Безопасность АСУ ТП:
все только начинается

27–28 февраля в Конгресс-центре МТУСИ состоялась шестая конференция «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». Организатором конференции выступил Издательский дом «КОННЕКТ». Мероприятие традиционно прошло при активном участии ФСТЭК России. На конференцию прибыли делегаты из оперативно-аналитического центра при Президенте Республики Беларусь, Министерства обороны Республики Армении, Министерства энергетики и Государственной технической службы Комитета национальной безопасности Республики Казахстан.
К участию в мероприятии были приглашены представители органов исполнительной власти, предприятий топливно-энергетического комплекса, нефтехимической отрасли, транспортной индустрии, металлургии, машиностроения, оборонно-промышленного комплекса, горнодобывающей промышленности, ЖКХ, а также разработчики средств промышленной автоматизации, производители и интеграторы в области защиты информации. Шестую конференцию «Информационная безопасность АСУ ТП критически важных объектов» посетило более 337 человек (примерно на 100 человек больше, чем в прошлом году).
В этом году стратегическим партнером конференции стала компания «АйТи Бастион», а партнерами выступили «Лаборатория Касперского», Honeywell, ЭЛВИС-ПЛЮС, Positive Technologies, ГК InfoWatch, ГК «Конфидент», ФГУП «НПП «Гамма», ООО «УЦСБ», «АМТ-ГРУП» и КРОК. Спонсорами программы второго дня конференции, который был посвящен практическим аспектам защиты АСУ ТП, стали компании Yokogawa, «ДиалогНаука» и «Модульные Системы Торнадо». За два дня конференции было заслушано 32 доклада представителей регулирующих органов, ключевых участников рынка информационной безопасности, разработчиков АСУ ТП, промышленности и высшей школы.

ЗОКИИ России

В центре внимания конференции были принятый в 2017 г. Федеральный закон № 187-ФЗ и подзаконные акты, разработанные ФСТЭК для его реализации. С принятием этого закона становятся обязательными к исполнению требования по информационной защите критической информационной инфраструктуры РФ в 12 сферах деятельности, в большей части из которых присутствуют АСУ ТП. Закон уже вступил в силу с 1 января 2018 г., и на конференции неоднократно подчеркивалось, что при возникновении ущерба от хакерских атак на предприятия может наступить уголовная ответственность за нарушение правил эксплуатации объектов КИИ вплоть до заключения под стражу сроком на десять лет.

Ключевым в этом году стал доклад **заместителя директора ФСТЭК России Виталия Сергеевича Лютикова** на тему «О безопасности критической информационной инфраструктуры Российской Федерации». В докладе представитель регулятора обнародовал подробности применения подписанного Минюстом 22 февраля приказа ФСТЭК № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» и других подзаконных актов, принятых в рамках закона № 187-ФЗ. Два приказа ФСТЭК № 235 и № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», которые находятся на регистрации в Минюсте, составляют основу требований к информационной безопасности значимых объектов КИИ (ЗОКИИ).

Виталий Сергеевич Лютиков раскрыл в своем докладе особенности нормативной базы и взгляд ФСТЭК России на проблему обеспечения безопасности ЗОКИИ. Однако, чтобы объект стал значимым для КИИ, вначале ему нужно присвоить категорию. Правила категорирования утверждены Постановлением Правительства РФ № 127-ПП от 8 февраля «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». В нем указаны два типа объектов:

Виктор ГАВРИЛОВ,
главный специалист по информационной безопасности, ФИЦ ИУ РАН

Виталий ЛЮТИКОВ,
заместитель директора ФСТЭК России

Андрей ДЕНИСЕВИЧ,
начальник сектора Оперативно-аналитического центра при Президенте Республики Беларусь

сами КИИ, подпадающие под соответствующие сферы деятельности, и значимые объекты КИИ, которые в соответствии с указанными в Постановлении № 127-ПП правилами и показателями критериев значимости прошли категорирование, были отнесены к одной из категорий и внесены в реестр значимых объектов. Эти объекты необходимо защищать в соответствии с требованиями уточняющих приказов ФСТЭК. На организацию их защиты распространяется государственный контроль. В соответствующем постановлении указано, что государственный контроль проводится не реже чем раз в три года.

Если будет определено, что субъекты прошедшего категорирование объекта не попали ни в одну из категорий, это еще не значит, что он не подпадает под действие закона № 187. Он является объектом КИИ, но не является ЗОКИИ. Тем не менее у него остается обязанность реализовать требования подзаконных актов, однако требований для таких объектов будет меньше. Безопасность ЗОКИИ обеспечивается в полном соответствии с требованиями указанных выше приказов ФСТЭК. Причем проведенные процедуры подлежат государственному контролю.

