# Аспекты защиты АСУ ТП в 2024 году
## Круглый стол экспертов

Кибербезопасность АСУ ТП остается критически важной и сложно решаемой задачей, с существенными отличиями от защиты корпоративного сегмента. Эксперты в области безопасности промышленных систем поделились своим мнением по нескольким вопросам, подготовленным редакцией журнала "Информационная безопасность".

**Дмитрий Даренский,** *руководитель практики промышленной кибербезопасности Positive Technologies*
**Антон Елизаров,** *руководитель отдела защиты АСУ ТП и КИИ "Инфосистемы Джет"*
**Илья Карпов,** *ведущий специалист по кибербезопасности BI.ZONE*
**Алексей Комаров,** *региональный представитель УЦСБ в Москве*
**Дмитрий Кузин,** *начальник управления ИБ АСУ ТП "Облачные сети"*
**Дмитрий Михеев,** *технический директор компании "АйТи Бастион"*
**Михаил Молчанов,** *руководитель группы систем защиты АСУ ТП компании "Газинформсервис"*
**Андрей Никонов,** *главный аналитик компании "Фродекс"*
**Алексей Петухов,** *руководитель отдела развития бизнеса InfoWatch ARMA, лидер центра компетенций "Кибербезопасность" НТИ Энерджинет*
**Валерий Степанов,** *руководитель направления Центра компетенций по информационной безопасности T1 Интеграция*
**Артем Туренок,** *руководитель отдела технических решений АО "ДиалогНаука"*

### Какие проблемы остро стоят в аспекте защиты АСУ ТП в 2024 г.?

**Илья Карпов, BI.ZONE:**
Одной из главных проблем остается импортозамещение. Сложности затрагивают как системы управления, так и средства защиты информации, поскольку обеспечить продление лицензий и технической поддержки часто бывает сложно или невозможно. Это приводит к использованию уязвимого оборудования и ПО, а также препятствует решению возникающих технических проблем. Еще одной сложностью является недостаточная проверка импортозамещающих решений на наличие уязвимостей. Недооценка рисков может привести к слабому инвестированию в проекты по обеспечению безопасности АСУ ТП.

**Алексей Петухов, InfoWatch:**
1. Импортозамещение. Сюда входит (требуемое) изменение АСУ ТП с зарубежных на российские, а также необходимость замены ряда средств защиты. Все это требует значительного перепроектирования и соответствующих последующих затрат.
2. Ограниченность средств защиты информации. Для большинства зарубежных АСУ ТП использовались зарубежные, проверенные ими, средства защиты информации. Теперь требуется проводить проверки самостоятельно.
3. Ограничение кадровых ресурсов и их компетенций.

**Алексей Комаров, УЦСБ:**
Вопросы с поддержкой установленного оборудования и программного обеспечения покинувших российский рынок производителей за прошедшие два года в целом удалось так или иначе решить. Сейчас в приоритете вопросы, связанные с реализацией систем защиты для АСУ ТП, модернизируемых в связи с необходимостью импортозамещения и реализации требований по переходу на доверенные программно-аппаратные комплексы (ПАК).

**Антон Елизаров, Инфосистемы Джет:**
Главной проблемой остается большое количество устаревших систем АСУ ТП, на которых сложно поддерживать необходимый уровень безопасности. Процесс модернизации двигается небыстро и требует большого количества оборудования и человеческих ресурсов. Остро стоит вопрос сегментирования технологических сетей и выделения буферных зон для взаимодействия технологического и корпоративного сегментов, чтобы выстроить защиту от атак извне.

**Дмитрий Даренский, Positive Technologies:**
Возрастающая сложность сетевой инфраструктуры и использование новых технологий, среди которых, например, частные облака, контейнеризация критичных приложений, анализ больших данных, Интернет вещей, открытые технологии обработки технологических данных, а также рост числа киберугроз и расширение технических возможностей у злоумышленников делают технологическую сеть любого предприятия более уязвимой к кибератакам. Проблемы заключаются в недостаточной защите от распространенных угроз, слабой аутентификации и авторизации, трудностях с обновлением систем. Остро стоит вопрос с надежностью и защищенностью новых технологий и систем, построенных с их использованием. Сегодня мы наблюдаем недостаточную готовность предприятий к поддержанию непрерывности работы своих критичных систем и оперативному восстановлению после киберинцидентов.

