web и «СайберЛимфа», представил на конференции **начальник отдела технического сопровождения продаж «Доктор Веб» Василий Севостьянов**. Его компания разрабатывает средство защиты рабочих станций, но до недавнего времени не имела централизованной системы сетевого мониторинга и анализа происходящих событий. Эта часть функционала была реализована партнером – компанией «СайберЛимфа», которая разработала систему сетевого мониторинга промышленных сетей. Оказалось, что решения хорошо дополняют друг друга – их совместное использование было протестировано лабораториями обеих компаний. **Директор компании «СайберЛимфа» Алексей Шанин** более подробно рассказал о самом средстве мониторинга состояния защищенности

Василий СЕВОСТЬЯНОВ,
«Доктор Веб»

Алексей ШАНИН,
«СайберЛимфа»

Стенд компании «СайберЛимфа»

DATAPK, которое позволяет выявить и даже ликвидировать большую часть инцидентов информационной безопасности. Предлагаемое его компанией решение использует методы искусственного интеллекта для выявления аномальных событий в потоке мониторинга.

Таким образом, на российском рынке сформировалось несколько семейств инструментов для комплексной защиты промышленных сетей от компаний Positive Technologies, InfoWatch ARMA, «Лаборатория Касперского» и «Доктор Веб»/«СайберЛимфа».

Компоненты защиты

Впрочем, есть продукты, которые выпадают из общей схемы комплексной защиты АСУ ТП. Так, **директор по развитию бизнеса «АйТи БАСТИОН» Сергей Бочкарев** обсудил в своем выступлении возможности автоматизации процесса обеспечения безопасности удаленной работы сотрудников. Он отметил, что при переходе на удаленную работу количество событий безопасности увеличивается, а число работников службы ИБ – нет. Для надежного контроля удаленной работы сотрудников нужно использовать автоматизированные средства защиты.

Сложность атак возрастает, а уровень квалификации хакеров – падает.
Виктор Гаврилов

На этом рынке постоянно появляются и новые компоненты для организации защиты промышленных предприятий. В частности, компания «ИнфоТеКС», которая специализируется на создании VPN-продуктов, решила попробовать себя в качестве производителя защищенных средств безопасности для промышленных сетей. О ее продуктах рассказала на конференции **руководитель направления в отделе развития продуктов «ИнфоТеКС» Марина Сорокина**. В качестве темы доклада она выбрала импортозамещение по части криптошлюзов для промышленных сетей. Криптомаршрутизаторы, выпускаемые компанией, позволяют защитить от вмешательства линии связи, которые расположены на протяженных или распределенных объектах КИИ. Компания выпустила криптошлюз ViPNet Coordinator IG, предназначенный для защиты промышленных сетей от перехвата данных посторонними. Построен он на российской аппаратной платформе и выпускается компанией на собственном заводе.

Сергей БОЧКАРЕВ,
«АйТи БАСТИОН»

Марина СОРОКИНА,
«ИнфоТеКС»

Дмитрий ГОРЛЯНСКИЙ,
«Гарда Технологии»

Стенд компании InfoWatch

Андрей ПРОШИН,
«Ростелеком-Солар»

> *Товарища с топором мы не рассматриваем как компьютерную атаку.*
>
> **Елена Торбенко**

Очередной продукт для анализа трафика IP-сетей в сегментах АСУТП с возможностью выявления в нем аномального поведения представил **руководитель технического сопровождения клиентов компании «Гарда Технологии» Дмитрий Горлянский**. Компания разработала инструмент для анализа более 200 различных промышленных протоколов, в которых средство защиты понимает, в частности, контекст тех или иных операций. Инструмент обращает внимание и на использование нестандартных портов для протоколов, большие объемы для передачи файлов и количество нестандартных запросов, например, к DNS-сервису. В целом практически все средства мониторинга АСУ ТП понимают промышленные протоколы, поэтому конкуренция идет уже на уровне количества поддерживаемых протоколов, удобства анализа и составления правил реагирования на инцидент.

Еще одним компонентом, который не вписывается в сложившиеся альянсы, стали однонаправленные шлюзы, о развитии рынка которых рассказал **руководитель направления собственных продуктов департамента информационных систем компании АМТ-ГРУП Вячеслав Половинко**. Инфодиоды являются важной частью сегментации промышленных сетей, позволяющих подключать к промышленным сетям системы мониторинга без влияния их на процессы, происходящие внутри промышленной сети. Аналогично подключаются к защищенным сегментам и средства сбора телеметрической информации и даже видеопотоков с камер наблюдения.