Думали, как всегда, процесс размажется по срокам, но ФСТЭК поработала на славу.

Севостьянов А.В.

В постановлении написано, что перечень объектов КИИ согласовывается с отраслевым регулятором по подведомственным субъектам и в течение пяти дней направляется во ФСТЭК России. Формально уже в 20-х числах февраля – в течение семи дней с момента принятия постановления – должен быть согласован перечень объектов для категорирования. Понятно,

Президиум

Ваши АСУТП уже могут генерировать для кого-то криптовалюту.

Петросюк Г.Г.

Компания «АйТи БАСТИОН»

что сформировать и тем более согласовать перечень в столь короткие сроки затруднительно, хотя эту работу необходимо провести в минимальные сроки. «Мы будем отслеживать скорость процесса. Если он станет неуправляемым и предприятия не будут предпринимать никаких попыток сформировать перечень, мы выйдем в Правительство с предложением установить конкретный срок для предоставления перечня объектов для категорирования, – пояснил Виталий Сергеевич Лютиков. – Но в этом случае срок будет очень небольшой. Причем есть мнение, что следует ввести административную ответственность за нарушение сроков. Если же процесс пойдет сам собой, тогда отпадет и потребность в установлении конкретных сроков».

Сформированный перечень должен быть согласован с вышестоящей организацией. С отраслевым регулятором его согласовывать не надо. Например, предприятие ФГУП, входящее в структуру «Роскосмоса», согласовывает список с ГК «Роскосмос» – вышестоящей для него организацией. Предприятия, подведомственные, например, Минпромторгу, согласовывают перечни категорирования с Минпромторгом. Вначале нужно согласовать список, а потом его утвердить, хотя в постановлении последовательность иная.

В Постановлении № 127-ПП указано, что категорированием занимается комиссия во главе с субъектом КИИ – организацией, обслуживающей объект в указанных в Законе № 187-ФЗ сферах деятельности. Следует отметить, что при определении категорий рассматриваются только системы, которые автоматизируют деятельность в сферах регулирования законодательства о КИИ. Можно не рассматривать второстепенные системы, связанные, например, с пропуском на предприятие, с кадрами и бухгалтерией, если по уставу они не относятся к основным видам деятельности предприятия.

Поскольку Постановление № 127-ПП касается только компьютерных атак и инцидентов, то при оценке угроз и последствий необходимо ориентироваться на целенаправленные воздействия в результате компьютерных атак на систему, а не на случайные аварии или происшествия. При этом следует оценивать ущерб по всем критериям без изъятия, вне зависимости

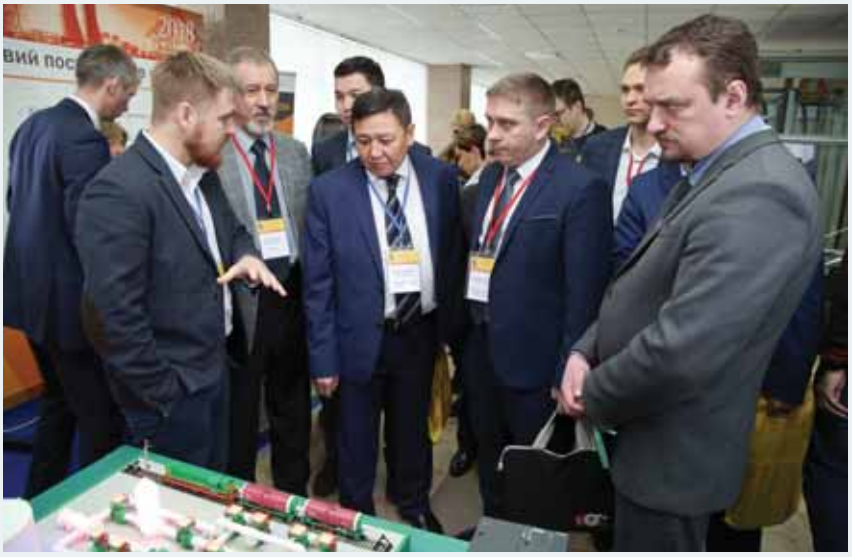
Георгий ГРИЦАЙ,
исполняющий обязанности директора направления «Информационная безопасность», АНО «Цифровая экономика»

Виктор ПОКУСОВ,
председатель ОЮЛ «Казахстанская Ассоциация информационной безопасности»

Александр НОВОЖИЛОВ,
генеральный директор компании «АйТи БАСТИОН»

