ИБКВО:
Десять лет на службе безопасности АСУ ТП

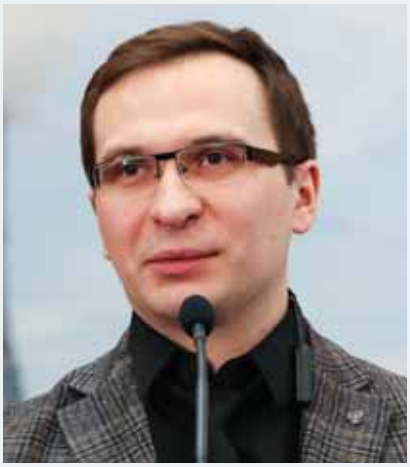
2–3 марта 2022 г. в Москве состоялась Десятая юбилейная конференция «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». Мероприятие прошло при участии ФСТЭК России, Минэнерго РФ, представителей Казахстана и других специалистов по промышленной безопасности РФ. Партнерами конференции в этом году стали ООО «АйТи БАСТИОН», ООО «УЦСБ», «ИнфоТеКС», InfoWatch, Check Point Software Technologies, АО «Лаборатория Касперского», АО «ДиалогНаука», AMT GROUP, CyberLympha, 3Logic Group, «Газинформсервис», Positive Technologies и «Элвис-Плюс». В фойе конференции была организована выставка продукции партнеров, в которой приняли участие компании КРОК, «КСБ-Софт», Angara Security, UserGate, Ideco, Security Vision, Центр компетенции МЭИ и The Stendoff. Спонсорами второго дня конференции стали компании etherCUT, IBS Platformix и «Норси-Транс». Количество участников составило 351 человек. Организатором конференции выступил Издательский дом «КОННЕКТ».

Рекомендации регулятора

Ключевым докладом на пленарном заседании было выступление **заместителя начальника Управления организации обеспечения безопасности КИИ ФСТЭК России (8-е управление ФСТЭК России) Алексея Валентиновича Кубарева**. Он подробно рассказал о первоочередных мерах, которые его ведомство рекомендует принять в условиях массовых атак на объекты информационной инфраструктуры РФ. Ведомство рекомендует всем владельцам информационной инфраструктуры (не только критической) на время повышенной вероятности атак через киберпространство провести следующие мероприятия:

- отключить автоматическое обновление программного обеспечения через сеть Интернет;

Президиум



Алексей КУБАРЕВ,
начальник Управления организации обеспечения безопасности КИИ ФСТЭК России (8-е управление ФСТЭК России)

Виктор ГАВРИЛОВ,
главный научный сотрудник, ФИЦ ИУ РАН

Андрей КОРНЕЕВ,
руководитель Центра проблем энергобезопасности Института США и Канады РАН

- выявить возможные точки проникновения (ВТП) внешнего нарушителя на объекты ИИ;
- ограничить доступ к объектам ИИ через ВТП, в том числе удаленное подключение к объектам и подключение к системам связи общего пользования (ССОП);
- проанализировать уязвимости узлов, являющихся ВТП, в частности, уязвимостей конфигураций и кода прикладного и системного ПО;
- устранить критические уязвимости узлов объектов ИИ, являющихся ВТП;
- активировать все функции межсетевых экранов (в том числе DPI) и других СЗИ, в частности WAF по защите от компьютерных атак и анти-DDoS;
- провести инвентаризацию веб-сервисов и служб, используемых для функционирования сайтов, веб-приложений, и отключить неиспользуемые;
- обеспечить взаимодействие администраторов и пользователей с сайтами и веб-приложениями по защищенным протоколам;
- исключить применение на сайтах сторонних зарубежных сервисов, API и виджетов;
- ограничить количество подключений к ИИ, сайтам и веб-приложениям с каждого IP-адреса;

Модераторы Виктор ГАВРИЛОВ, ФИЦ ИУ РАН (слева), и Дмитрий КОРЕШКОВ, «КОННЕКТ» (справа)

В 25 году новые технологии могут сокрушить оборону всех объектов и организовать глобальную киберпандемию.
Виктор Гаврилов

- сменить аутентификаторы УЗ пользователей ПО, установленного на соответствующих узлах сети;
- ограничить возможность удаленного управления прикладным и системным ПО, телекоммуникационным оборудованием через ССОП;
- исключить применение систем удаленного доступа;
- обновить базы данных антивирусного ПО и решающих правил СОВ;
- организовать анализ критических событий безопасности.

Кроме того, предлагается рассмотреть возможность реализации дополнительных, более сложных мер защиты второй очереди, к которой можно отнести следующие мероприятия:

- настроить межсетевые экраны на блокировку по «белым спискам», блокировку входящего трафика с иностранных IP, из Tor, по ненужным портам и ограничить использование ССОП;
- проверять наличие вредоносного ПО в поступающих незапрошенных электронных сообщениях;

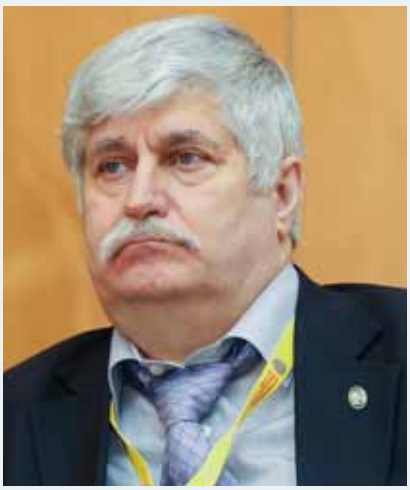
Как обстановка? Можете не отвечать – я и так знаю.