**Дмитрий Михеев, АйТи Бастион:**
В 2024 г. проблемы защиты АСУ ТП остаются крайне актуальными и сложными. Среди ключевых проблем можно выделить следующие:
- увеличение числа кибератак, в том числе целенаправленных;
- уязвимости в ПО и оборудовании, проблемы поддержки имеющихся решений;
- интеграция АСУ ТП с корпоративными ИТ-сетями, вопросы ответственности и подчиненности в части контроля рисков;
- все еще встречаются ситуации, когда не реализованы даже самые базовые контроли безопасности и сегментация сетей;
- низкая осведомленность и недостаток квалификации сотрудников по вопросам ИБ;
- угрозы со стороны собственных сотрудников и привлекаемых исполнителей;

● нереализованные процессы мониторинга и реагирования на инциденты.

Безопасность – это постоянная работа, и эта тема требует и будет требовать серьезного внимания и ресурсов.

### Артем Туренок, ДиалогНаука:

В настоящее время в рамках проектов по защите АСУ ТП мы сталкиваемся у некоторых заказчиков с использованием устаревших (неподдерживаемых) версий ОС (например, Windows XP, поддержка которых закончилась еще в 2019 г.), старого оборудования (на которое зачастую затруднительно установить наложенное средство защиты) и наличием устаревшего сетевого оборудования, не поддерживающего технологии SPAN/RSPAN.

### Дмитрий Кузин, Облачные сети:

Наиболее остро стоит вопрос импортозамещения самих компонентов АСУ ТП. В промышленности львиная доля систем работает на ушедших с рынка Emerson, Yokogawa, Siemens, Schneider и пр. Их уход критичен не только с точки зрения отсутствия комплектующих, но прежде всего из-за отсутствия обновлений прикладного ПО, закрывающих найденные уязвимости.

### Валерий Степанов, Т1 Интеграция:

Первоочередные задачи в защите АСУ ТП в 2024 г. включают таргетированные атаки, распространение вредоносного ПО (в частности, шифровальщиков), утечки данных и атаки на системы управления технологическим процессом.

### Михаил Молчанов, Газинформсервис:

В связи с активным импортозамещением систем АСУ ТП одной из ключевых проблем в аспекте защиты является совместимость средств защиты информации с новыми отечественными SCADA-системами и ПЛК. СрЗИ должны взаимодействовать с АСУ ТП, но при этом не должны оказывать влияния на технологический процесс при выполнении функций безопасности. Производителям компонентов АСУ ТП необходимо плотно сотрудничать с производителями СрЗИ по вопросам интеграции оборудования и ПО.

## Каких классов российских решений особенно не хватает для защиты промышленного сегмента сети?

### Артем Туренок, ДиалогНаука:

Мы считаем, что на текущий момент на рынке присутствует недостаточное количество решений класса Deception,

Изображение: ГРОТЕК

обеспечивающих эмуляцию АРМ, серверов АСУ ТП и поддерживающих достаточно широкий перечень ПЛК.

### Дмитрий Даренский, Positive Technologies:

Мы наблюдаем нехватку решений, которые обеспечивают киберустойчивость технологических сетей с возможностью комплексной защиты от современных киберугроз. Это в первую очередь продвинутые системы мониторинга и обнаружения инцидентов, средства анализа угроз и реагирования. Кроме этого – интегрированные решения для защиты от внутренних и внешних угроз, являющиеся полнофункциональными элементами систем промышленной автоматизации предприятий.

### Михаил Молчанов, Газинформсервис:

Самая острая потребность сегодня наблюдается в таких решениях, как виртуальные частные сети (VPN) для промышленных сегментов (территориально распределенных АСУ ТП), где для передачи технологической информации (в том числе управляющих сигналов) применяются каналы связи сторонних поставщиков услуг и, как следствие, требуется защита этих каналов связи. Сложность таких решений обусловлена не только требованиями к наличию сертификата ФСБ России, но и необходимыми характеристиками (низкое энергопотребление, высокая отказоустойчивость, быстродействие).