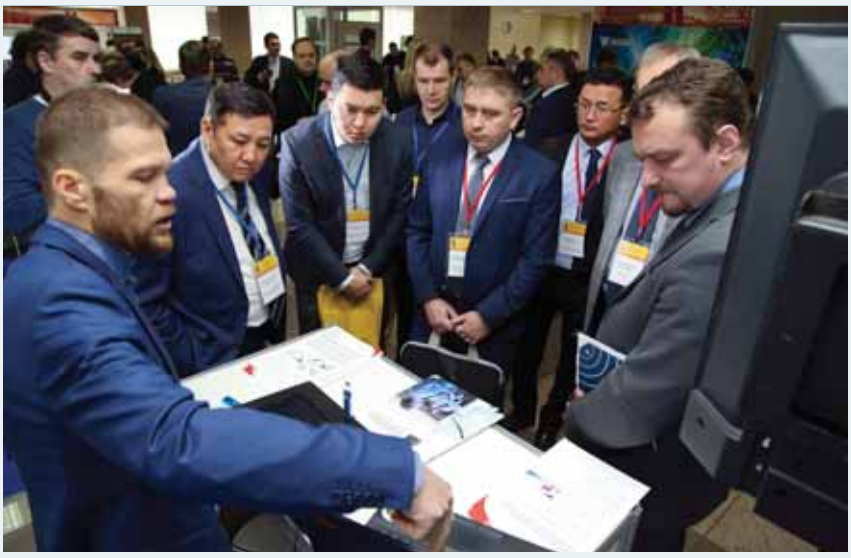
от того, характерны те или иные показатели для данного предприятия. Например, если для предприятий ОПК не нужно оценивать финансовые показатели по нарушению количества операций, то напротив данного показателя ставится отметка «не применим». Кроме того, при категорировании подсчитывать следует только прямой ущерб критическому процессу от нарушения работы информационной системы. Сложные логические цепочки вероятных событий, конечно, строить можно, но их полноту ФСТЭК оценивать не будет.

Если показатели по всем критериям ниже указанных в таблице, то делается вывод, что ни одна из категорий не присвоена, т. е. объект является КИИ, но не ЗОКИИ. Если же хотя бы по одному критерию пределы из таблицы выполнены, то категория объекту присваивается по максимальному значению. Для организации защиты ЗОКИИ необходимо выполнить требования приказов № 235 и № 239. Если приказ № 235 налагает требования на субъекта, у которого есть значимые объекты, и определяет правила организации информационной защиты объектов КИИ, то приказ № 239 налагает требования на сами объекты и определяет правила их защиты.



Компания «Лаборатория Касперского»

В соответствии с приказом № 235 на предприятиях, владеющих ЗОКИИ, необходимо построить систему обеспечения информационной безопасности. Ей должны быть переданы права на обеспечение, в частности, информационных ресурсов, отнесенных к КИИ. ФСТЭК против того, чтобы создавались параллельные организационные структуры для защиты конкретно КИИ. Единственное ограничение: подразделение по информационной безопасности не должно заниматься другими вопросами, такими как внедрение ИТ-решений, сопровождения АСУ ТП и т. п.



Корпорация Honeywell

Если компания заболевает, то она идет к аудитору за диагнозом, но четыре аудита – четыре разных заключения.
Воеводин В.А.

Требования к средствам защиты определяются приказом № 239. В его основу сознательно были положены наработки приказа № 31 ФСТЭК. Разница в мерах между этими приказами после официального опубликования будет минимизирована: все приказы (№ 17, № 21 и № 31) будут приведены ФСТЭК к единой таблице мер. Если меры для реализации различных приказов совпадают, защиту нужно организовывать по максимальным требованиям – набор мер будет унифицированный. Приказы № 17 и № 21 имеют соответствующие ветки законодательства и равную с Законом № 187-ФЗ силу, потому их требования нужно выполнять совместно. Иная ситуация с приказом № 31, где приоритет отдан Закону № 187-ФЗ по защите КИИ. Приказ № 31 отменен не будет – для применения его к тем АСУ ТП, которые не отнесены к ЗОКИИ.

Заметим, что Закон № 187-ФЗ не требует обязательной сертификации: в своих документах ФСТЭК определила, в частности, альтернативные формы оценки соответствия, которые могут

Мы сделали проект информационного диода под названием «ИДИОД», и у нас до сих пор идут споры о его необходимости.

Сердюков О.В.

Компания «ЭЛВИС-ПЛЮС»

применяться для построения защиты. Обязательной сертификация СЗИ является только тогда, когда это установлено другими законами. Для государственных информационных систем такое требование есть в рамках трехглавого Закона № 149-ФЗ. В иных случаях субъект сам организует оценку соответствия при приемке или испытаниях либо для отдельных средств защиты, либо в составе АСУ ТП целиком.