Алексей Кубарев

Стенд компании «АйТи БАСТИОН»

- реализовать многофакторную аутентификацию для удаленного и локального доступа привилегированных пользователей;
- обеспечить мониторинг информационной безопасности объектов ИИ;
- контролировать подключение неучтенных съемных носителей информации и мобильных устройств;
- провести отработку мер противодействия компьютерным атакам, восстановления работоспособности ИИ и устранения последствий компьютерных инцидентов;
- проверить соблюдение ограничений на использование личных СВТ, модемов, накопителей и правил личного использования таких средств;
- проверить соблюдение ограничений на применение наиболее часто используемого при реализации компьютерных атак ПО и правил его безопасного использования;
- проверить соблюдение ограничений на использование ПО, не требуемого для выполнения должностных обязанностей;
- информировать работников и иных лиц, имеющих доступ к объектам ИИ, о необходимости принятия мер по блокированию УБИ и строгого соблюдения требований информационной безопасности;
- актуализировать информацию об объектах КИИ в соответствующих реестрах;
- в случае обнаружения компьютерного инцидента на объектах ИИ незамедлительно связываться с НКЦКИ.

Кроме того, Алексей Валентинович Кубарев поделился опытом проведения первых плановых проверок объектов КИИ и рассказал о выявляемых нарушениях и недостатках. Он отметил, что наиболее частым вектором нападения являются атаки через работников. К таким, например, относится фишинг. Для защиты от этого вида нападений необходимо повышать квалификацию всех сотрудников предприятий в вопросах информационной безопасности. Он так описал текущую ситуацию: «С документами все хорошо, с аппаратным обеспечением в целом тоже, с силами также все нормально – прошли обучение и получили необходимые сертификаты, а вот с процессами организации защиты КИИ по-прежнему остаются проблемы».



Евгений НОВИКОВ,
заместитель директора департамента экономической безопасности, Минэнерго России

Антон БЕРЕЗОВСКИЙ,
консультант по информационной безопасности, Check Point

Обстановка в мире

Мировая обстановка сейчас не самая простая с точки зрения информационной безопасности. Обзор информационной безопасности и развития рынка средств защиты АСУ ТП за последние десять лет сделал **главный научный сотрудник ФИЦ ИУ РАН Виктор Гаврилов**. Он отметил, что сложность атак продолжает возрастать, а компетенции для проведения масштабных атак – снижаются. При этом до 60% уязвимостей для эксплуатации не требуют взаимодействия с пользователем. По прогнозам Всемирного экономического форума, в 2025 г. новые технологии могут достигнуть такого состояния,

что с их помощью можно будет сокрушить оборону всех объектов и организовать глобальную киберпандемию. В новых продуктах все чаще встречается избыточный функционал, который отрицательно сказывается на безопасности. Переход на системы с необходимым минимумом функциональности, но более защищенные поможет предотвратить их последующий взлом.

О принципиально новом курсе регулирования и обеспечения кибербезопасности в США и Канаде рассказал в своем докладе **руководитель Центра проблем энергобезопасности Института США и Канады РАН Андрей Корнеев**. В новой парадигме защиты предполагается, что спецслужбы США должны иметь доступ к любому компьютеру и любой системе на всем земном шаре, но при этом полностью защитить собственные системы от постороннего вмешательства. Предусматривается разработка механизмов, с помощью которых обеспечивается возможность блокировать или выводить из строя любые информационные системы других государств. Для собственных компаний в этих странах пропагандируется переход на архитектуру нулевого доверия (Zero Trust), которая предполагает, что безопасных систем нет и любой блок может быть скомпрометирован. Поэтому нужен постоянный контроль за всеми событиями, происходящими в системе, с привязкой их к конкретным пользователям. Причем все события необходимо записывать и собирать их в централизованные хранилища для дальнейшего анализа. Лучше всего делать это в облаках американских производителей средств защиты, что позволит создать условия для тотального контроля всех действий пользователей в информационных системах со стороны американских компаний.

Российские подходы на пленарном заседании озвучил **заместитель директора департамента экономической безопасности Минэнерго России Евгений Владимирович Новиков**, который рассказал о практике реализации требований Закона № 187-ФЗ «О безопасности КИИ РФ» в рамках ТЭК. Министерство несколько лет назад создало ведомственный центр ГосСОПКА, а сейчас проводит пилотное тестирование отраслевого центра, в котором участвуют 12 компаний из отрасли. В России сбором и анализом всех событий занимается иерархическая система ГосСОПКА, которая как раз и обеспечивает защиту российской критической информационной инфраструктуры.

В целях реализации требований по безопасности КИИ ведомство подготовило и согласовало

Гаечным ключом можно удалить все записи о нападении.
Константин Родин

с ФСТЭК методические рекомендации для подотчетных компаний по проведению процедуры категорирования, однако далеко не все представители отрасли ее завершили. Кроме того, на базе отраслевого института МЭИ сформирован специализированный киберполигон для отработки действий служб ИБ в энергетической отрасли по обнаружению и отражению атак. Сейчас важно не только построить систему защиты, но и научиться ею пользоваться.