### Дмитрий Кузин, Облачные сети:

Если рассматривать классические АСУ ТП, коих на сегодняшний момент абсолютное большинство, то набор решений по защите информации примерно одинаковый и во всех классах существуют отечественные продукты. Но в некоторых сегментах наблюдается отсутствие конкуренции, решения представлены одним, максимум двумя вендорами. Особенно остро это чувствуется в системах резервного копирования и хостовых средствах антивирусной защиты.

### Алексей Комаров, УЦСБ:

Наиболее острая потребность ощущается в сетевых решениях, которые хотя и присутствуют в портфелях уже многих отечественных производителей (и число их только растет), но пока не в достаточной степени апробированы на реальных объектах, часто не имеют широкой поддержки специфичных промышленных протоколов, да и в целом пока – давайте это признаем – по набору своих возможностей и стабильности явно имеют потенциал для дальнейшего роста и развития.

### Илья Карпов, BI.ZONE:

Сегодня промышленный сегмент сети остро нуждается в следующих классах российских решений по обеспечению безопасности:

1. Интегрированные средства защиты на основе программного обеспечения и оборудования для АСУ ТП.
2. Системы менеджмента активов для АСУ ТП, обеспечивающие контроль управления оборудованием.
3. Сетевые сканеры безопасности с поддержкой множественных промышленных систем.
4. Централизованные системы диагностики АСУ ТП.

### Антон Елизаров, Инфосистемы Джет:

Импортозамещение сильно подстегнуло развитие отечественного рынка средств защиты информации. Сейчас на нем представлены разные решения, начиная от защиты конечных устройств и заканчивая системами мониторинга событий информационной безопасности и управления инцидентами. Однако на

рынке практически не существует конкуренции: в некоторых сегментах представлено всего 1–2 продукта с богатым функционалом. Но многие вендоры начинают активно выпускать новые достойные решения, поэтому со временем ситуация нормализуется.

### Дмитрий Михеев, АйТи Бастион:

На данный момент в России существует широкий спектр решений в области ИБ для промышленного сегмента, включая системы уровня Enterprise, например SIEM, NGFW, EDR. Однако стоит отметить нехватку локализованных аппаратных платформ, что может затруднять полноценную защиту промышленных сетей. Необходимые решения на рынке существуют, могут быть приобретены и приносить пользу. Но их внедрение требует готовности инфраструктуры и процессов внутри предприятий, а также значительных бюджетов на закупку и техподдержку. Важно отметить, что в условиях санкционных ограничений растет спрос на российские решения и многие из них уже доступны на рынке благодаря достойным отечественным ИБ-разработчикам.

### Алексей Петухов, InfoWatch:

Для защиты промышленного сегмента чаще всего используется принцип блокирования всего, чего нет в списке разрешенных устройств и ПО – как в сети, так и на рабочих станциях и серверах соответственно. Второй принцип – выявление отклонений от эталона. На российском рынке достаточно средств защиты информации для этого. Большая проблема заключается в том, что не все можно сертифицировать, так как, например, Windows недоступен для России, а соответственно, и сертифицировать, поддерживать ПО под него достаточно проблематично.

## Каковы плюсы и минусы передачи сопровождения ИБ АСУ ТП внешнему подрядчику, в частности внешнему SOC?

### Алексей Комаров, УЦСБ:

Не так важно, внутренний SOC или внешний, как важно наличие эффективных механизмов оперативного выявления инцидентов и реагирования на них. С учетом особенностей АСУ ТП как объекта защиты принимать решение о том, самостоятельно ли создавать SOC либо воспользоваться аутсорсингом, нужно исходя из практической ситуации с кадровым обеспечением и возможностями по капитальным вложениям в создание соответствующих технической и организационной структур.

## Комментарий эксперта

**Руслан Амиров,** *руководитель экспертных сервисов мониторинга и реагирования Jet CSIRT "Инфосистемы Джет"*

Ряд работ по сопровождению ИБ АСУ ТП можно проводить только в ограниченный период времени – как правило, в рамках технологического окна. Привлекая внешнего подрядчика, специалисты заказчика успевают выполнить все работы в сжатые сроки, пока партнер проводит исследования, производит настройки безопасности и другие действия для устранения выявленных уязвимостей. Подрядчик также формирует план повышения уровня защищенности АСУ ТП, который можно реализовать при следующем плановом простое.