Следует отметить, что и наши ближайшие соседи начинают перестраивать свое законодательство в сфере защиты критически важных объектов. Так, **начальник сектора Оперативно-аналитического центра при Президенте Республики Беларусь Андрей Владимирович Денисевич** прочитал на конференции доклад «Особенности нормативно-правовых аспектов обеспечения безопасности критически важных объектов информатизации в Республике Беларусь», где раскрыл планы по изменению законодательства в сфере защиты критически важных объектов инфраструктуры (КВОИ). В Беларуси их защищают на законодательном уровне с 2011 г., а сейчас планируется модернизация законодательства в этой сфере. В частности, предполагается потребовать от владельцев КВОИ создания подразделения по защите информации (видимо, должен появиться аналог приказа № 235 ФСТЭК) и сформулировать базовые требования к системе безопасности КВОИ (приказ № 239). Предусматривается корректировка отраслевых критериев отнесения объекта к критическим и показателей уровня ущерба. Таким образом, Беларусь фактически повторяет действия России по защите своей критической инфраструктуры.

Подробности о защите критических объектов инфраструктуры в Казахстане рассказал в своем выступлении **председатель ОЮЛ «Казахстанская Ассоциация информационной безопасности» Виктор Владимирович Покусов**. В Казахстане утверждена концепция кибербезопасности «Киберщит Казахстана» и сформирован комитет по информационной безопасности Министерства оборонной и аэрокосмической промышленности, который будет отвечать за обеспечение защиты критически важных объектов. На уровне постановления Правительства в 2016 г. сформулированы

Панельная дискуссия

Алексей КОМАРОВ,
региональный представитель УЦСБ в Москве

Виктор СЕРДЮК,
генеральный директор АО «ДиалогНаука»

Владимир АКИМЕНКО,
руководитель Центра кибербезопасности критических инфраструктур, АО «ЭЛВИС-ПЛЮС»

Павел ЛУЦИК,
руководитель проектов направления информационной безопасности, компания КРОК

Степан ГРИГОРЯН,
ведущий специалист по ТЗИ отдела аттестационных работ екатеринбургского НТЦ ФГУП «НПП «Гамма»

единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, где предусмотрено усиление обеспечения ИБ и ужесточение ответственности за кибератаки. Одной из задач деятельности комитета является создание высокоадаптивной и интегрированной системы управления информационной безопасностью (аналог российской ГосСОПКА).

Практика защиты

Практика применения законодательных норм показывает, что предприятия не торопятся реализовывать требования даже достаточно жестких нормативных актов. Это обсудил в рамках своего доклада «АСУ ТП бессознательного» **генеральный директор компании «АйТи БАСТИОН» Александр Александрович Новожилов**. Он отметил, что предприятия после принятия Закона № 187-ФЗ летом прошлого года ждали разработки уточняющих подзаконных актов, после принятия Постановления № 127-ПП – уточняющих приказов ФСТЭК. Когда все приказы будут приняты, логично появление методических материалов по реализации приказов. Пока никто не торопится ничего реализовывать, полагая, что требования еще поменяются. Новожилов предложил компаниям, владеющим АСУ ТП, стать более сознательными и следить за тем, что происходит в их сетях. Для этого нужно, как минимум, контролировать действия наиболее важных пользователей.

В рамках конференции прошел даже отдельный круглый стол, организованный компанией «АйТи БАСТИОН», на тему «Безопасность производства: восстание людей», где подробно обсуждались вопросы влияния на информационную безопасность человеческого фактора.

На конференции с докладами выступили разработчики и системные интеграторы средств защиты информации, представлявшие практически всех ключевых игроков рынка. Интеграторы рассказали в основном о практике исполнения требований регуляторов при построении АСУ ТП. Некоторые из них уже приступили к подготовке своих клиентов к реализации требований приказов № 235 и № 239 ФСТЭК. В частности, **региональный представитель УЦСБ в Москве Алексей Витальевич Комаров** рассказал в своем докладе «№ 187-ФЗ «О безопасности КИИ РФ» об услугах по реализации требований приказа № 235 и № 239, причем первые четыре контракта его компания уже подписала.

Александр СЕВОСТЬЯНОВ,
начальник отдела защиты информации, ПАО «Трубная металлургическая компания»

Сергей ПОВЫШЕВ,
старший менеджер управления информационной безопасности, АО «Северсталь Менеджмент»

Андрей НУЙКИН,
начальник отдела обеспечения безопасности информационных систем, ЕВРАЗ

С АСУ ТП, как с кариесом, – хотите есть хлеб и получать удовольствие, нужно защищать зубы.

Сердюков О.В.