Особенности защиты промышленных сетей

В пленарной секции первого дня конференции обсуждалось развитие рынка информационных технологий в России. Общие тренды развития представил **консультант по информационной безопасности Check Point Антон Березовский**. Он отметил необходимость разделения операционных сетей, в которых обычно функционирует АСУ ТП, и офисных информационных с настройкой качественного контроля взаимодействия этих сегментов. Причем инструменты контроля должны

Марина СОРОКИНА,
руководитель направления развития продуктов, компания «ИнфоТеКС»

Константин РОДИН,
руководитель технического центра, компания «АйТи БАСТИОН»

Роман НЕСТУЛЯ,
директор компании etherCUT, к. ф.-м. н.

У студентов квалификация практически такая же, как у опытных разработчиков.

Вячеслав Половинко

быть максимально автоматизированы, чтобы для их настройки не требовались высокие компетенции, поскольку специалистов, которые могли бы разобраться в защите объектов промышленной автоматизации, обычно не очень много и стоят они дорого.

Однако нередко промышленные сегменты удалены от офисных на значительные расстояния, потому для их подключения приходится использовать те самые ССОП, доступ к которым рекомендуется строго ограничить. Тем не менее использовать их приходится, но с соблюдением специальных требований – о них рассказала **руководитель направления развития продуктов компании «ИнфоТеКС» Марина Сорокина**. Владельцы объектов критической инфраструктуры обычно пользуются ССОП для подключения удаленных объектов, часто даже не подозревая, что у Минцифры есть отдельные правила обеспечения безопасности для подобных подключений, утвержденные приказом № 75. В то же время к ССОП относятся и мобильные сети, и арендованные проводные и оптические линии связи, и новомодные подключения по технологии NB-IoT. При этом каждый сегмент, подключенный с помощью ССОП к центральному офису, должен рассматриваться как отдельный, с вытекающими из этого требованиями по категорированию, моделированию угроз и организации его защиты.

Об инструментах контроля внутренних коммуникаций рассказал в своем выступлении и **руководитель технического центра компании «АйТи БАСТИОН» Константин Родин**. Его компания производит систему контроля действий привилегированных пользователей (СКДПУ), которая обеспечивает запись всех действий наиболее опасных

Вячеслав ПОЛОВИНКО,
руководитель направления собственных продуктов, Департамент информационных систем АМТ-ГРУП

Алексей КОМАРОВ,
руководитель практики ИБ АСУ ТП, компания CyberLympha

пользователей – ИТ-администраторов и аутсорсеров. Основным направлением развития СКДПУ является интеграция с различными средствами защиты – антивирусами, системами мониторинга и обнаружения вторжений, инструментами надежной аутентификации и др. В опубликованном выше списке первоочередных действий, рекомендованных ФСТЭК по защите объектов информационной инфраструктуры, с помощью СКДПУ можно обеспечить реализацию таких пунктов, как ограничение возможности дистанционного управления, анализ критических событий информационной безопасности и т. д. В целом же контроль действий привилегированных пользователей относительно объектов КИИ становится важной частью корпоративной инфраструктуры защиты.

Более радикальное средство контроля взаимодействия операционных и информационных сетей предложил на конференции **директор компании etherCUT, к. ф.-м. н. Роман Нестуля**. Для надежной изоляции некоторых промышленных сегментов можно использовать ручную физическую сегментацию сетей АСУ ТП КИИ, т. е. физический разрыв Ethernet-соединения.

Стенд компании ИнфоТеКС

Денис ШМЫРЕВ,
заместитель руководителя Центра экспертизы по информационной безопасности, IBS Platformix

Иван ЧЕРНОВ,
менеджер по развитию, компания UserGate

Евгений ДРУЖИНИН,
эксперт компании КРОК

Устройства компании позволяют с помощью физического ключа разорвать Ethernet-соединение с сегментами, подключение которых к любым сетям нецелесообразно, и подключать обратно, например для проведения регламентных работ. Такой Ethernet-выключатель может стать ключевым элементом системы физической защиты промышленных сетей.

Вторым вариантом физической защиты является однонаправленная передача данных с помощью информационного диода – эту тему уже несколько лет развивает на нашей конференции компания АМТ-ГРУП. **Руководитель направления собственных продуктов из департамента информационных систем Вячеслав Половинко** рассказал о возможностях средства однонаправленной передачи данных для мониторинга промышленных сетей и сегментов, физически отрезанных от всех остальных коммуникаций, например с помощью Ethernet-выключателя, описанного выше. Для этих устройств находятся и другие применения. В частности, для защиты конфиденциальных сегментов офисной сети, где необходимо организовать получение данных извне и полностью блокировать утечки информации наружу.

Впрочем, даже для самых защищенных сегментов необходимо регулярно проводить оценку их защищенности, чтобы определить, насколько точно соблюдаются требования по полному отключению промышленных сегментов. Для проведения подобной оценки компания CyberLympha разработала мобильный комплекс контроля защищенности АСУ ТП и проверки реализации требований Закона № 187-ФЗ. О его возможностях рассказал на конференции **руководитель практики ИБ АСУ ТП компании CyberLympha Алексей Комаров**. Это не просто мониторинговый инструмент – он должен работать в режиме запрос – ответ с АСУ ТП, чтобы максимально подробно определить, насколько правильно организована ее защита. В штатном режиме функционирования данный инструмент использовать нецелесообразно – достаточно включать его во время регламентных работ для подготовки отчетов по защищенности промышленных объектов. Инструмент разработан недавно и сейчас находится в фазе активного развития, тем не менее уже имеется достаточно большое количество его установок на промышленных предприятиях.