К плюсам такого сотрудничества можно отнести экономию времени, сохранение плановых сроков простоя, получение дополнительной внешней экспертизы и глубокого понимания состояния ИБ АСУ ТП, оценку состояния ИБ для модернизации и долгосрочного планирования изменений в АСУ ТП.

В качестве минусов отмечу необходимость предоставления очного доступа для сотрудников подрядчика к целевым системам, передачу доступов и реквизитов (которые могут быть утеряны), подтверждение изменений конфигураций, а также потребность в тестировании АСУ ТП после внесенных изменений.

Мониторинг ИБ АСУ ТП силами внешнего SOC в большинстве случаев (кроме АСУ ТП, изолированных от любых сетевых сегментов) производится непрерывно и позволяет отследить любые изменения как в штатном режиме функционирования, так и в ходе простоя, когда АСУ ТП подвержены повышенному риску. Это помогает выявить инциденты ИБ на раннем этапе или найти предпосылки к их возникновению. Например, во время технологического окна компоненты АСУ ТП могут получить доступ в Интернет, внешний носитель с легитимным обновлением для специального ПО АСУ ТП может быть заражен вредоносным ПО, а к АСУ ТП могут появиться временные доступы, которые из-за спешки могут стать постоянными.

Среди ключевых плюсов такого подхода можно отметить возможность контроля и повышение видимости процессов ИБ в АСУ ТП в любом режиме функционирования системы, значительное ускорение реакции на возникающие инциденты и снижение возможного ущерба, сокращение незапланированного простоя, а также адекватные параметры SLA. Что касается недостатков, я бы отметил потребность в организации безопасных каналов для передачи телеметрии и прочих данных внешнему SOC, настройку встроенных, накладных и дополнительных средств обеспечения ИБ, а также внесение изменений во внутренние нормативные документы в целях повышения оперативности реагирования на инциденты.

### Михаил Молчанов, Газинформсервис:

Плюсом является экономия заказчика на содержании внутреннего штата дорогостоящих сотрудников. Из минусов стоит отметить, что внешний подрядчик не имеет доступа к компонентам АСУ ТП, а значит, не может сопровождать ИБ в части встроенных средств защиты информации прикладного ПО и оборудования АСУ ТП. А значит, для обеспечения комплексного подхода к обеспечению ИБ необходимо привлекать штатный персонал, эксплуатирующий АСУ ТП.

### Артем Туренок, ДиалогНаука:

Из минусов следует отметить:

1. SOC не обладает возможностью оперативного отслеживания изменения в инфраструктуре АСУ ТП в организационной части.
2. Отсутствует возможность оказания услуг по оперативному реагированию на инциденты и сбору и обработке событий с контролируемых узлов в случае пропадания канала связи.
3. Увеличена поверхность атаки на объект КИИ за счет появления внешнего SOC.

### Дмитрий Кузин, Облачные сети:

Кадровый голод в нашей сфере – это проблема последних нескольких лет. Но если для администрирования СЗИ должны быть специалисты в каждой службе заказчика, то в случае с внешним подрядчиком один инженер может заниматься администрированием сразу на нескольких объектах. При этом этот инженер будет иметь все необходимые сертификаты и на постоянной основе проходить продуктовые обучения и курсы повышения квалификации. Минусы – необходимость предоставлять удаленный доступ к инфраструктуре и, соответственно, искусственно добавлять дополнительные векторы атаки. Для минимизации рисков в процессе создания систем защиты, до момента передачи на аутсорсинг, потребуется внедрять дополнительные классы СЗИ.

### Дмитрий Михеев, АйТи Бастион:

Решение о передаче сопровождения АСУ ТП внешнему подрядчику (внешнему SOC) должно быть тщательно взвешено. Необходимо оценить риски, провести глубокий аудит потенциальных подрядчиков, подробно проговорить условия обслуживания и зоны ответ-

ственности, однако важно учитывать все плюсы и минусы данной инициативы.