Аналогичные услуги по реализации требований регуляторов оказывают и другие интеграторы. В частности, **генеральный директор АО «ДиалогНаука» Виктор Александрович Сердюк** в своем докладе «Практический опыт создания системы обеспечения информационной безопасности АСТУ электросетевой компании» рассказал о практике защиты энергетической компании. Особенность предложенного решения заключалась в том, чтобы не устанавливать средства защиты на каждую удаленную подстанцию, но организовать защищенный доступ к ее технологическому оборудованию. В этом случае удалось добиться оптимальной безопасности без излишних расходов на устройства ИБ в защищенном исполнении.

Тему практической безопасности продолжил **руководитель Центра кибербезопасности критических инфраструктур АО «ЭЛВИС-ПЛЮС» Владимир Викторович Акименко**. В докладе «Опыт организации защищенного информационного обмена в системах автоматизации производственных процессов» он рассмотрел особенности применения защиты в промышленном секторе – на нефтегазовом производстве, где была организована однонаправленная передача данных диагностической информации из АСУ ТП в офисную сеть на уровне MES при помощи средств сегментации компании «ЭЛВИС-ПЛЮС».

Руководитель проектов направления информационной безопасности КРОК Павел Луцик в своем докладе «Особенности реализации требований № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» привел пример инициации процедуры категоризации объектов для транспортной отрасли. Он сказал, что для производственных предприятий совсем не обязательно использовать сертифицированные средства защиты – можно организовать проверку соответствия в форме оценки защищенности и приемочных испытаний.

Ведущий специалист по ТЗИ отдела аттестационных работ екатеринбургского НТЦ ФГУП «НПП «Гамма» Степан Григорян в докладе «Необходимость создания систем удаленного мониторинга событий информационной

Компания Positive Technologies

Промышленный коммутатор можно легко превратить в кирпич одной неправильной командой в скрипте.

Краснов Р.А.

ГК InfoWatch

безопасности на объектах критической информационной инфраструктуры» отметил, что «владельцы КИИ при возникновении инцидентов информационной безопасности стараются максимально быстро их устранить, в то время как учет, расследование и принятие мер защиты по результатам инцидента обычно не осуществляются». Эти пробелы и призвана решить ГосСОПКА, которая относится к ведению ФСБ и позволяет учитывать все инциденты, проводить их анализ и рекомендовать предприятиям конкретные меры защиты, адекватные для совершенных на них нападений.

Значительная часть докладов конференции была посвящена обсуждению практических проблем безопасности, но обойти тему современной нормативной базы было невозможно. В частности, **начальник отдела защиты информации ПАО «Трубная металлургическая компания» Александр Владимирович Севостьянов** в своем докладе «Проблемные вопросы категорирования объектов КИИ в рамках Постановления Правительства № 127-ПП» описал ситуацию с реализацией нормативных требований нового постановления. Он, в частности, отметил, что перечень объектов для категорирования стоит отсылать в последний момент, поскольку для процедуры отводится только год, а все средства защиты за это время полноценно внедрить не получится. В то же время реализацию требований приказа № 239 нужно начинать максимально быстро. Естественно, в его компании работа уже ведется.

Начата работа над созданием системы защиты и в «Северстали», о чем в своем докладе «Реализованные проекты по защите критически важных объектов ПАО «Северсталь» рассказал **старший менеджер управления информационной безопасности АО «Северсталь Менеджмент» Сергей Алексеевич Повышев**.

Группа компаний «Конфидент»

Компанией было принято решение о защите от информационных угроз трех АСУ ТП, для которых уже создается система обнаружения и предотвращения неправомерных действий. Для построения такой системы планируется сегментировать компьютерные сети компании, выделив технологические компоненты, организовать защиту от вредоносного ПО и внедрить систему мониторинга инцидентов ИБ на базе SIEM. Изначально в качестве требований планировалось использовать приказ № 31, но сейчас будут учитываться и требования приказа № 239.

О сегментации рассказал и **начальник отдела обеспечения безопасности информационных систем ЕВРАЗ Андрей Витальевич Нуйкин**. Тема его доклада – «Разделение корпоративной и технологической сети. Вопросы масштабирования». Собственно, еще на прошлой конференции он рассказал о принципах сегментации, принятых в международной компании ЕВРАЗ, однако год назад речь шла о пилоте. Предполагалось, что за несколько лет решение можно будет масштабировать на все предприятие,

Проблемы ИБ схожи с гастритом – они у всех есть, но не все об этом знают.

Краснов Р.А.

ФГУП «НПП «Гамма»

однако процесс пришлось ускорять из-за эпидемии WannaCry и других вредоносных программ. В отделенные защитой сегменты АСУ ТП вреднос не попал, а вот там, где технологическая сеть соединялась с офисной, проблемы возникли. Сегментация покрывает большинство требований проекта приказа № 239 ФСТЭК, кроме двух пунктов – обеспечение целостности и защита машинных носителей информации, для закрытия которых придется использовать другие решения.