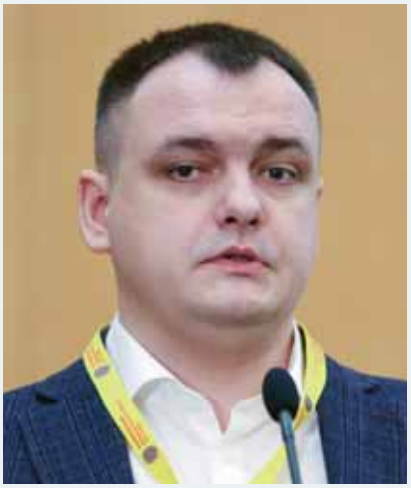
Комплексная защита

Однако отдельные инструменты защиты необходимо еще объединить в работающую систему.

Больше всего пострадал завод, у которого не было ручного привода.
Антон Березовский

Решением этой задачи обычно занимаются интеграторы. В этом году их выступления были сконцентрированы на различных аспектах построения комплексных систем защиты промышленных объектов. О принципах построения наложенных средств защиты для систем АСУ ТП рассказал на конференции **заместитель руководителя Центра экспертизы по информационной безопасности IBS Platformix Денис Шмырев**. Он подробно остановился на методах тестирования совместимости наложенных СЗИ с встроенными элементами защиты и самой АСУ ТП. Тему продолжил **менеджер по развитию компании UserGate Иван Чернов**, который рассказал об особенностях интеграции наложенных средств в технологические процессы предприятия и влиянии средств защиты на работу автоматизированных систем управления. Своими лучшими практиками построения систем защиты поделился и **эксперт интегратора КРОК Евгений Дружинин**. Он сконцентрировал внимание на безопасности в процессе модернизации АСУ ТП и ее удаленном администрировании.

Азат ШАЙХУТДИНОВ,
менеджер по развитию бизнеса, Kaspersky ICS



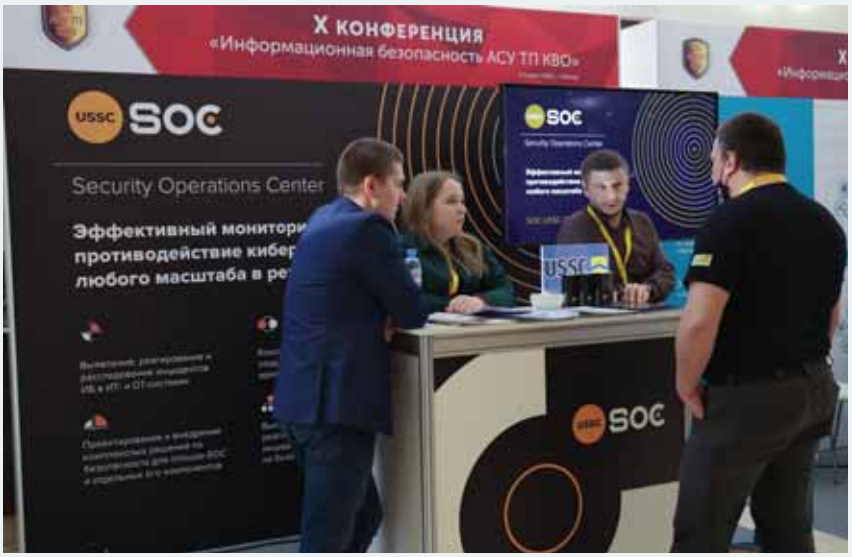
Николай ДОМУХОВСКИЙ,
заместитель генерального директора по научно-технической работе, УЦСБ

Алексей АНАСТАСЬЕВ,
руководитель направления по развитию бизнеса департамента развития бизнеса, компания Positive Technologies

ИБ-специалисты не знают магию искусственного интеллекта.

Николай Домуховский

Важным элементом защиты является система управления всеми перечисленными инструментами защиты, анализа поступающей от них информации и блокирования обнаруживаемых атак. Поиском признаков нападения в собираемой из других средств защиты информации занимаются системы обнаружения вторжений (СОВ). Их возможности и принципы выбора стали темой выступления на конференции **менеджера по развитию бизнеса Kaspersky ICS Азата Шайхутдинова**. С точки зрения Закона № 187-ФЗ именно СОВ является основным элементом обнаружения атак, который должен быть включен в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Именно СОВ собирает мониторинговые данные, обрабатывает их для выявления признаков атак и уже выявленные инциденты отсылает в системы более высокого уровня – SOC или напрямую в ГосСОПКА. В качестве источника информации об уязвимостях, которые СОВ использует для обнаружения признаков работы эксплойтов, желательно использовать не только отечественные банки данных угроз и уязвимостей, которые поддерживает ФСТЭК, но и международные источники. Уникальность разработки СОВ от «Лаборатории Касперского» заключается в том, что она получает информацию о процессах защиты из инструмента проектирования системы защиты Security CAD – недавней разработки компании.