К безусловным плюсам можно отнести экспертизу и четкую специализацию, снижение затрат, непрерывный мониторинг и анализ событий безопасности, быстрое реагирование на инциденты.

К минусам можно отнести конфиденциальность данных (всегда есть риск утечек данных), зависимость от третьей стороны (так или иначе, это приглашенный подрядчик), ограниченное понимание ситуации со стороны бизнеса, возможные проблемы в коммуникации.

### Илья Карпов, BI.ZONE:

Плюсы: наличие у внешнего SOC компетенций в области АСУ ТП, круглосуточный мониторинг, сокращение затрат на обучение персонала, обеспечение взаимодействия с государственными регуляторами в области кибербезопасности, предоставление периодической аналитики и отчетов.

Минусы: возможное отсутствие понимания у подрядчика специфики вендоров АСУ ТП, вопросы доверия к стороннему подрядчику, ограниченная осведомленность о бизнес-процессах компании.

Преимущества и недостатки передачи сопровождения кибербезопасности АСУ ТП внешним подрядчикам схожи с работой SOC-подразделения в классических ИТ-структурах. Внедрение гибридного формата может устранить некоторые минусы, но все зависит от конкретных обстоятельств.

### Дмитрий Даренский, Positive Technologies:

К плюсам передачи сопровождения внешнему подрядчику, например MSS- или MDR-провайдеру с внешним SOC, можно отнести доступ к экспертам высокого уровня, которых многие предприятия не могут себе позволить держать в штате, а также расширенные ресурсы и возможность получения экономически более выгодных сервисов непрерывного мониторинга, администрирования средств защиты, анализа защищенности и реагирования на инциденты. Однако есть и минусы: потенциальные риски конфиденциальности и управления данными, зависимость от стороннего поставщика и возможное снижение качества предоставляемых услуг.

### Валерий Степанов, Т1 Интеграция:

Плюсы передачи сопровождения ИБ АСУ ТП внешнему подрядчику, включая внешний SOC, включают более высокую компетентность и экспертизу в области кибербезопасности, возможность оперативного реагирования на инциденты и повышение общего уровня защиты. Минусом является наличие отраслевой специфики промышленных организаций, поэтому командам SOC требуется немного больше времени на адаптацию процессов мониторинга и реагирования.

## Как импортозамещение систем АСУ ТП влияет на уровень информационной безопасности?

### Артем Туренок, ДиалогНаука:

В случае перехода на импортозамещенные системы АСУ ТП, которые несильно распространены на рынке ИБ, наблюдаются проблемы интеграций и совместимости в работе с СрЗИ.

### Илья Карпов, BI.ZONE:

Отечественные производители обычно работают под надзором регулирующих органов, таких как ФСТЭК России. Это позволяет им быстрее реагировать на обнаруженные уязвимости, а также ускорять процессы их устранения и публиковать информацию. Некоторые российские решения пока уступают зарубежным аналогам по части функциональности в области кибербезопасности, однако производители активно работают над добавлением и расширением опций. Некоторые производители выдают решения из стран Азии за отечественные, предлагая легкие способы импортозамещения. Это может привести к тому, что компания приобретает не то, за что платит. Это чревато трудностями с поддержкой и обновлением данных систем. Для того чтобы не быть обманутыми, мы рекомендуем компаниям проводить комплексный анализ защищенности перед внедрением новых решений.

### Алексей Комаров, УЦСБ:

При наличии достаточного бюджета проводимая модернизация является хорошей возможностью внедрить средства защиты для тех систем, которые ранее оставались ими неохваченными. Дополнительно при перепроектировании систем появляется возможность предусмотреть и реализовать меры защиты на достаточно раннем этапе, что при грамотном подходе также дает положительный эффект, так как не надо изобретать варианты повышения безопасности давно работающей эксплуатируемой АСУ ТП, с постоянной оглядкой на необходимость внесения минимума изменений в ее компоненты.

### Дмитрий Кузин, Облачные сети:

Уход зарубежных вендоров сказался отрицательно с точки зрения патч-менеджмента. Но есть один, на мой взгляд самый существенный положительный момент в истории с импортозамещением (которое началось задолго до 2022 г.) – качественный рост продуктов как в сфере АСУ ТП, так и в специализированных СЗИ для промышленного сегмента.