Илья Борисов, менеджер по ИБ регионального кластера стран СНГ «ТиссенКрупп Индастриал Солюшнс (РУС)», раскрыл в своем докладе тему «Кибербезопасность промышленного производства – от проекта до эксплуатации. Проблемы и решения». Он подробно рассказал о совмещении требований различных стандартов по безопасности, в том числе международных, – для транснациональных компаний такая проблема является достаточно сложной в решении. Однако он отметил, что вполне возможно связать требования приказа № 21 ФСТЭК с требованиями стандартов ISO 27001, NIST SP 800-82, PCI DSS, NERC CIP и др. При этом Илья Борисов отметил, что в документах ФСТЭК не учитывается финансовый аспект защиты: «В методичке ФСТЭК по использованию средств защиты хотелось бы видеть и экономические показатели».

Впрочем, кроме исполнения требований ФСТЭК компаниям приходится строить системы для выявления инцидентов ИБ. Своим опытом в построении ведомственного центра ГосСОПКА поделилась на конференции **директор центра кибербезопасности, ФГУП «ЗащитаИнфоТранс» Наталья Владимировна Хмелевская**, которая прочитала доклад на тему «Опыт создания и дальнейшее развитие ведомственного сегмента ГосСОПКА Минтранса России в 2017–2018 гг.». В докладе было отмечено, что сейчас пока нет готового набора компонентов для построения центров ГосСОПКА, поэтому пришлось самостоятельно подбирать основные компоненты и интегрировать их между собой. Центром системы реагирования является SIEM, которая собирает информацию от других средств защиты и обнаруживает в ней признаки компьютерных атак. На центр реагирования возложены также задачи инвентаризации ресурсов ведомственных сетей и проведения инструментального анализа защищенности.

ООО «УЦСБ»

В рамках цифровизации экономики проблематика импортозамещения по-прежнему остается на повестке дня. Более того, для многих промышленных предприятий из-за внешнего давления импортозамещение и снижение рисков потери технической поддержки для уже внедренных АСУ ТП выходят сегодня на первый план. При этом в России отмечается интеграция производителей АСУ ТП и разработчиков средств защиты. В частности, **генеральный директор «Модульные Системы Торнадо» Олег Викторович Сердюков** в докладе «Влияние систем информационной безопасности

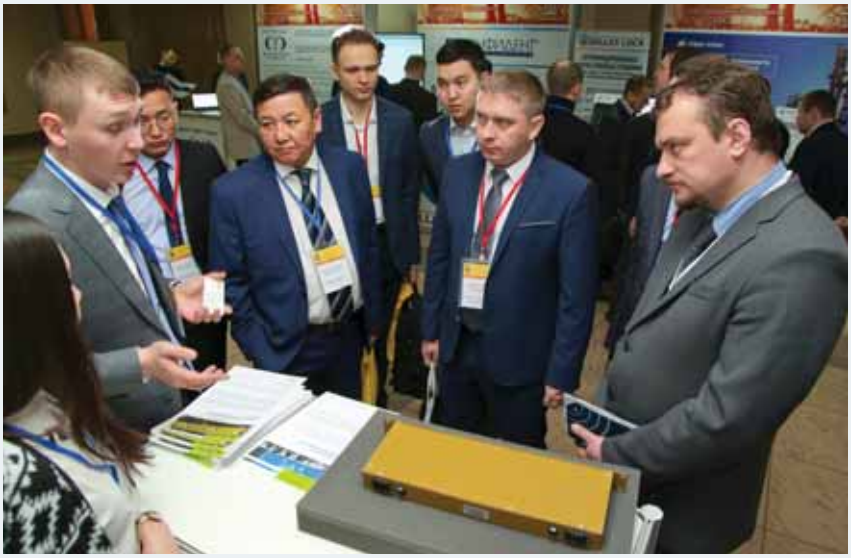
Илья БОРИСОВ,
менеджер по ИБ регионального кластера стран СНГ «ТиссенКрупп Индастриал Солюшнс (РУС)»

Наталья ХМЕЛЕВСКАЯ,
директор центра кибербезопасности, ФГУП «ЗащитаИнфоТранс»

Олег СЕРДЮКОВ,
генеральный директор «Модульные Системы Торнадо»

на целевые функции АСУТП» рассказал о совместном проекте по защите АСУ ТП с компанией InfoWatch, а **руководитель отдела компании «Иокогава Электрик СНГ» Илья Николаевич Мухин**, выступая на тему «Актуальные средства защиты данных АСУ ТП «Иокогава Электрик СНГ» в соответствии с российской законодательной базой», упомянул о совместном проекте с «Лабораторией Касперского».