Стенд компании УЦСБ

Если СОВ занимается обнаружением вторжений, то реагирование на них – это задача Security Operations Center (SOC). **Заместитель генерального директора по научно-технической работе УЦСБ Николай Домуховский** сконцентрировался на модернизации интеллектуальных возможностей центра реагирования на события информационной безопасности, отметив, что ИБ-специалисты не знают магию искусственного интеллекта, хотя именно SOC владеет хорошим набором размеченных данных. Он предложил использовать в составе SOC инструмент на базе искусственного интеллекта, которым могли бы по анализу размеченной статистики выявлять аномальные события и обнаруживать опасное

Валерий ФИЛИН,
технический директор,
компания CITUM

Федор ТРИФОНОВ,
руководитель отдела технического сопровождения продаж,
компания ИНФОВОТЧ АРМА

поведение информационных систем и средств защиты. Тему автоматизации и интеллектуализации SOC продолжил **руководитель направления по развитию бизнеса департамента развития бизнеса компании Positive Technologies Алексей Анастасьев**, который рассказал о том, как построить «автопилот для СОВ и SOC», который мог бы управляться одним человеком и сделать неприемлемые события невероятными. По его словам, это можно реализовать с помощью новой версии давно известного продукта PT ISIM, где в версии 4.1 реализованы механизмы полного контроля цепочки инцидентов для предотвращения атак на значимые активы компании.

Из доклада **технического директора компании CITUM Валерия Филина** можно было узнать о работе системы автоматизации тестов на проникновение Pentera Automated Security Validation. Из известных элементов она создает такую последовательность событий, чтобы специалист для контроля средств защиты мог максимально точно имитировать действия хакера по проникновению в информационные системы жертвы и добиться совершения невероятных, но критических для предприятия событий. **Руководитель отдела технического сопровождения продаж компании ИНФОВОТЧ АРМА Федор Трифонов** предупредил, что спецслужбы США предложили президенту Джо Байдену использовать кибероружие против российской критической инфраструктуры. С конца февраля отмечается резкий рост числа подобных атак, что требует максимально бдительно подходить к эксплуатации средств защиты КИИ.

В целом векторы современных атак давно известны, тем не менее определенные изменения в попытках взлома присутствуют. В частности, в последнее время отмечаются попытки проникновения посторонних через инфраструктуру партнеров (supply chain). Увеличение числа подобных попыток отметил в своем докладе **руководитель отдела анализа защищенности Angara Security Сергей Гилев**: восемь атак было зафиксировано в 2020 г.,16 – только за первое полугодие 2021 г. Среди них случай с SolarWinds Inc., когда угрозе подверглись информационные системы огромного количества клиентов данной компании. Защититься от атак через поставщиков особенно сложно – это требует контроля всех обновлений от производителей. Поэтому в списке первоочередных мер защиты, опубликованном ФСТЭК, содержится требование по отключению обновления ПО, поскольку

Некоторая часть зоопарка в ближайшее время отвалится.
Федор Трифонов

именно через этот канал появляется возможность получить либо вредоносное обновление, либо деактивацию уже используемых продуктов компаний, которые покинули российский рынок. Атаку через поставщика наиболее трудно предотвратить, особенно если он сам заинтересован в проведении подобной атаки. Таким образом, импортозамещение – элемент общенациональной защиты информационных систем страны.

После введения жестких ограничений на поставки иностранных решений из большинства высокоразвитых стран вопрос о переходе на российские продукты стоит максимально остро. И если программных решений достаточно много, то с аппаратной поддержкой могут возникнуть проблемы. Действительно, большинство программных средств защиты ориентировано на Windows, основной аппаратной платформой для которой являются процессоры Intel. Однако и Microsoft, и Intel объявили о прекращении поддержки своих российских пользователей. В результате важным элементом защиты становятся отечественные аппаратные решения. О них, в частности, рассказал **начальник отдела информационной безопасности ЗАО «НОРСИ-ТРАНС» Артем Минаков**. Его компания выпускает готовые решения на базе отечественных процессоров «Эльбрус-8С», «Эльбрус-8СВ» и «Байкал-М». Причем в ассортименте компании есть как классические серверные решения, так и готовые системы хранения. Есть даже готовая ПАК «Яхонт-112», которая представляет собой комплекс архивного хранения и доступа к информации обращений в «Системе-112», ЕДДС и других экстренных служб. Аналогично разработано и решение PACS «НТ», которое является DICOM-системой хранения и доступа к результатам

Стенд компании ГРАВИТОН

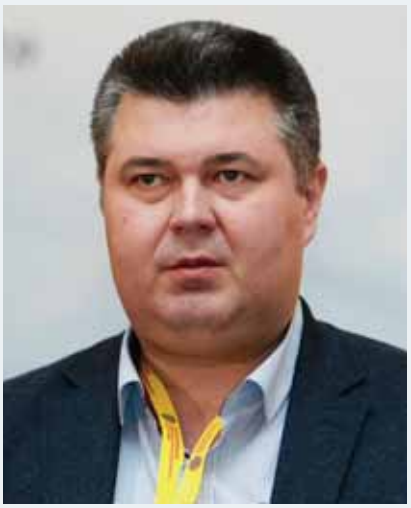
> *В России мало компаний, которые страдают от ИБ-рисков.*
>
> **Азат Шайхутдинов**

медицинских исследований. У компании разработано еще несколько решений для массового внедрения в государственные информационные системы.