Стенд компании Positive Technologi

Сложность использования промышленных систем защиты заключается в том, чтобы понять, какое именно нарушение они обнаружили. Поэтому необходимы инструменты для анализа результатов деятельности средств защиты. Об организации процедуры анализа происходящих на предприятии событий в части обеспечения безопасности АСУ ТП рассказал **начальник отдела службы технического директора «Газинформсервис» Анатолий Большаков**. Его компания разработала платформу для создания системы операционного мониторинга и анализа данных (СОМА), которая собирает информацию из системных журналов ИТ- и ИБ-продуктов, а также дополняет

Вячеслав ПОЛОВИНКО,
АМТ-ГРУП

Анатолий БОЛЬШАКОВ,
«Газинформсервис»

Ирина НОСОВА,
R-Vision

их сведениями с данными технологического процесса. Это позволяет посредством методов больших данных построить зависимости состояний технологического процесса от работоспособности ИТ и состояния защищенности, обеспечиваемого ИБ-инструментами. В целом компания реализует концепцию расширенной аналитики безопасности (Advanced Security Analytics Platform – ASAP), которую разработала и продвигает компания Ankey.

На российском рынке имеются и средства для автоматизации процессов соответствия требованиям Федерального закона № 187, которые собирают информацию об объектах КИИ, готовят по ней отчеты и подготавливают их для предоставления в контрольные службы. Об одном из таких продуктов рассказала **ведущий пресейл-менеджер R-Vision Ирина Носова**. Инструмент предназначен для инвентаризации активов субъекта КИИ, моделирования угроз и нарушителя, проведения аудита по приказу ФСТЭК № 239, подготовки автоматической отчетности и организации взаимодействия с НКЦКИ. Несмотря на то что он скорее снижает юридические риски, чем повышает защищенность АСУ ТП, для многих промышленных предприятий, особенно подпадающих под действие Закона № 187-ФЗ, он может оказаться весьма полезным.

Услуги защиты объектов КИИ

Анализ степени угроз из различных источников провел на конференции **руководитель направления по развитию бизнеса услуг и сервисов SOC «Ростелеком-Солар» Андрей Прошин**. Он выделил пять основных типов нарушителей: боты, киберхулиганы, киберкриминал, кибернаемники и кибервойска. У каждой из этих групп свои цели и методы атак, поэтому для защиты от них приходится использовать разные инструменты защиты. К примеру, если для защиты от ботов и хулиганов достаточно простых инструментов типа антивирусов и межсетевых экранов, то для блокирования действий кибервойск или хотя бы их обнаружения придется привлекать сторонних экспертов.

Все облака находятся в юрисдикции одной страны.
Георгий Петросюк

Об особенностях построения центра реагирования на инциденты (SOC) рассказал **заместитель генерального директора по научно-технической работе УЦСБ Николай Домуховский**. Именно

Стенд компании «Лаборатория Касперского»

Николай ДОМУХОВСКИЙ,
УЦСБ

Виктор СЕРДЮК,
«ДиалогНаука»

Денис МАРЕЕВ,
«ОЭК»

При категорирования сложно сформировать единую сущность и поставить ее на контроль.
Ирина Носова

SOC позволяет собирать события информационной безопасности с различных средств защиты, быстро обнаруживать в них признаки нападения, блокировать распространение атаки, параллельно аккумулировать информацию об инциденте и направлять ее в соответствии с Федеральным законом № 187 в систему ГосСОПКА. Если же из этой системы поступает конкретное предупреждение об атаке с подробным описанием признаков заражения, то инструменты SOC обеспечивают возможность проверить на инфраструктуре наличие этих признаков, а иногда и провести анализ на них исторических данных – в зависимости от функциональных возможностей SOC. Таким образом, компаниям, которым приходится защищаться от высокоуровневых угроз, необходимо иметь собственный SOC либо арендовать его.

Практические примеры построения системы защиты привел в своем докладе **генеральный директор «ДиалогНаука» Виктор Сердюк**. Уже несколько лет на нашей конференции он делится опытом построения защиты в одной из наиболее тяжелых в этом отношении отраслей – электроэнергетике. Проблемы связаны с тем, что объекты защиты распределенные, потому обеспечить для них периметровый контроль весьма сложно. При этом у самих энергетиков при управлении инфраструктурой остается соблазн обойти средства защиты и подключиться напрямую к удаленным объектам. Таким образом, внедрение системы ИБ было связано не только с защитой сетей передачи и конечных точек, но и с постоянным мониторингом исполнения правил безопасности. Компании пришлось также внедрять подсистемы управления обновлениями и контроля привилегированных пользователей, двухфакторную аутентификацию.