При этом «Модульные Системы Торнадо» – российский производитель АСУ ТП без специализированных контроллеров – начинает сам разрабатывать компоненты для обеспечения информационной безопасности своих производственных систем. У компании уже есть проект создания информационного диода с рабочим названием «ИДИОД», который должен отделить средства защиты от технологической сети, чтобы не повлиять на работу последней. Правда, инженеры компании до сих пор считают, что правильно настроенный межсетевой экран вполне может заменить информационный диод. В компании также не очень понимают необходимость обновления операционной системы Windows, на базе которой работают все компоненты решения.



Компания АМТ-ГРУП

Наши люди (в Беларуси) соблюдают требования по ИБ, только если их бьют палкой.
Денисевич А.В.

Компания Yokogawa имеет программу для обеспечения защиты на всех уровнях АСУ ТП – от полевых устройств до централизованного управления SCADA. Она занимается сертификацией специализированных средств защиты на предмет их совместимости с АСУ ТП и отсутствия отрицательного влияния защиты на технологические процессы. Кроме того, компания разработала целый пакет документов для удовлетворения требований Закона № 187-ФЗ, куда входят политика безопасности, проекты приказов, регламентов и инструкций, которые клиенты могут взять в качестве примера для разработки всей необходимой по закону организационной документации.

В направлении разработки специализированных средств защиты для их АСУ ТП движутся и другие разработчики. Доклад о подобных разработках для АСУ ТП Honeywell прочитал **консультант по защите АСУ ТП Honeywell Руслан Михайлович Стефанов**. Его компания приобрела производителя специализированных средств защиты под названием ICS Shield. Компания

Если вы не попадаете под категории значимости, это еще не значит, что вы не объект критической инфраструктуры.

Лютиков В.С.

даже получила лицензию ФСТЭК на разработку средств защиты в соответствии с требованиями российского законодательства и открыла два производства – в Арзамасе и Липецке, где будут выпускать компоненты для информационной защиты АСУ ТП.

Впрочем, появляются и российские разработчики АСУ ТП, которые предлагают свои решения с ориентацией на защиту от целенаправленных атак. В частности, **Вадим Подольный, заместитель генерального директора по системной интеграции и кибербезопасности ООО «Московский завод «Физприбор»**, представил на конференции доклад «Настоящее и будущее кибербезопасности АСУ ТП КИИ. Гиперконвергентные решения, облачные технологии VS традиционная жесткая логика», в котором сформулировал новые принципы построения средств защиты технологических процессов. Например, он предложил использовать в АСУ ТП контроллеры на основе различных процессорных архитектур, чтобы появилась возможность сравнивать результаты их работы. Одновременно контроллеры на всех процессорных архитектурах взломать затруднительно, поэтому если один

Илья МУХИН,
руководитель отдела, компания «Иокогава Электрик СНГ»

Руслан СТЕФАНОВ,
консультант по защите АСУ ТП, Honeywell

из контроллеров выдает результат, противоречащий остальным, то его команды можно просто игнорировать и заняться диагностикой неисправности.

Финальным аккордом программы конференции стала панельная дискуссия, ведущим которой стал **главный специалист по информационной безопасности ФИЦ ИУ РАН Виктор Евдокимович Гаврилов**. В процессе дискуссии обсуждались вопросы полноты и качества нормативно-правовой базы, оптимизации проведения работ по выполнению требований регуляторов, квалификации кадров, готовности предприятий из 12 указанных в законе сфер деятельности к реализации мер защиты, привлечения сторонних исполнителей к работам по защите информационных ресурсов КИИ и др. Отмечалась необходимость обеспечения безопасности критических объектов, и без стимулирования этого процесса со стороны государства не обойтись. Важно, чтобы при выполнении требований регуляторов владельцы объектов КИИ не подходили к процессу формально, а реально обеспечивали безопасность своих информационных систем.

Информационная защита промышленных предприятий – это защита цифровых активов с целью цифровой трансформации российской экономики. Принятая в 2017 г. программа «Цифровая экономика» включает в себя направление, посвященное информационной безопасности. Его характеристики описал на конференции **исполняющий обязанности директора направления «Информационная безопасность» АНО «Цифровая экономика» Георгий Анатольевич Грицай**. В своем докладе «Направление «Информационная безопасность» программы «Цифровая экономика Российской Федерации» он раскрыл экономические параметры, заложенные в программу на информационную безопасность.

Программа «Цифровая экономика» принята на уровне распоряжения Правительства № 1632-Р

Компания «ДиалогНаука»

Вадим ПОДОЛЬНЫЙ,
заместитель генерального директора по системной интеграции и кибербезопасности, ООО «Московский завод «Физприбор»

Компания «ICL Системные технологии»

в июне 2017 г. В результате согласования части программы, относящейся к информационной безопасности, было утверждено около 400 мероприятий, на которые планируется потратить до 34 млрд руб., из них 11 млрд – внебюджетных средств государственных институтов развития: фондов «Сколково», ФРИИ, «Развития промышленности» и др.