Аналогичным бизнесом занимается и **компания ГРАВИТОН, руководитель департамента серверных систем которой Александр Фильченков** рассказал о планах по выпуску на рынок серверов, моноблоков, персональных компьютеров и ноутбуков на отечественных процессорах. Уже сейчас компания выпускает серверы и системы хранения на отечественных процессорах, создав на их базе даже собственное облако под названием Helius. В нем можно арендовать вычислительные мощности отечественных процессоров «Эльбрус», «Байкал», «Элвис» и «Модуль», чтобы у разработчиков программного обеспечения была возможность проверить работоспособность своего ПО на соответствующей аппаратной базе. До конца текущего года компания рассчитывает разработать и выпустить ноутбуки, моноблоки и терминалы на базе отечественного процессора «Байкал М», а также настольные компьютеры и терминалы с процессором «Эльбрус 2С3» (после его выпуска). Правда, работать эти устройства будут под управлением операционных систем семейства Linux – ALT Linux и AstraLinux. Сама компания ГРАВИТОН входит в группу компаний 3Logic Group, которая занимается переводом инфраструктуры российских заказчиков на комплексные отечественные решения.

Для компаний, которые подпадают под действие законодательства о критической информационной инфраструктуре, важно не только выполнить все требования отечественных регуляторов, но и доказать это документарно. **Руководитель центра кибербезопасности критических инфраструктур системного интегратора «ЭЛВИС-ПЛЮС» Владимир Акименко** описал концепцию организации подобного документарного обеспечения системы защиты. Он предложил разделить набор документов на шесть групп: концепция системы управления информационной безопасности (СУИБ); стандарты и положения, описывающие СУИБ; положения о структурном подразделении, комиссиях, назначении работников и должностные инструкции, необходимые для функционирования СУИБ; ТЗ на СЗИ, модели угроз

Сергей ГИЛЕВ,
руководитель отдела анализа защищенности, Angara Security



Артем МИНАКОВ,
начальник отдела информационной безопасности, ЗАО «НОРСИ-ТРАНС»

Александр ФИЛЬЧЕНКОВ,
руководитель департамента серверных систем, компания ГРАВИТОН

и нарушителей, проектно-сметная и эксплуатационная документация на СУИБ; регламенты реализации организационных мер, планы реагирования на инциденты и взаимодействия с ГосСОПКА, инструкции по безопасной работе; план мероприятий, документы работы комиссии по категорированию, акт работы комиссии по контролю состояния безопасности и отчет о выполнении плана мероприятий по обеспечению безопасности. Все документы нужно составить, проверить их соответствие требованиям регуляторов и ввести в действие. Скорее всего, при этом придется использовать специализированную систему управления нормативно-справочной документацией, которая ориентирована на соблюдение требований Закона № 187-ФЗ.

Впрочем, подобные решения уже разработаны и активно эксплуатируются, например в энергетической отрасли. Одной из таких систем был посвящен доклад **начальника отдела защиты объектов КИИ и АСУ ТП компании «КСБ-СОФТ» Анатолия Белинова**. Он рассказал о разработанной его компанией системе специализированного документооборота «АльфаДок», которая обеспечивает как подготовку первичных документов для проведения категорирования объектов КИИ, так и моделирование угроз с последующим управлением инцидентами. Решение компании может пригодиться при вводе и изменении данных в системе на всех этапах организации защиты, при разработке документации по защите информации, при согласовании моделей угроз, при подготовке и прохождении проверок регуляторов, при построении технической защиты информации и аттестации информационных систем. Компания уже внедрила инструмент в 3800 российских компаниях из энергетического, химического и промышленного секторов российской экономики.

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

Анатолий БЕЛИНОВ,
начальник отдела защиты объектов КИИ и АСУ ТП, компания «КСБ-СОФТ»

Хорошо бы сместить время работы ИБ-специалистов в сторону технических мер от бумажной работы.
Анатолий Белинов

Практика использования

Второй день конференции начался с дискуссии между разработчиками средств защиты и их пользователями. Основной темой была организация диалога между всеми участниками процесса обеспечения безопасности промышленных объектов: разработчиками средств защиты, ИТ-подразделениями, инженерами АСУ ТП, разработчиками оборудования для промышленной автоматизации и службами ИБ на предприятиях. Среди обсуждаемых вопросов были следующие: в чем сходство и различие подходов в организации ИБ у промышленных компаний и производителей СЗИ; чем отличаются понятия, используемые сторонами, и возможно ли выработать общие подходы; как обе стороны понимают функциональную безопасность объектов автоматизации; на что готовы тратить бюджет промышленные предприятия в рамках защиты КИИ и на что рекомендуют в первую очередь тратить ИБ-компании; хватает ли на рынке кадров в области защиты АСУ ТП и достаточно ли у них компетенций для защиты промышленных объектов?