О результатах эксплуатации построенной «ДиалогНаукой» системы рассказал **начальник департамента информационной безопасности «ОЭК» Денис Мареев**. В результате внедрения системы защиты в компании было создано специальное подразделение, которое занимается обеспечением защиты промышленной сети, причем от воздействия как из Интернета, так и из корпоративной среды.

Стенд компании «Ростелеком-Солар»

Артем МИНАКОВ,
«НОРСИ-ТРАНС»

Стенд компании АМТ-ГРУП

Информационная безопасность и импортозамещение

Второй день открыла дискуссионная панель по вопросам импортозамещения в сфере ИБ АСУ ТП, на которой обсуждались темы влияния импортозамещения и открытого ПО на процесс обеспечения информационной безопасности, внедрения доверенных АСУ ТП и средств защиты, а также безопасной организации обновлений. В большинстве своем российские компании вынуждены доверять предоставляемым разработчиками обновлениям, поскольку у них нет ресурсов для всесторонней проверки. Однако наиболее опасные злоумышленники, контролируемые иностранными государствами, уже начинают осваивать технологии атаки через посредников, в число которых попадают и разработчики, в частности, промышленного ПО.

Участники дискуссии отметили, что назрел вопрос о централизованной проверке обновлений, особенно поставляемых зарубежными компаниями, в интересах защиты ключевой информационной инфраструктуры РФ. Своим опытом проверки приложений для промышленных систем поделился **заместитель начальника отдела ИБ АСУ ТП «Транснефть» Дмитрий Кобзев**. В его компании сформирован отдел анализа защищенности кода, который выполняет проверку обновлений перед их загрузкой на промышленные объекты и позволяет провести до 600 испытаний в год для новых приложений. Компания даже ведет разработку статистического анализатора для языка программирования, который используется в ПЛК. Введение этой организационной единицы в строй позволило сократить количество обновлений ПО и сделать их более надежными.

> *Важно не только быстро продать и уйти в тень, но лечить, где болит.*
> **Константин Родин**

Тему импортозамещения продолжил доклад **начальника отдела информационной безопасности «НОРСИ-ТРАНС» Артема Минакова**. Предлагаемые компанией комплексные продукты являются преимущественно российскими, причем не только по программному обеспечению, но и по компонентной базе.

Директор департамента информационных технологий НИЦ

Стенд компании ДиалогНаука

С ущербом мы умеем работать, а вот с вероятностью – проблемы.

Борис Безродный

«Институт имени Н.Е. Жуковского» Георгий Петросюк традиционно осветил проблему передачи конфиденциальных данных в информационные системы их производителей. Причем не только IoT, где подобная технология является неотъемлемой частью концепции, но и в существующих операционных системах, браузерах и плагинах для них.

Обмен опытом

Изюминкой конференции всегда были доклады пользователей решений по защите промышленных систем. Так, **заместитель руководителя по реализации проектов в области Индустрии 4.0 компании «ММК-МЕТИЗ» Артем Губайдуллин** рассказал о классификации объектов КИИ. Многие организации уже практически завершили процедуры категорирования, однако всегда есть отстающие, которым будет полезно ознакомиться с опытом категорирования наиболее крупных промышленных предприятий. «ММК-МЕТИЗ» объединила все свои промышленные информационные системы в пять объектов КИИ по территориальному признаку, для которых было организовано пять демилитаризованных зон, т. е. их число удалось сократить за счет консолидации по принципу отнесения к конкретным объектам КИИ.

Опытом обеспечения безопасности объектов КИИ поделился **начальник Управления информационной безопасности «НЛМК» Алексей Овчинников**. Он отметил, что в процессе категорирования все подразделения старались стать значимыми, однако выяснилось, что производство не является критичным фактором для функционирования предприятия. При выходе из строя одной домны ее заказы можно перераспределить на другие без существенного ущерба. Критичными оказались только три экономических подразделения, остановка работы которых может привести к значительным потерям для бюджета страны.

Наиболее остро проблему оценки опасности взломов компьютерных систем поставил **заместитель руководителя Центра кибербезопасности «НИИАС», доктор технических наук профессор Борис Безродный**. Его институт занимался моделированием последствий компьютерных атак, направленных на нарушение штатного функционирования систем железнодорожной автоматики и телемеханики (СЖАТ). Предложенная методика оценки сложных последствий компьютерных атак на железнодорожную инфраструктуру и стала предметом активного обсуждения. На текущий момент в разработке находятся методические рекомендации по категорированию СЖАТ, а также требования по построению защиты системы автоматики и телемеханики, которую придется внедрять по результатам категорирования.

Разработками в части проведения процедуры категорирования объектов РЖД поделилась **заместитель начальника отдела**

Георгий ПЕТРОСЮК,
НИЦ «Институт имени Н.Е. Жуковского»

Артем ГУБАЙДУЛЛИН,
«ММК-МЕТИЗ»

мониторинга и анализа угроз безопасности центра компетенций по информационной безопасности (структурное подразделение РЖД) Наталья Хмелевская. Для проведения процедуры категорирования в РЖД были разработаны два документа: «Регламент определения объектов КИИ ОАО «РЖД» и «Методические рекомендации по категорированию объектов КИИ ОАО «РЖД». Первый предназначен для подготовки перечня, передаваемого во ФСТЭК, второй – для проведения основной процедуры, на которую отводится год. Инфраструктура РЖД распределенная, как и у электроэнергетиков, поэтому сложности возникают даже на этапе определения принадлежности того или иного объекта КИИ. Потому кроме обязательной организационной единицы – комиссии по категорированию – компания создала экспертный совет при комиссии и даже специальную рабочую группу по определению объектов КИИ, принадлежащих РЖД.

Начальник отдела нормативно-технического обеспечения кибербезопасности «ВНИИАЭС» Денис Бабаев привел в своем докладе пример анализа безопасности энергоблока АЭС, обусловленного воздействием компьютерных атак на АСУ ТП АЭС. Основным активом компании, который необходимо защищать от компьютерных атак, является энергоблок. Ранее его безопасность оценивалась без учета антропоморфных угроз, таких как компьютерные атаки, сейчас ситуация поменялась, и подходы к оценке безопасности приходится корректировать. В частности, для расчета последствий компьютерных атак «ВНИИАЭС» предлагает использовать технологию цифрового двойника, которая разработана для управления энергоблоками. Институт уже проводит моделирование влияния компьютерных инцидентов на технологические процессы. В АЭС как раз и возникает та самая ситуация, когда защитный отказ, вызвавший срабатывание ПАЗ при успешной компьютерной атаке, может привести к серьезным экономическим проблемам для региона. То есть экологическая безопасность будет обеспечена, а вот оставшиеся без энергоснабжения предприятия и государственные службы могут понести серьезные убытки.

Стенд компании «ИнфоТеКС»

Информационную безопасность старых домн 60-х годов постройки обеспечить оказалось сложнее.
Андрей Нуйкин


Алексей ОВЧИННИКОВ,
«НЛМК»


Борис БЕЗРОДНЫЙ,
Центр кибербезопасности «НИИАС»


Наталья ХМЕЛЕВСКАЯ,
РЖД

Денис БАБАЕВ,
АО «ВНИИАЭС»

Олег ГРАФЕЕВ,
НТЦ «Заря»

Евгений БЕЛОВ,
ФУМО СПО ИБ

Проектов по импортозамещению АСУ ТП нет – есть проекты по защите иностранных АСУ ТП.
Николай Домуховский

Начальник отдела мониторинга информационной безопасности НТЦ «Заря» Олег Графеев рассказал о построении отраслевого центра мониторинга КС СОПКА «Роскосмос», построенного на базе его предприятия. До декабря 2020 г. центр функционировал в пилотном режиме, сейчас он заключает договоры с компаниями, находящимися под контролем «Роскосмоса», на предоставление услуг мониторинга информационной безопасности из КС СОПКА «Роскосмос».

На конференции также была представлена концепция защиты промышленных предприятий в рамках цифровизации, которая принята на предприятии «НПП «Исток» им. Шокина». О ней рассказал **начальник отдела информационной безопасности предприятия Дмитрий Гаращенко**. Он отметил, что до недавнего времени используемые на предприятии станки с ЧПУ не были подключены к единой сети, и казалось, что все хорошо. Однако при внедрении системы контроля рабочего времени обнаружилось, что простой дорогостоящих станков составляет 40%. Для того чтобы повысить производительность технологических линий, станки были подключены к единой информационной системе, что обусловило необходимость обеспечить для них информационную безопасность. В компании была построена полноценная комплексная система защиты станков с антивирусами, межсетевыми экранами и SIEM, поскольку предприятие оборонное, а станки произведены в Германии.

Стенд компании «Доктор Веб»

Кадры в безопасности

Актуальную тему обучения специалистов по защите промышленных технологий осветили на конференции представители профильных организаций ФУМО СПО ИБ и МИЭТ. Как известно, с 1 января 2021 г. вступило в силу требование наличия в службе безопасности сертифицированных специалистов по защите. Государственные программы для массового обучения таких специалистов были приняты только в этом году, а действовать они начнут со следующего. Подробности организации обучения ИБ-специалистов рассказал **заместитель председателя Федерального учебно-методического объединения**

Анатолий ХОРЕВ,
МИЭТ

Стенд компании «КСБ-СОФТ»

в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность» председатель ФУМО СПО ИБ Евгений Белов. Он подробно описал новые образовательные и профессиональные стандарты для кадрового обеспечения информационной безопасности российских предприятий. Предполагается, что все вузы России будут выпускать в год до 10 тыс. специалистов по информационной безопасности, что и должно привести к насыщению рынка необходимыми кадрами.

Тему образования развил **заведующий кафедрой ИБ МИЭТ Анатолий Хорев**. Он рассказал о программах подготовки специалистов, которые разработаны в его вузе в соответствии с применяемыми стандартами. Однако, по словам выступающего, было бы правильно, чтобы в формировании программы образования специалистов участвовали компании, где эти специалисты в дальнейшем будут работать. Образовательное учреждение может подготовить специалистов для работы с различными инструментами защиты, но конкретный набор решений лучше формировать под заказ для каждого предприятия в отдельности.

Мы учим, как пытать нарушителей, чтобы не нарушить международные соглашения.
Анатолий Хорев

Посткатегорирование

В целом можно отметить, что у большинства собравшихся на конференции специалистов уже есть понимание процедуры категорирования. Теперь более насущными проблемами становятся импортозамещение средств защиты и АСУ ТП, а также организация комплексной системы обеспечения безопасности, гарантирующей безопасность использования информационных технологий на предприятиях. В некоторых случаях опыт, полученный при построении защиты в промышленных сегментах, был распространен на все информационные системы предприятия.

В рамках конференции было проведено анкетирование слушателей по наиболее актуальным проблемам информационной безопасности. Результаты обзора публикуются отдельной статьей в журнале, однако наиболее важные выводы можно сформулировать и привести здесь. Основной вывод в том, что Федеральный закон № 187-ФЗ подогрел интерес промышленных предприятий к построению системы защиты промышленных сетей,

В идеале нам нужен человек с двумя головами: одна – ИБ, другая – АСУ ТП.

Денис Мареев

Стенд компании R-Vision

что, в свою очередь, потребовало разработки специализированных средств защиты и внедрения в АСУ ТП современных механизмов обеспечения безопасности.

Опрос также показал определенное недоверие к аутсорсингу информационной безопасности, что говорит о плохом качестве работы компаний, предоставляющих подобные услуги. Однако нехватка кадров на рынке информационной безопасности должна подвигнуть компании лучше относиться к аутсорсингу. К тому же современные атаки, особенно действия наемников и кибервойск другого государства, сложно отразить одной командой – требуется объединение усилий, что и позволяют сделать аутсорсинговые команды. В целом у коммерческих центров реагирования сейчас открывается окно возможностей, которое скоро может закрыться, поскольку вузы готовят массовый выпуск специалистов по ИБ промышленных систем.

Следует отметить, что если изначально требования по безопасности промышленных сетей выдвигались в основном ФСТЭК России и ФСБ России, то теперь к этому процессу подключились и отраслевые регуляторы. Они выпускают различные требования, стандарты и методические рекомендации, которые помогают предприятиям ускорить процесс и категорирования, и построения комплексной защиты. Впрочем, и сами предприятия начинают понимать важность внедрения надежных средств обеспечения безопасности.

Частично это связано с пандемией коронавируса, когда резко возросло количество удаленных подключений к информационным системам предприятия, – в сложившейся ситуации только службы ИБ способны предотвратить доступ посторонних к ресурсам предприятия.

Кроме того, цифровизация превращает офлайновые активы в онлайновые, доступ к которым тоже приходится защищать с помощью инструментов ИБ. В опросе было отмечено, что треть современных проектов по цифровизации уже на уровне технического задания содержит требования по обеспечению информационной защиты. Практически все прорывные промышленные технологии – искусственный интеллект, роботизация, индустриальный IoT – также требуют повышения защищенности ключевых информационных систем предприятия. Таким образом, информационная безопасность промышленных объектов оказалась в центре наиболее значимых тенденций развития современных ИТ.

В рамках конференции была организована выставка, где специалисты могли ознакомиться с последними достижениями отечественных разработчиков. Кроме того, было организовано голосование за лучший доклад. Лидерами по результатам подсчета голосов стали заместитель генерального директора по научно-технической работе «УЦСБ» Николай Домуховский, заместитель руководителя Центра кибербезопасности «НИИАС», доктор технических наук профессор Борис Безродный и начальник отдела информационной безопасности «НОРСИ-ТРАНС» Артем Минаков. Поздравляем победителей! ■