Не только доклады

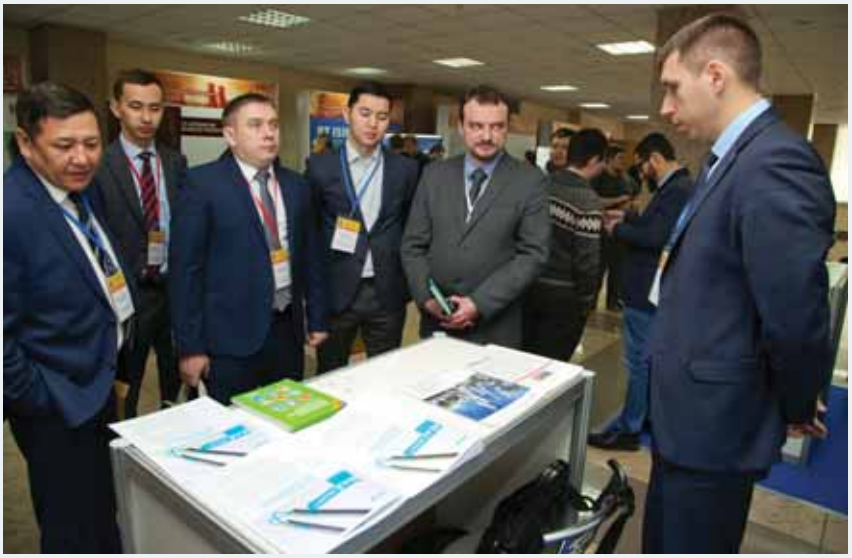
В ходе конференции в фойе работала выставка, на которой было представлено 15 стендов. В ней приняли участие компании «ICL Системные технологии», ООО «Московский завод «Физприбор» и «Сервионика». В частности, Московский завод «Физприбор» демонстрировал модульное шасси для контроллеров АСУ ТП, которые могут быть построены как на основе процессоров классической архитектуры Intel, так и по спецификации ARM. Впрочем, были продемонстрированы и модули контроллеров с однократным программированием, которые не подвержены атакам на перепрограммирование логики. Компания Honeywell представила на выставке специализированный защищенный планшет Secure Media Exchange, который обеспечивает проверку USB-накопителей перед подключением их к отделенным гальванической развязкой элементам АСУ ТП.

Компания «АМТ Групп» демонстрировала на стенде свой информационный диод под названием InfoDiode, который может быть использован для мониторинга безопасности АСУ ТП. Специалисты компании Positive Technologies представили решение PT Industrial Security Incident Manager, которое как раз и может быть отделено диодом данных от АСУ ТП, но позволяет обнаружить признаки информационных атак в технологических сетях с учетом низкоуровневых промышленных протоколов. Группа компаний «Конфидент» показала аппаратные электронные замки, которые обеспечивают целостность первоначальной загрузки операционной системы и будут полезны при построении доверенных решений АСУ ТП.

В выставке принимали участие две компании, оказывающие услуги по обеспечению защиты и мониторинга безопасности АСУ ТП. Одной из них была «ICL Системные технологии», которая имеет собственный SOC и центр компетенции по обеспечению безопасности АСУ ТП. Вторая компания

ООО «Московский завод «Физприбор»

Компания «Сервионика»



Компания «КРОК»

«Сервионика», входящая в группу компаний «Ай-Теко», предложила посетителям полный спектр услуг в области аутсорсинга ИТ-инфраструктуры и облачных вычислений для клиентов среднего, малого и крупного бизнеса, холдинговых структур и госсектора. Такие компании, скорее всего, и будут выполнять основную массу работ по обеспечению безопасности АСУ ТП и приведению их в соответствие с требованиями Закона № 187-ФЗ.

В целом можно отметить, что процесс защиты информационной инфраструктуры только начался, но работа эта необходима, поскольку уже происходят ИБ-инциденты, которые могут и нанести вред компьютерам и оборудованию, и привести к ущербу для страны в виде отключенного электропитания, нарушения работы транспорта или выброса в атмосферу опасных веществ. Сейчас уже нельзя оставить защиту подобных объектов на уровне прошлого века – просто разорвав соединение и не получив данных диагностики от оборудования. Правильная информационная защита АСУ ТП позволит избежать неприятных для всех последствий хакерских атак на промышленные объекты. Принятый закон даст возможность ФСТЭК в самом ближайшем будущем заинтересовать владельцев таких объектов в обеспечении их кибербезопасности. ■