Давид МАМЕДОВ,
начальник службы информационной безопасности, ТОО «АЭС Шульбинская ГЭС»

Наталия УСТИЧ,
руководитель направления по информационной безопасности АСУ ТП, ПАО «Интер РАО»

Александр СЕВОСТЬЯНОВ,
начальник управления информационной безопасности, СЭБ ПАО «ТМК»

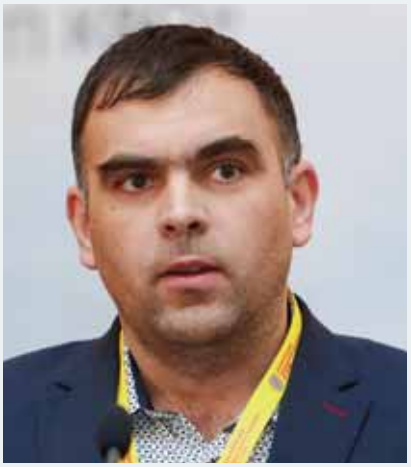
Информационная безопасность – это не бокс, это самбо или даже танец.

Давид Мамедов

Сейчас необходимость диалога между сотрудниками служб ИБ, ИТ и АСУ ТП уже никем не оспаривается, поскольку всем понятно, что требуется координация деятельности всех сторон для повышения эффективности защиты от попыток дистанционного взлома оборудования и остановки технологических процессов. Основной задачей, которую должны решать участники процесса обеспечения защиты промышленной системы, является не сохранение информации, а обеспечение функциональной безопасности при работе оборудования. Инструменты ИБ должны защитить функциональные элементы технологического процесса от постороннего вмешательства и нарушений. Наиболее активное обсуждение развернулось вокруг минимально необходимого набора технических средств и организационных мер, которые позволили бы эффективно защитить объекты КИИ предприятия от постороннего вмешательства со стороны злоумышленников. Практики на предприятиях готовы использовать инструменты с минимальным набором функций и не хотят платить значительные суммы за удобство и избыточный функционал.

Доклады представителей промышленных предприятий на конференции были связаны в основном с решением довольно узкого круга задач, которые приходится решать их компаниям, однако вызвали живой интерес у собравшихся, поскольку те в свое время тоже сталкивались с аналогичными «мелочами». Так, **начальник службы информационной безопасности ТОО «АЭС Шульбинская ГЭС» Давид Мамедов** рассказал о своем подходе к построению и определению принципов работы службы ИБ. Он отметил, что основная цель промышленной кибербезопасности – обеспечение безопасности жизни и здоровья людей, поскольку среди возможных рисков – инциденты со смертельным исходом. Именно такие инциденты и нужно относить к недопустимым событиям.

Руководитель направления по информационной безопасности АСУ ТП ПАО «Интер РАО» Наталия Устич подробно разобрала решение задачи сбора событий информационной безопасности с оборудования



Константин КУРТУКОВ,
менеджер по безопасности критической информационной инфраструктуры, ООО «Распадская угольная компания»

Сергей ПОВЫШЕВ,
старший менеджер – руководитель направления, АО «Северсталь Менеджмент»

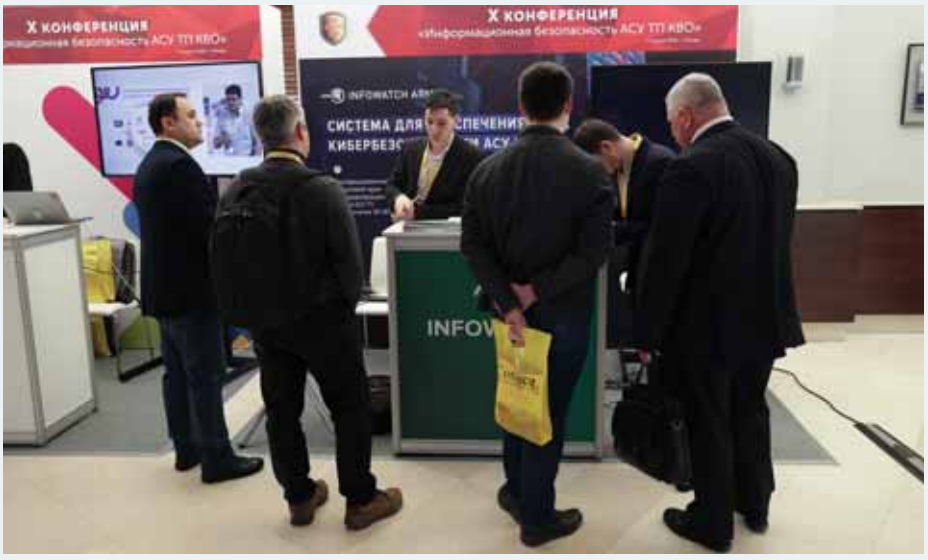
ПТК АСУТП. Она рассмотрела методику выбора целей, событий и объектов мониторинга, формирования перечня инцидентов, которые требуют немедленного реагирования. А **заместитель генерального конструктора ФГУП «НПЦ автоматики и приборостроения им. академика Н.А. Пилюгина» Геннадий Румянцев** провел замечательную презентацию отечественной операционной системы Astra Linux, которая может эффективно использоваться для решения задач информационной безопасности.