### Дмитрий Михеев, АйТи Бастион:

Импортозамещение АСУ ТП может оказывать серьезное влияние на уровень ИБ, как позитивное, так и негативное. С одной стороны, оно способствует увеличению контроля и независимости, повышая общую устойчивость к внешним угрозам. С другой стороны, выбор решений сократился, а имеющиеся стали дороже и дешеветь в обозримом будущем не собираются. Учитывая сложившуюся ситуацию и традиционное внимание регулирующих органов к безопасности, потребуются значительные затраты на ИБ как с технической, так и с формальной стороны.

### Алексей Петухов, InfoWatch:

С одной стороны, российские производители достаточно гибки и готовы внедрять и согласовывать средства защиты на свои системы. Поэтому возможности создания защищенных систем гораздо выше. С другой стороны, процессы выявления и управления уязвимостями, безопасной разработки чаще менее развиты в российских АСУ ТП. Отсутствуют проработанные решения от поставщика, и глубокая настройка может проходить очень тяжело. Вопрос по-прежнему остается в том, кто и как ведет конкретный проект.

### Дмитрий Даренский, Positive Technologies:

Импортозамещение систем АСУ ТП может оказать как положительное, так и отрицательное влияние на уровень информационной безопасности. С одной стороны, развитие отечественных решений повышает независимость от иностранных поставщиков и снижает вероятность воздействия внешних угроз. С другой стороны, недостаточное качество отечественных решений, их технологическое отставание от мировых стандартов может увеличить риски безопасности.

### Антон Елизаров, Инфосистемы Джет:

С точки зрения информационной безопасности есть свои плюсы. Как минимум – переход на отечественные ОС со встроенным функционалом безопасности минимизирует количество наложенных средств защиты. При этом применение подходов к безопасной разработке ПО АСУ ТП позволяет задействовать механизмы безопасности. За счет этого создается базовая защищенная среда исполнения, на которую уже можно добавлять дополнительные компоненты безопасности исходя из актуальных угроз.

### Валерий Степанов, Т1 Интеграция:

В рамках импортозамещения систем АСУ ТП стоит обратить внимание на следующие аспекты.

1. Версии и виды операционных систем, а также скорости их обновления для развития продукта. В российских изделиях часто используют старые или

самописные версии ОС, основанные на ядрах прошлого поколения, что, в свою очередь, дает возможность злоумышленнику реализовывать эксплойты ядра ОС.

2. Наличие или отсутствие процедур статического и динамического анализа кода при проектировании АСУ ТП, так как изделия для коммерческого рынка могут содержать уязвимости и ошибки кода, приводящие к выходу систем из строя.

### Михаил Молчанов, Газинформсервис:

Несмотря на возникающие проблемы, переход АСУ ТП на отечественных производителей не только обеспечивает технологическую независимость, но и дает возможность развиваться рынку ИБ, совершенствовать существующие решения по ИБ, разрабатывать новые. Общая заинтересованность и общие цели у российских производителей способствуют улучшению качества ИБ в технологическом сегменте.

## Каковы особенности процесса управления уязвимостями и патч-менеджмента в промышленном сегменте?

### Дмитрий Кузин, Облачные сети:

Критичность потери доступности системы является самой существенной особенностью. АСУ ТП зачастую – это системы управления в режиме онлайн, потеря контроля даже на минуту может привести к печальным последствиям. Поэтому все обновления и патчи перед установкой на рабочую систему необходимо тестировать в изолированной среде.

### Артем Туренок, ДиалогНаука:

При проведении работ по защите систем АСУ ТП мы наблюдали следующие особенности на стороне заказчиков:

- отсутствие обновлений ОС и СПО, СПО не поддерживают обновленные версии ОС;
- специалисты ИБ пытаются максимально закрыть сетевое взаимодействие до защищаемых узлов;
- производится периодический контроль перечня установленного ПО на АРМ/серверы АСУ ТП.