Опытом организации защиты промышленных систем поделился **начальник управления информационной безопасности СЭБ ПАО «ТМК» Александр Севостьянов**, который провел краткий анализ текущей ситуации с обеспечением информационной безопасности в металлургии. Он отметил, что велика вероятность приостановления и отказа в продлении технической поддержки оборудования, увеличения числа атак на промышленные сегменты, распространения вредоносного ПО через партнеров и подрядчиков, отключения иностранных облаков и острой нехватки высокопроизводительных серверов и оборудования АСУ ТП. Кроме того, обострятся проблемы, связанные с нехваткой квалифицированных специалистов, которые должны обеспечивать защиту промышленных объектов.

Менеджер по безопасности критической информационной инфраструктуры ООО «Распадская угольная компания» Константин Куртуков подробно рассмотрел процесс исполнения требований Закона № 187-ФЗ, начиная с процесса категорирования, который стартовал в компании в августе 2019 г., через проектирование средств защиты и согласование законодательных требований до внедрения системы безопасности, проведения ее приемочных испытаний и введения в строй. Процесс завершился к июлю 2021 г.

Постараюсь представить на слайде поиски дьявола, который кроется в деталях.
Наталия Устич

Старший менеджер – руководитель направления АО «Северсталь Менеджмент» Сергей Повышев рассказал о структурировании удаленной работы. До недавнего времени компания использовала различные инструменты для удаленного доступа, однако быстро было установлено, что и злоумышленники могли использовать те же инструменты для проникновения внутрь информационной системы предприятия. Поэтому было принято решение централизованно развернуть единую систему удаленного доступа, причем с использованием российского программного решения. Компания выбрала продукт под названием «Ассистент», который подключался к сети через СКДПУ. Остальные средства удаленного доступа были полностью заблокированы. Тесное взаимодействие с разработчиком решения позволило подточить продукт под требования компании, что вряд ли удалось бы при внедрении иностранных решений.



Стенд ГК InfoWatch

Если человек не разбирается, то ему предлагают наиболее дорогие продукты.

Андрей Нуйкин

КИИ России

Всего в рамках конференции было заслушано 35 докладов. Модераторами были **главный научный сотрудник ФИЦ ИУ РАН Виктор Евдокимович Гаврилов и заместитель генерального директора ИД «КОННЕКТ» Дмитрий Юрьевич Корешков**. В фойе конференции была организована выставка продукции партнеров. Среди участников конференции прошел опрос, результаты которого ищите на страницах нашего журнала.

В рамках выступлений на конференции неоднократно звучало мнение, что российские регуляторы сделали все возможное, для того чтобы построить государственную систему обеспечения безопасности критической информационной инфраструктуры, – подготовили всю нормативную базу, сформировали стандарты, подготовили разработчиков средств защиты для перехода на отечественные платформы и даже сформировали государственную систему обнаружения инцидентов и реагирования на них. Остался только вопрос формирования отраслевых центров ГосСОПКА, которые не упоминаются в законодательных актах, но потребность в их создании есть. В банковской сфере FinCERT существовал изначально, а сейчас Минэнерго тестирует собственный отраслевой центр. Вполне возможно, что и другим ведомствам будет полезно воспользоваться опытом лидеров построения государственной кибероборонны.

Когда совершаются массовые атаки на российскую инфраструктуру как иностранными государственными службами, так и хактивистами, построенная система проходит боевое крещение. Пока результаты этих атак не очень понятны, однако серьезных жертв на коротком промежутке времени удалось избежать, что говорит о достаточной эффективности работы ГосСОПКА. Да, были зафиксированы несколько дефейсов государственных сайтов и ведомств, утечки конфиденциальной информации – в основном из коммерческих инфраструктур, которые фактически не относятся к КИИ, но значительных нарушений в работе банковской системы, российского сегмента Интернета или крупных промышленных систем зафиксировано не было. Таким образом, проделанная за несколько лет работа по повышению защищенности российских промышленных предприятий от атак через киберпространство оказалась эффективной.

Да, с точки зрения установленных государством требований не все компании и не в должной мере реализовали предписания регуляторов – нужно продолжать работу в этом направлении. Однако за десять лет проведения конференции предприятиями критически важных объектов сделано достаточно много, чтобы предотвратить в том числе профессиональные атаки на собственную корпоративную инфраструктуру. Однако требования регуляторов являются разрозненными, т. е. в приказах нет требований по интеграции всех инструментов в единую систему реагирования. Предполагается, что компании, закупив необходимое оборудование и приняв на работу соответствующих специалистов, сами создадут систему реагирования на инциденты. Но далеко не все компании способны самостоятельно наладить процессы обеспечения безопасности. Назрела необходимость разработки методологии по процессам обеспечения безопасности, которые рекомендуется организовать в рамках системы управления информационной безопасностью на предприятиях.

На конференции также было отмечено, что документы по КИИ концентрируются вокруг защиты ИТ-инфраструктуры, однако для предприятий не менее важно обеспечить функциональную и промышленную безопасность, которая сейчас также зависит от функционирования ИТ. В промышленности уже достаточно давно разработаны подходы к обеспечению функциональной и промышленной безопасности, правда, базируются они на несколько других принципах – случайности аварий и катастроф. Сегодня ИТ-компоненты можно целенаправленно использовать для провоцирования промышленных аварий, что требует от промышленных предприятий пересмотра подходов к работе всех инструментов защиты. Именно учет подобных отраслевых особенностей киберзащиты и является одним из наиболее перспективных направлений совершенствования инструментов защиты, которые уже не разделялись бы на ИТ, функциональную или промышленную безопасность. ■