### Дмитрий Даренский, Positive Technologies:

Необходима более тщательная предварительная проверка обновлений. Промышленные системы часто требуют длительных циклов тестирования и внедрения обновлений, из-за их критичности и потенциального влияния на производственные процессы. Причем тестирование должно выполняться на отдельных изолированных стендах, дублирующих функциональность и инфраструктуру эксплуатируемых систем. Это может быть технически сложно и финансово затратно. Есть также определенная сложность в управлении уязвимостями на устройствах, работающих в реальном времени или в условиях ограниченной сетевой связанности.

### Андрей Никонов, Фродекс:

Аудит промышленной инфраструктуры (в частности, АСУ ТП) должен проводиться с минимально возможным влиянием на работу оборудования: снижение работоспособности или полный отказ просто недопустим. Взаимодействовать с промышленной инфраструктурой нужно так, чтобы как можно меньше нагружать ее сеть и активы. Основные условия для патч-менеджмента: планирование процедур обновления и предварительная проверка файлов обновлений как по части ИБ, так и по сохранению работоспособности целевого ПО.

### Антон Елизаров, Инфосистемы Джет:

Основной особенностью является тестирование всех вносимых изменений до их внедрения в промышленном сегменте. Можно использовать облегченные режимы сканирования промышленного сегмента для минимизации влияния на работу технологического процесса.

### Илья Карпов, BI.ZONE:

Можно выделить следующие особенности процесса управления уязвимостями и патч-менеджмента в промышленном сегменте: учет критичности и непрерывности производственных процессов, наличие плана и назначенных ответственных лиц, регулярная инвентаризация активов, использование проверенных источников обновлений, проверка обновлений на наличие вредоносного содержимого, установка обновлений на стенде с последующим тестированием, включая изменение времени работы, своевременное определение интервалов для внесения обновлений.

### Алексей Комаров, УЦСБ:

Зачастую в силу приоритета непрерывности технологических процессов оперативная установка обновлений невозможна, поэтому любые изменения в технологических сегментах должны быть тщательно предварительно протестированы, а реализованы они могут быть в подавляющем большинстве случаев исключительно в рамках сервисных обслуживаний (технологических остановов). Поэтому нужно четко понимать, какие именно уязвимости наиболее критически значимы и должны быть устранены в первую очередь. Общий подход к выполнению нужных изменений должен обязательно учитывать, что любые потенциальные технические сбои и проблемы вынудят откатиться к изначальным настройкам, рискуя свести на нет все приложенные до этого усилия по повышению уровня защищенности АСУ ТП.

### Дмитрий Михеев, АйТи Бастион:

Промышленные системы часто работают круглосуточно и не могут быть легко остановлены для проведения обновлений или устранения уязвимостей. Поэтому патч-менеджмент должен быть тщательно спланирован и проверен на тестовой среде. Важно предусмотреть возможность отката изменений в случае возникновения проблем. Не редкость, что на практике в АСУ ТП используются не самые новые системы и оборудование, для которых обновления безопасности могут не выпускаться. В таких случаях нужно использовать дополнительные меры защиты: сегментацию сети, межсетевые экраны, системы обнаружения вторжений (IDS) и др. Сложные масштабные автоматизированные системы часто распределены по зонам ответственности разных юрлиц и обслуживаются различными подрядчиками, поэтому вопросы встречного контроля и определения зон ответственности являются одними из самых популярных проблем.

### Валерий Степанов, Т1 Интеграция:

В рамках управления уязвимостями в промышленном сегменте стоит в первую очередь определить бизнес-процессы на предприятии, прибыль и ущерб в случае их остановки. Таким образом, специалисты будут понимать критичность процессов на предприятии и смогут подобрать гибкую систему их поддержания. Главной задачей для специалистов должно быть управление основными процессами производства и, как следствие, отслеживание новых уязвимостей АСУ ТП, задействованных в этих процессах, и осуществление незамедлительного их устранения как организационными мерами, так и посредством патч-менеджмента. Процесс патч-менеджмента менее значимых процессов для производства стоит вести на ежемесячной или ежеквартальной основе.

### Алексей Петухов, InfoWatch:

АСУ ТП располагается в закрытом сегменте, это создает свою специфику: необходимо через флешки получать обновления с определенной периодичностью. Периодичность патчей зависит от возможностей технологического обслуживания, которые могут быть крайне редко. Есть физические противоаварийные системы, которые нивелируют большинство уязвимостей. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru