Безопасность делового информации

№ 09
I квартал
2015

ФСТЭК России на страже АСУ ТП

Виталий Лютиков

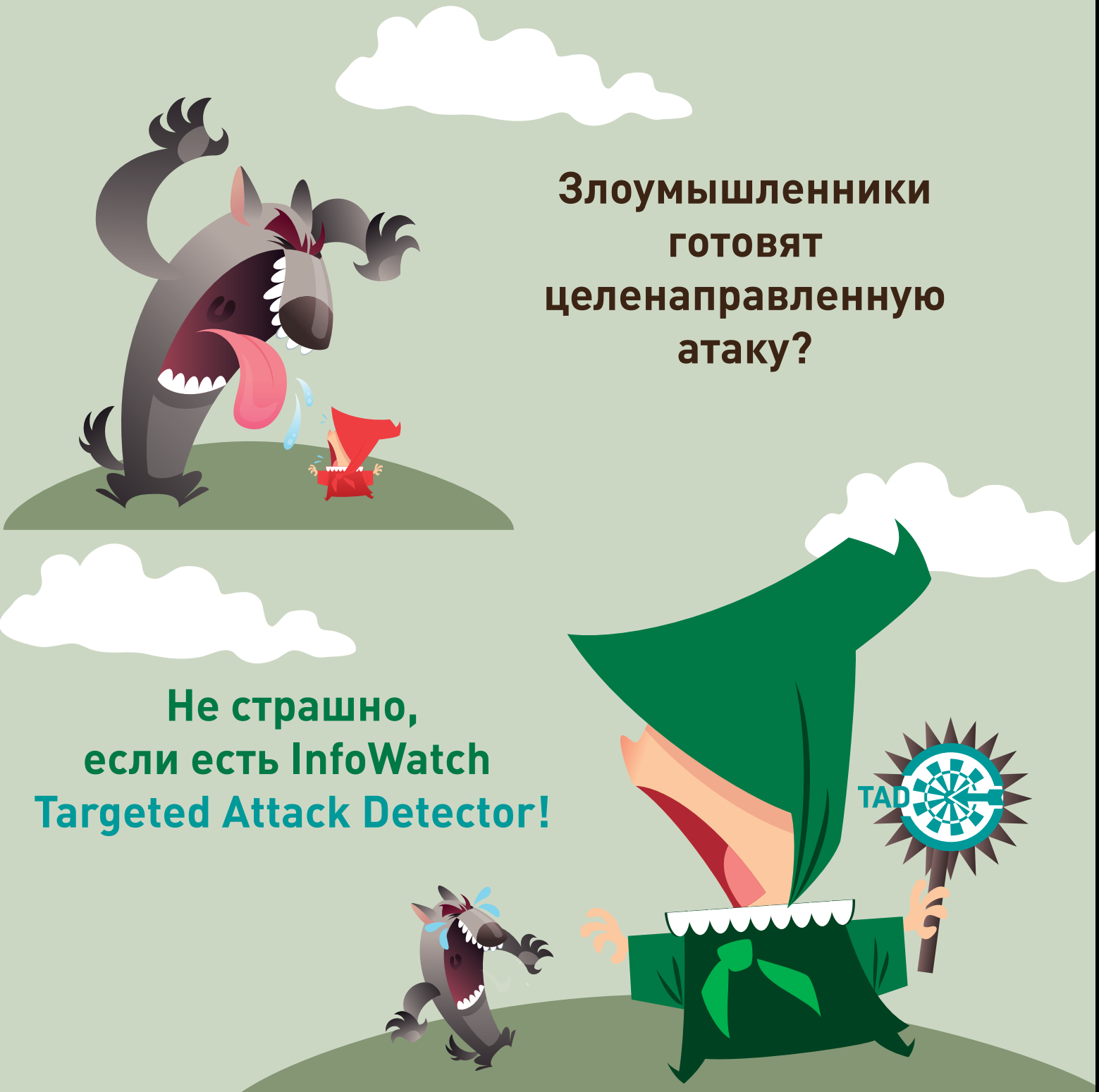
Кризис авторитета ИБ

Наталья Касперская

Битва пяти воинств

Дмитрий Даренский

ИБ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ



InfoWatch Targeted Attack Detector для защиты от целенаправленных атак

Мы все зависим друг от друга, или Синдром Вольдемара

ОЛЕГ СЕДОВ

Главный редактор журнала «!Безопасность Деловой Информации»

Россия — страна крайностей: на войну — с песнями, под венец — в слезах. Но в новое время и крайности проявляются по-новому.

Кажется, почти у каждого есть знакомый с гламурным именем Вольдемар или что-то типа этого. Гардероб такого Вольдемара состоит из множества вещей высочайшего качества и прекрасного фасона, демонстрирующих его изысканный вкус, поскольку все они — от Dolce&Gabbana, Gucci, Prada и Calvin Klein. И он ценит только то, что престижно и оснащено правильными логотипами. Если вы покажете ему в качестве примера инженерной мысли автомобиль, при сборке которого каждый ученик слесаря гордится, что ему доверили затянуть болты, то на лице Вольдемара появится такое выражение, будто ему прищемили палец капотом. Можно долго объяснять, что этот автомобиль — быстрый, как артиллерийский снаряд, умеет останавливаться мгновенно, словно ударившись о бетонную стену, что обода его колёс — гофрированные, дабы на поворотах не срывало в занос, а двигатель изготавливается в герметичном цеху, где все компоненты одинаково расширяются при нагреве... В ответ Вольдемар, зевнув, скажет: «Но ведь это — всего лишь Nissan».

Сейчас у вольдемаров в моде — ура-патриотизм. По той же формуле счастья они готовы отвергать все импортное только потому, что оно — не отечественное. Разумно ли это в мире, в котором все от всех зависят? Думаю, нет. Если, конечно, вы живете в мире, а не отгораживаетесь от него.

Его нынешнюю специфику можно пояснить на простом примере — тоже «автомобильном». Несколько лет назад на пресс-конференции команды «КАМАЗ-мастер» один из журналистов спросил с интонацией того самого Вольдемара: «А что у вас в КАМАЗе есть отечественного?». Парни из команды отреагировали спокойно и дали достойный развернутый ответ. Для них deadline — старт очередной гонки, которую никто не перенесет. Инженеры команды должны успеть разработать к ее началу новый узел, изготовить его прототип на опытном производстве и передать серийное изготовление узла какому-либо европейскому заводу (поскольку производственные мощности самого КАМАЗа обычно загружены). Для адаптации необходимы компетенции местных дизайн-бюро, знакомых с гоночной спецификой. По согласованию с командой «КАМАЗ-мастер» они дорабатывают изделие, передают европейскому заводу для изготовления, а готовые детали заказывают по всему миру. Теперь — вопрос «Вольдемару»: так чье это изделие, да и важно ли это знать, если в результате работы специалистов из разных стран гоночная команда подтверждает свое право взойти на пьедестал почета?

С ИТ и ИБ происходит нечто подобное. Складывается впечатление, что мы готовы отказаться от всех зарубежных продуктов, не понимая, какие риски и угрозы могут прийти с новыми отечественными решениями. На мой взгляд, более правильно — строить мультивендорные архитектуры, но для этого требуется высокий уровень компетенции всех участников проекта. Действительно, его реализация предполагает, во-первых, интеграцию с уже имеющимися ИТ/ИБ-архитектурами, во-вторых, интеграцию, разделение и взаимодействие конкурирующих платформ, а в-третьих (и это, пожалуй, — главное), управление обновленной архитектурой для обеспечения контроля над ее состоянием и обновлениями.

От того, что импортные жучки и закладки с НДВ (недекларированными возможностями) будут заменены аналогичными наборами «сюрпризов» отечественного производства, хорошо станет далеко не всем. Нужно уметь управлять ИБ-архитектурой и контролировать ее состояние. И без этих навыков, без проверенных практик и постоянно обновляемых компетенций импортозамещение превращается лишь в наивную мечту. А тем, кто еще верит в нее, позвольте напомнить, что симптом Эдварда Сноудена проявился в абсолютно «импортозамещенной» среде — ни одного российского аппаратного или программного решения в АНБ внедрено не было. Или я пропустил что-то важное в потоке пресс-релизов?

СОДЕРЖАНИЕ

ИБ и бизнес

ИБ-практика

Киберкриминалистика

Компетенции ИБ

ФСТЭК России на страже АСУ ТП

Задачи импортозамещения, рост количества уязвимостей и инцидентов, экономическая и политическая нестабильность — все это обуславливает необходимость новых подходов к обеспечению информационной безопасности. И выработка таких подходов особенно актуальна для области защиты информации автоматизированных систем управления технологическими процессами (АСУ ТП).

Сегодня обеспечение безопасности АСУ ТП является проблемой государственного масштаба, и Федеральная служба по техническому и экспортному контролю России активно развивает нормативно-правовые и методические документы по защите информации ограниченного доступа. Выступая в феврале на международном форуме «Технологии безопасности» с докладом «Актуальные вопросы защиты информации», начальник 2-го управления ФСТЭК России Виталий Лютиков представил отчет о работе этой службы, связанной с защитой АСУ ТП, и рассказал о планах ФСТЭК.

Методические документы ФСТЭК РФ по ИБ АСУ ТП

К 2016 г. служба готовит к выпуску проекты четырех методических документов по защите информации в АСУ ТП:

- Меры защиты информации в автоматизированных системах управления;
- Методика определения угроз безопасности информации в автоматизированных системах управления;
- Порядок выявления и устранения уязвимостей в автоматизированных системах управления;
- Порядок реагирования на инциденты, связанные с нарушением безопасности информации.

Кроме того, ФСТЭК разработала методические рекомендации по обеспечению защиты информации в АСУ ТП в соответствии с Приказом ФСТЭК России от 14 марта 2014 г. № 31. Цели документа — помочь в реализации требований к защите информации АСУ ТП, соответствующих процедур и уменьшить количество разночтений при изучении данного документа.

Со времени выхода Приказа №31 на многих предприятиях России наметилась положительная динамика в решении вопросов защиты информации АСУ ТП. Несмотря на продолжающиеся споры об обязательности выполнения требований этого приказа, многие предприятия газовой, нефтеперерабатывающей, атомной отраслей успешно их выполняют, осуществляют работы по совершенствованию политик безопасности и приведению отраслевых документов в соответствие со специальными требованиями и рекомендациями по технической защите информации.

Несмотря на продолжающиеся споры об обязательности выполнения требований приказа №31, многие предприятия газовой, нефтеперерабатывающей, атомной отраслей успешно их выполняют

Основной принцип классификации АСУ ТП КВО

При классификации АСУ ТП КВО, как правило, во главу угла ставятся

Комментарий

Илья Медведовский, генеральный директор Digital Security

Сегодня безопасности АСУ ТП необходимо уделять повышенное внимание. Уровень сложности и интеграции всех процессов на промышленных предприятиях очень высок, что порождает колоссальную уязвимость по отношению к внешним и внутренним воздействиям. И если вплотную не заняться решением этой задачи на государственном уровне, нам не избежать катастроф техногенного характера в самом ближайшем будущем.

В области ИБ АСУ ТП отмечается масса проблем, две из которых можно отметить особо.

Во-первых, существуют два параллельных враждующих мира — информационной безопасности и инженеров. Специалисты по ИБ сейчас воспринимаются как выскочки, которые пришли в мир инженеров, привыкших заниматься техническими решениями, со своими идеями об уязвимости системы, о возможности проникновения в нее. Инженеры недоумевают: 30 лет они занимались своим делом без какой-либо информационной безопасности, и все было прекрасно!

Во-вторых, массу проблем порождают руководители промышленных предприятий. Их главный принцип — «работает — не трогай!». На многих предприятиях имеется этакий ИТ-зоопарк 20-летней давности, в работу которого менеджмент предпочитает не вмешиваться, полностью полагаясь на механический контроль. У руководства предприятий мотивации к защите информации АСУ ТП нет: все работает, катастрофы не происходят, так зачем этим заниматься?

Именно поэтому так важна работа регуляторов в данной области. Без нормативных требований, которые они создают и пытаются внедрить в жизнь, у руководства промышленных предприятий не будет мотивации серьезно заниматься ИБ АСУ ТП. А значит, все мы рискуем оказаться в беде.

потенциальные экологический и технологический ущерб, техногенные аварии, катастрофы и тому подобные серьезные проблемы, связанные с работой таких систем. В общем, это правильно. И это — основной показатель, по которому оценивают возможные последствия нарушений требований безопасности. Однако многие упускают из виду те пункты Приказа № 31, в которых говорится об экономических и социальных последствиях нарушений безопасности информации и функционирования АСУ ТП.

Исходя из этого, необходимо, чтобы специалисты, участвующие в формировании отраслевых политик, хорошо понимали: простои в работе предприятия из-за сбоя автоматизированной системы управления могут стать причинами техногенных катастроф, принести колоссальные убытки и последствия социального характера в целых регионах. А потому при выборе мер обеспечения ИБ необходимо ориентироваться на защиту не только конфиденциальности информации, но и доступности критически важных систем и сервисов.

Особенности требований к ИБ АСУ ТП

При реализации требований к защите информации АСУ ТП следует помнить о некоторых их особенностях:

• эти требования не распространяются на информацию, составляющую государственную тайну;
• возможно применение средств защиты информации, прошедших оценку соответствия на основе законодательства РФ о техниче-

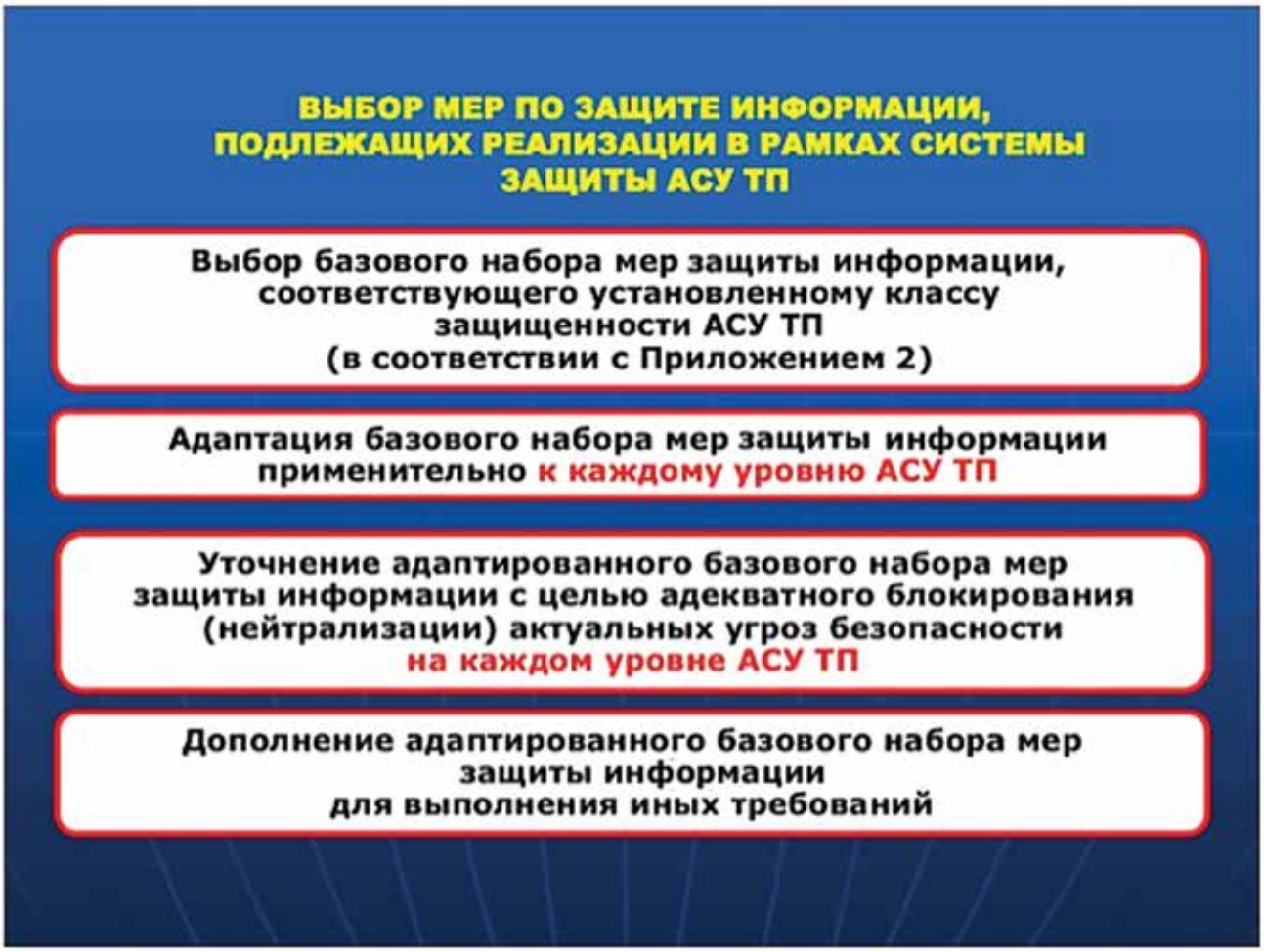
Простои в работе предприятия из-за сбоя автоматизированной системы управления могут стать причинами техногенных катастроф, принести колоссальные убытки и последствия социального характера в целых регионах.

ском регулировании (по любой из форм);
• необходима согласованность мер защиты информации и мер обеспечения технологической безопасности;
• оценка соответствия системы защиты АСУ ТП проводится в рамках приемочных испытаний АСУ или аттестации;
• возможен гибкий подход к выбору мер защиты информации АСУ ТП для каждого класса защищенности;
• есть возможность принятия компенсирующих мер.

ФСТЭК России проделала большую работу по совершенствованию своих подходов к защите информации и планирует и дальше развивать это направление. Пока выполнение требований методических документов ФСТЭК России по обеспечению ИБ АСУ ТП становится лишь проявлением сознательности и профессионализма руководителей промышленных предприятий, поскольку эти документы имеют рекомендательный характер (обязывающего закона еще нет). Однако, в связи с сегодняшней политической и экономической ситуацией, на государственном уровне уделяется особое внимание защите промышленных предприятий, и в самое ближайшее время будет разработана система штрафов за невыполнение рекомендаций по защите АСУ ТП.

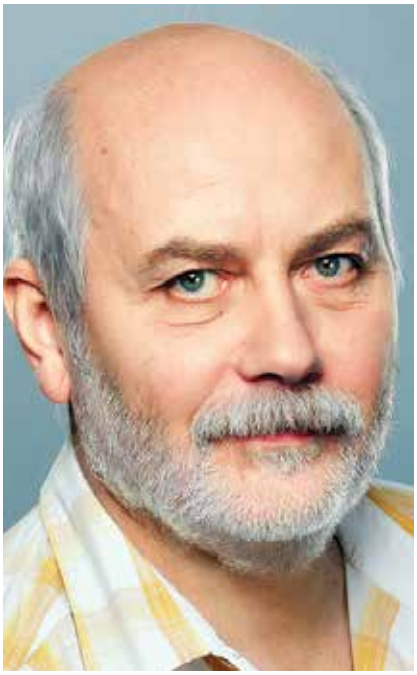
В связи с сегодняшней политической и экономической ситуацией на государственном уровне уделяется особое внимание защите промышленных предприятий, и в самое ближайшее время будет разработана система штрафов за невыполнение рекомендаций по защите АСУ ТП.

Подготовила Наталья Мутель, BISA



Не обязательно быть целью, чтобы стать жертвой

Вредоносные программы порой распространяются «в свободном полете» и не всегда попадают именно туда, куда их намеревались доставить злоумышленники. В этой ситуации промышленному предприятию, пренебрегающему мерами обеспечения ИБ, легко стать жертвой, не будучи целью атаки. О том, как на таких предприятиях относятся к ИБ, рассказывает Андрей Духвалов, руководитель Управления перспективных технологий «Лаборатории Касперского».



!БДИ: Тема информационной безопасности промышленных объектов, в частности АСУ ТП, актуальна давно, но сейчас интерес к ней превзошел все мыслимые пределы. Чем это можно объяснить?

Андрей Духвалов: Да, обеспечение безопасности АСУ ТП давно стало актуальной темой, но сейчас она вышла на новый виток популярности. И это не случайно.

Раньше производственники не придавали ИБ должного значения. Защита критически важных объектов (КВО) была сфокусирована на других аспектах (таких как физическая безопасность, видеонаблюдение, контроль над доступом и пр.), и на первый план выходили исключительно задачи надежности. Промышленное оборудование должно работать весьма надежно при выполнении своих основных задач, а безопасным оно должно быть ровно настолько, чтобы не пострадали люди, не возникла экологическая катастрофа и т. п.

Сейчас развитие технологий привело к тому, что реализация этих задач стала напрямую зависеть от ИТ, а следовательно, пришлось обратить внимание на обеспечение ИБ. Если промышленные системы управляются АСУ ТП, то появляется опасность воздействия на них с помощью информационных потоков, которое может привести к их выходу из-под контроля. И понимание таких угроз постепенно приходит к специалистам, отвечающим за безопасность промышленных и технологических процессов конкретных производств.

!БДИ: Вы считаете, что руководство промышленных предприятий понимает задачи ИБ?

А. Д.: Такое понимание, как и понимание информационных рисков для бизнеса и его эффективности, растет, и отдельные руководители начали уделять больше внимания данным вопросам. Но не могу сказать, что эта тенденция проявляется повсеместно. Дело в том, что обеспечение любой безопасности, в том числе информационной, снижает эффективность бизнеса. Организация защиты подразумевает серьезные затраты, которые не влияют на увеличение выпуска продукции. И руководители, у которых еще не сформировано представление об острой необходимости ИБ, воспринимают эти затраты как лишние.

!БДИ: Думаю, руководителей мотивирует к активным действиям информация о происшествиях у «соседей». Это заставляет их понять, что обсуждаемые угрозы являются вполне реальными, а не мифическими.

А. Д.: Серьезное, да к тому же недавнее происшествие у соседа — действительно, серьезный «мотиватор» для руководителей. Интерес к теме ИБ промышленных предприятий давно бы остыл, если бы не постоянные публикации сведений о реальных инцидентах — скажем, произошедших в Европе. Так, немецкое федеральное агентство по безопасности опубликовало официальной отчет с указанием того, какое предприятие и когда пострадало от воздействий хакеров, какой физический ущерб оно получило. Другими словами, факты ущерба,

понесенного индустриальными объектами при воздействиях на них через информационную среду, фиксируются и обнародуются. А в результате профессиональное сообщество начинает понимать важность этих задач, и его приоритеты меняются.

Правда, в России даже то, что происходит у «соседей», далеко не всегда воспринимается промышленными предприятиями как предупреждение о возможных угрозах для них самих. Вот, например, инцидент со Stuxnet: да, мы о нем знаем, но он произошел давно, далеко и не в нашей отрасли, а потому нам ничего не грозит. Но это — ложное чувство защищенности, ведь информационные технологии очень легко дуплицируются. Судя по коду Stuxnet, его писали высококвалифицированные специалисты, но после распространения отдельные компоненты кода оказались доступными для многих и стали использоваться, в том числе, не очень квалифицированными людьми. А такая ситуация порождает массовость угроз и бесконтрольное распространение вредоносных программ, порой попадающих совсем не к тем «адресатам», на которых ориентировался инициатор атаки. В результате появилось своеобразное определение: не обязательно быть целью атаки, чтобы стать ее жертвой.

!БДИ: А от кого должна исходить инициатива обеспечения ИБ промышленного предприятия?

А. Д.: Это — непростой вопрос. Решения по информационной безопасности в индустриальной среде должны приниматься на основе знаний и опыта из различных областей — информационная безопасность, автоматизированные системы управления технологическими процессами (АСУ ТП) и собственно технологический процесс на конкретном производстве. Специалисты должны обладать всей палитрой нужных компетенций — иначе нельзя обеспечить ИБ промышленного предприятия. Проблема состоит в том, что сейчас данный комплекс компетенций практически не встречается. Ну не готовят таких специалистов, и нет для них штатных единиц! Я уверен, что ситуация скоро должна измениться, тем более что сейчас явно видно движение государственных регуляторов в сторону обеспечения ИБ АСУТП.

!БДИ: В этой ситуации неопределенности с кем приходится вести диалог на промышленном предприятии?

А. Д.: Есть разные кандидаты — служба безопасности, служба ИБ (если ее нет, то специалисты, поддерживающие информационную инфраструктуру предприятия, в том числе офисную), технологи, а также специалисты по АСУ ТП. Энтузиасты, которые продвигают тему ИБ, встречаются в любой из упомянутых областей, и зачастую именно они становятся драйверами внедрения соответствующих мер на промышленных предприятиях. Ответственных за обеспечения информационной безопасности АСУ ТП на большинстве предприятий не существует — нет тех самых штатных единиц. В такой ситуации инициатива, безусловно, должна исходить от руководителей предприятий. Другой альтернативы быть не может!

!БДИ: Какую роль играют государственные органы, регулирующие эту деятельность?

А. Д.: Как минимум, благодаря действиям регуляторов и их указаниям предприятия начинают обращать внимание на информационную безопасность АСУ ТП — появляется ответственность за нее. Так, в 2012 г. Совет безопасности РФ опубликовал стратегию информационной защиты автоматизированных систем управления. В прошлом году ФСТЭК выпустил Приказ № 31, который регламентирует средства и методы защиты АСУ ТП. И хотя сейчас этот Приказ имеет лишь рекомендательный характер, я не исключаю того, что через какое-то время он станет обязательным для исполнения. По предварительной версии закона, который активно обсуждается, именно руководители предприятий будут нести уголовную ответственность за неадекватную защиту их АСУ ТП.

!БДИ: При всем уважении к регуляторам у меня остается вопрос: как в их инициативах учитывается отраслевая специфика промышленных предприятий?

А. Д.: При разработке необходимых мер защиты, действительно, нужно понимать специфику как технологического процесса, так и самого промышленного объекта. Но в Приказе ФСТЭК № 31 приведены лишь наиболее общие меры, дана своего рода методика. А для обеспечения практической оценки уровня информационной безопасности конкретных предприятий в нем вводится понятие «классы предприятий» и указывается, какие меры можно принимать в зависимости от важности объекта. На основе этих рекомендаций для каждого предприятия должен быть разработан свой собственный проект по ИБ АСУ ТП. Думаю, появление таких общих понятий и рекомендаций — это значимый шаг в правильном направлении. А кроме того, деятельность регуляторов продолжается, и стоит ожидать их новых инициатив в данной области.

В России даже то, что происходит у «соседей», далеко не всегда воспринимается промышленными предприятиями как предупреждение о возможных угрозах для них самих.

Кризис авторитета ИБ

В рамках VII Уральского форума «Информационная безопасность банков» состоялась встреча в формате «круглого стола», на которой рассматривались проблемы, влияющие на авторитет ИБ в условиях кризиса. Вела «круглый стол» генеральный директор компании InfoWatch Наталья Касперская. В дискуссии приняли участие заместитель начальника ГУБиЗИ Банка России Артем Сычев, начальник Управления ИБ Банка Москвы Василий Окулесский, глава Appercut Security и президент ассоциации BISA Рустем Хайретдинов, заместитель генерального директора компании «ЭЛВИС-ПЛЮС» Сергей Вихорев, управляющий партнер консалтингового агентства «Емельянников, Попова и партнеры» Михаил Емельянников. Коротко расскажем, какие тенденции и проблемы они обсуждали.

Веяния кризиса

Если вам кажется, что кризис не очень сильно сказался на магазинных ценах, то попробуйте внимательно рассмотреть упаковки товаров. Выяснится, например, что в слегка подорожавшей пачке пельменей стало меньше, то есть на деле их стоимость выросла гораздо больше. Последствия кризиса можно увидеть повсюду, и Наталья Касперская предложила обсудить, как он влияет на индустрию ИБ.

С точки зрения Банка России, чью позицию представлял Артем Сычев, заметно изменившаяся политическая обстановка обусловила дополнительные ограничения. Это огорчает, но есть и положительные моменты. У ряда банков появился выбор: что из возможного арсенала будет обеспечивать рост их бизнеса, а что — просто освоение бюджетов? Тем не менее в условиях сложного кредитования многим банкам не очень понятно, как зарабатывать. В результате, прогнозирует Михаил Емельянников, не исключено значительное уменьшение числа инфраструктурных проектов — банки уже их сворачивают. Зато растет интерес к локальным решениям, которые позволяют оптимизировать бизнес.

Сейчас практически весь бизнес представлен в онлайне. А это означает, что для оптимизации расходов понадобится перенести транзакционную нагрузку туда, где онлайн-сервисы будут обходиться дешевле, то есть в Интернет и облака.

Василий Окулесский уверен, что не почувствовать кризис нельзя. Вопрос — лишь в том, насколько сильно вы его ощущаете. Сильно! Серьезно выросла нагрузка на ИБ-подразделения и технические средства, а система финансирования изменилась в пользу того, что уже установлено и работает. Резко изменилось и отношение к продуктам, которые банк выпускает на рынок, а это, в свою очередь, обусловило еще большее увеличение нагрузки на специалистов по ИБ.

Казалось бы, кризис позитивно повлиял на авторитет ИБ-служб, ведь они оказались весьма востребованными, но не помешает взглянуть на ситуацию и под другим углом зрения. В «мирное» время телефоны работают в штатном режиме, и мало кто вспоминает о необходимости обеспечения ИБ. Когда возникают кризисные ситуации, телефонами начинают пользоваться чаще, и нагрузка на сети увеличивается. При этом денег больше не становится, а объем работы растет. До кризиса руководители среднего звена редко задумывались об ИБ, а сейчас то и дело упоминают персонал соответствующих служб в негативном плане, не принимая в расчет его физическую нагрузку.

Кроме того, работа служб информационной безопасности основана на прогнозах и реализации мер, позволяющих этим прогнозам не сбыться. Экономическая и политическая ситуация, в которой мы сейчас находимся, приводит к необходимости пересмотра моделей угроз и рисков, актуальных для той или иной организации. Например, еще вчера над большинством кредитных организаций не висела угроза отключения от каких-то финансовых инструментов, а сегодня эта угроза не только имеется, но и периодически воплощается в жизнь.

Михаил Емельянников придерживается очень жесткого взгляда на то, что нас ожидает. По его мнению, в тех компаниях, которые прежде не имели служб информационной безопасности (а это — примерно половина предприятий), в ближайшие годы они и не появятся. Там, где служба безопасности была и приносила реальные деньги, она останется. Ну а на тех предприятиях, где такая служба денег

не приносила, ее сократят, и весьма существенно. При этом на кадровом рынке происходят удивительные события: достаточно много людей ищут вакансии руководителя службы ИБ или начальника отдела банка, но нашелся лишь один претендент на должность, предполагающую «работу руками», написание нормативных документов и т. п. Все привыкли руководить, и от этой вредной привычки в период кризиса многим придется избавляться.

Приоритеты ИБ во время кризиса

Мы уже привыкли к тому, что самым модным словом представителей бизнеса становится «оптимизация». Но не всегда эту самую оптимизацию удается верно трактовать и применять. Так, во время кризиса 2008—2009 гг. руководители одной из страховых компаний решили сократить с целью оптимизации 10 % своих агентов. Сократили, и эти 10 % увели с собой 40 % клиентской базы, а в результате потери компании превысили все мыслимые плюсы от оптимизации. Как бы то ни было, сокращения персонала во время кризиса неизбежны, и уже первые слухи о готовящемся увольнении провоцируют сотрудников на противоправные действия. Каждый уносит с собой то, что позволит ему пережить трудные времена: менеджеры — клиентские базы, руководители среднего звена — описания бизнес-процессов, а топ-менеджеры — целые бизнесы. В этом нет ничего нового, однако Наталья Касперская предложила обсудить те риски для ИБ, которые будут характерны именно для текущей ситуации.

Сейчас практически весь бизнес представлен в онлайне. А это означает, что для оптимизации расходов понадобится перенести транзакционную нагрузку туда, где онлайн-сервисы будут обходиться дешевле, то есть в Интернет и облака. Рустем Хайретдинов пояснил это на примере банков, услугами которых он пользуется. Закрыв ближайшие к нему отделения, банки предложили ему получить ключ и настроить Интернет-банк. Но если многие клиенты начнут пользоваться Интернет-банком, это станет массовым сервисом, и нагрузка на него существенно вырастет. Соответственно, требования к его доступности и защищенности кардинально изменятся. И если раньше через мобильные приложения в банк обращались 5% клиентов, а теперь их доля увеличится до 30%, то «дыры» в таких приложениях будут оказывать на банк больше влияния. Соответственно, обеспечение безопасности относится к числу тех немногих направлений, которые во время кризиса должны расти, поскольку необходимо защищать именно дешевые каналы обслуживания.

По мнению Василия Окулесского, кризис не спровоцировал выход бизнеса в Интернет, а лишь его ускорил. Если раньше вывод банковских продуктов в Интернет числился в планах, и данную задачу решали постепенно, шаг за шагом, то сейчас ее реализация становится залогом выживания. А это влечет за собой ряд нюансов. В частности, сократилось время подготовки продуктов и их выхода на рынок, поэтому на него вываливаются «сырые» решения, не всегда удовлетворяющие требованиям ИБ. Значит, резко возрастет спрос на услуги компаний, предоставляющих качественный сервис тестирования мобильных приложений

с точки зрения безопасности. Скорее всего, это — одна из немногих дополнительных услуг, за которые бизнес согласится платить.

Зло социальных сетей

Один из набирающих силу рисков, чьи последствия хорошо видны, — это риск для деловой репутации и имиджа. За последнее время активность, нацеленная на дискредитацию отдельных банков и всей российской банковской системы, проявлялась неоднократно.

Так, можно упомянуть информационную атаку на «Сбербанк», которая была спровоцирована, очевидно, по политическому заказу, поскольку экономической основы не имела, да и в стабильности «Сбербанка» никто не сомневался. Ажиотаж был спровоцирован через механизмы социальных сетей. По словам Натальи Касперской, социальные сети — это новая сфера для банков, которые, как правило, консервативны и довольно трудно адаптируются к новому. Но с точки зрения ИБ было важно вовремя эту атаку выявить и правильно на нее отреагировать, причем не только «Сбербанку», но и Банку РФ. Службы ИБ порой трактуют такие задачи как непрофильные. Но если их решением не будет заниматься ИБ-служба, то вообще никто не станет уделять им внимания. А наша страна в целом очень уязвима перед подобными информационными атаками.

Василий Окулесский не скрывал негативного отношения к социальным сетям. По его мнению, с точки зрения информационной безопасности соцсети — большое зло. Сообщения в Интернете могут не только спровоцировать ухудшение деловой репутации той или иной компании, но и принести прямой финансовый ущерб. С такими проблемами приходилось сталкиваться достаточно часто, но до сих пор никто не знает правильных методов реагирования на них.

Например, в какой-либо группе создается негативное отношение к определенной организации, которое влияет на другие группы. Правда, это можно выявить, используя определенные технические решения, но на деле такая возможность имеет постактивный характер. Средства анализа контента социальных сетей позволяют узнать о готовящемся ударе лишь секунд за 30 до него. Другими словами, информация поступает тогда, когда мы уже не в состоянии ее использовать для предотвращения падения репутации. Кроме того, мы не умеем на такие сведения реагировать, и даже не представляем, как этого добиться в перспективе.

Нужно научиться извлекать пользу из получаемой информации. По мнению Натальи Касперской, при решении этих проблем не обойтись помощью вендоров. Предоставленный ими сервис анализа соцсетей может оказаться не очень эффективным без участия консультантов. Нам нужны их компетенции reputation management, и, возможно, в России вскоре появится такой сектор рынка.

Активность в соцсетях может быть вызвана и вполне конкретной задачей. Если деятельность по подрыву репутации сложно спрогнозировать и оценить извне, то парализованный ресурс или сервис всегда заметен. Как заверяет Рустем Хайретдинов, в нынешнем кризисном политизированном контексте добавилась не новая угроза, а новая характеристика угроз. Раньше эффективной считалась защита, которая позволяла добиться того, чтобы выгода злоумышленника от атаки оказалась меньшей, чем цена самой атаки. С появлением политизированных активистов в соцсетях эта эра закончилась. Люди ломают ресурсы любой ценой, даже не желая извлечь что-то «вещественное» из банковской системы. Их вполне устраивает иной результат: банковский сервис оказывается недоступным, и они сообщают об этом в соцсетях. Сообщение тут же тиражируется, и множество людей узнает, что банк не работает и всем клиентам необходимо срочно забрать из него деньги. Итак, угрозы остались теми же, но их весовые коэффициенты стали другими.

В Санкт-Петербурге кто-то однажды написал в соцсети, что первый зарегистрирует своего ребенка на госпортале, и тот будет учиться в нормальной школе, а остальные — «в школах с таджиками» (это цитата). В результате в 9.01 на питерском портале госуслуг насчитывалось уже 10 млн нажатий клавиш, и он на три дня оказался недоступным. Сочетание технических и социальных методик порождает новую угрозу? Сергей Вихорев считает историю с порталом госуслуг доказательством того, что модель угроз не меняется. Разве не была в ней предусмотрена DDOS-атака? Была, и это — известный риск. Только вот цена его изменилась, а потому предстоит масштабная переоценка угроз и рисков.

Раньше эффективной считалась защита, которая позволяла добиться того, чтобы выгода злоумышленника от атаки оказалась меньшей, чем цена самой атаки. С появлением политизированных активистов в соцсетях люди начали «ломать» ресурсы, даже не желая извлечь что-то «вещественное» из банковской системы.

Дефицит антикризисных компетенций

Порассуждав о влиянии кризиса на ИБ, соцмедиа — на бизнес и о новых угрозах, было бы странно обойти стороной тему актуальных компетенций. Наталья Касперская предложила обсудить новые роли и компетенции в сфере ИБ, без которых решение актуальных задач может оказаться крайне затруднительным.

По мнению Василия Окулесского, определение ролей в области информационной безопасности — дело интимное, да и вообще, сейчас очень сложно просить о выделении дополнительной роли. Например, доказать, что кто-то должен заниматься исключительно контролем соцсетей, практически невозможно, так как это нельзя обосновать экономически, но саму функцию все равно нужно кому-то выполнять. Другими словами, при возникновении новых ролей новые люди «под них» не появляются. Проблема формирования ролей в период кризиса существенно усложняется и потому, что обостряются проблемы, с которыми связаны эти роли. А значит, при наличии тех же ресурсов, а то и меньших, приходится выполнять гораздо большие объемы работы.

При этом новым ролям нужны новые компетенции. Специфика ИБ-службы такова, что в ней должен быть свой бизнес-аналитик, который понимает бизнес-процессы и, исходя из этого, рекомендует, что и как защищать. Должен быть и свой юрист, который может «построить мост» к нормативной документации, доказательной базе, а при необходимости обеспечит взаимодействие с правоохранительными органами и вынесение каких-то вопросов в суд. Плюс нужны аналитики, которые могут работать с информацией и той же доказательной базой. Безусловно, эти квалификации могут сочетаться в одном или нескольких сотрудниках. Тем не менее, обеспокоен Артем Сычев, проблема наличия нужных квалификаций — достаточно серьезная. Политика государства в области образования такова, что в ближайшее время мы можем получить «полярную» кадровую ситуацию: с одной стороны — техники, умеющие строить и поддерживать системы ИБ, а с другой — менеджеры. Выполнять «промежуточные» аналитические функции, которые максимально востребованы в области ИБ, просто будет некому.

Нельзя упускать из виду и качество подготовки специалистов. Михаил Емельянников отмечает две тяжелые болезни поколения Y. Во-первых, приходящие на предприятия после ВУЗов молодые люди нацелены не на работу, а на получение зарплаты. Все попытки набирать специалистов на проектную работу с соответствующим принципом оплаты заканчиваются тем, что после двух-трех проектов никто не хочет работать, предпочитая получать каждый месяц определенные деньги. Во-вторых, колоссальная проблема представителей поколения Y — неспособность воспринимать большие объемы текста, что не позволяет им читать и понимать документы, в которых насчитывается свыше 50—60 страниц. Кроме того, преподаватели утверждают, что серьезно упал общий образовательный уровень студентов. На это повлияли доступность информации в Интернете и то, что никто не проверяет источники ее формирования. Если и дальше будет продолжаться продвижение в данном направлении, то квалифицированных специалистов с базовым образованием, которые умеют учиться и ориентироваться в потоках информации, останется очень мало.

Политика государства в области образования такова, что в ближайшее время мы можем получить «полярную» кадровую ситуацию: с одной стороны — техники, а с другой — менеджеры. Выполнять «промежуточные» аналитические функции, которые максимально востребованы в области ИБ, просто будет некому.

Подготовил Олег Седов, BISA

СЕРГЕЙ ВИХОРЕВ

Заместитель по развитию генерального директора «ЭЛВИС-ПЛЮС»

Гибридное импортозамещение

Тема импортозамещения многогранна. При ее обсуждении необходимо не только понять, от каких зарубежных продуктов и решений можно отказаться и чем их заменить, но и уяснить, какими компетенциями мы обладаем для создания отечественных аналогов.

Сомнения в целесообразности импортозамещения высказывают многие, но это зачастую становится, скорее, эмоциональной реакцией. Хотелось бы, избегая крайностей, трезво проанализировать ситуацию и реальные возможности импортозамещения.

Многочисленные дискуссии, состоявшиеся в 2014 г. в профессиональных сообществах, свидетельствуют, что обеспечить 100-процентное импортозамещение в российской ИТ-сфере сегодня (впрочем, как и в ближайшей перспективе) невозможно. Согласно данным Минпромторга, доли импортных продуктов, применяемых в некоторых российских отраслях, таковы:

- станкостроение — более 90%;
- тяжелое машиностроение — 60—80%;
- легкая промышленность — 70—90%;
- электронная промышленность — 80—90%;
- фармацевтическая, медицинская промышленность — 70—80%;
- машиностроение для пищевой промышленности — 60—80%.

Что из этого следует? В интервью «Российской газете» от 05.08.2014 г. заместитель министра промышленности и торговли Сергей Цыба сказал: «В случае реализации продуманной политики импортозамещения к 2020 г. можно рассчитывать на снижение уровня импортозависимости по разным отраслям промышленности с 70—90% до 50—60%». Другими словами, в масштабах экономики в целом мы можем решить задачу не полностью, а лишь частично.

Давайте посмотрим, что в проблеме импортозамещения относится непосредственно к ИТ-отрасли. Первой задачей является импортозамещение аппаратной платформы, а второй — импортозамещение программной платформы и прикладного ПО. Только решив эти задачи именно в такой последовательности, мы сможем полностью перейти на отечественные продукты. Однако из-за отсутствия необходимых технологий замена аппаратной платформы растянется на десятки лет. Для замены программной платформы нужны специалисты, которые, к счастью, в России есть, но все равно для реализации данной задачи потребуется лет 5—7. Сегодня мы можем заменить лишь прикладное программное обеспечение — для этого есть все необходимое.

В случае реализации продуманной политики импортозамещения к 2020 г. можно рассчитывать на снижение уровня импортозависимости по разным отраслям промышленности с 70—90% до 50—60%.

Отраслевые приоритеты импортозамещения

Приходится признать, что в ближайшие несколько лет нам придется продолжать строить инфраструктуры с использованием зарубежных информационных технологий. А следовательно, уместны такие вопросы: какие риски у нас возникают, и как мы можем этими рисками управлять? Среди рисков

стоит отдельно выделить угрозы для инфраструктуры, для информации и экономические угрозы. В первых двух случаях риски могут проявляться либо в виде закладок и НДВ (недекларированных возможностей), либо в виде санкций. Экономические угрозы состоят в вытеснении с рынка российских производителей и возникновении помех к развитию промышленности, и это — серьезные мотивирующие факторы для реализации планов импортозамещения.

В частности, эксперты ассоциации НАИРИТ оценивают объем лицензионных отчислений за рубеж крупнейших иностранных вендоров, работающих в России, примерно в 300 млрд руб., что составляет более 40% отечественного рынка ИТ. Можем ли мы этого избежать? Можем! Однако потребуются огромные государственные средства, время и, самое главное, кадры, которых у нас сейчас нет. Например, в области производства микрочипов и кристаллов мы можем разработать и создать архитектуру, но не можем позволить себе массовое производство и тиражирование необходимого количества кристаллов для выпуска собственных компьютеров. Правда, технологию можно купить. Но это опять-таки означает лицензию и колоссальные деньги. А ведь, по прогнозам АПКИТ и McKinsey & Company, доля информационных технологий в ВВП страны будет оставаться на уровне 1—1,3%. Важно и другое: к большому сожалению, мы утратили культуру программирования с использованием микрокодов, и для ее восстановления потребуется лет 5—7 (хотя бы на организацию обучения и выпуск специалистов).

Получается, что масштабная поддержка импортозамещения ИТ-технологий для снижения экономических рисков имеет больше ограничений, чем мотивирующих факторов. Словно подтверждая этот неутешительный вывод, Минэкономразвития определило 18 отраслей, приоритетных с точки зрения задач импортозамещения: планируется обеспечить господдержку данных отраслей при налаживании производства продукции, которая должна заместить импортируемую. Отрасль информационных технологий в этот список не вошла, и рассчитывать на помощь государства ей не приходится.

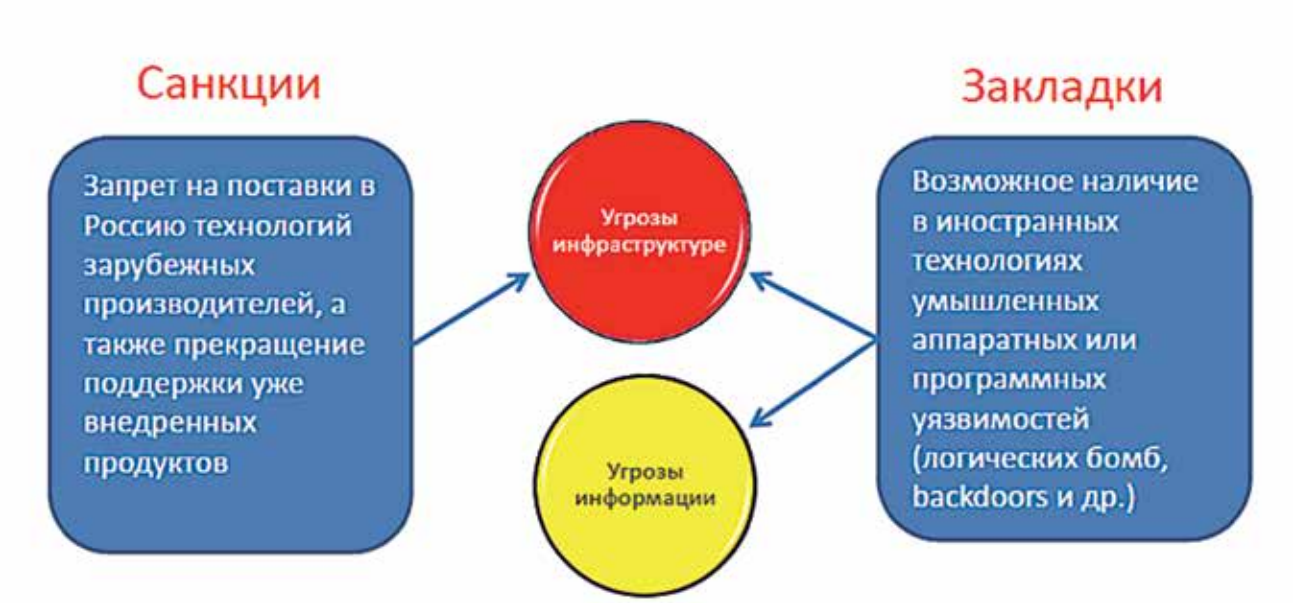
Еще раз об источниках угроз

Необходимость импортозамещения в сфере ИТ мотивируется угрозами для информации и инфраструктур, в том числе рисками утечек госсекретов, нарушений работы критически важных объектов (КВО), ГИС и пр. Но для решения проблем опять-таки нужны средства, время и кадры (причем высококвалифицированные). Сегодня, в условиях кризиса, всего этого у нас нет. Получается, что стопроцентное импортозамещение — само по себе огромный риск. Однако это не означает, что нужно сидеть сложа руки и оставаться заложниками ситуации.

На расширенном заседании Комитета ТПП РФ по промышленному развитию, состоявшемся 21 мая 2014 г., председатель этого Комитета Валерий Платонов сказал: «Развитие в российской промышленности процессов импортозамещения не означает сворачивания кооперационных и интеграционных направлений, которые позволяют сконцентрироваться на самых перспективных направлениях, рационально построить схемы ресурсообеспечения». Другими словами, Платонов призывает не отвергать все огульно, а изучать ситуацию и стараться понять, что и как мы можем сделать в кооперации.

Попробуем рассмотреть пути нейтрализации упомянутых угроз. С одной

Экономические угрозы состоят в вытеснении с рынка российских производителей и возникновении помех к развитию промышленности, и это — серьезные мотивирующие факторы для реализации планов импортозамещения.



стороны, имеются антироссийские санкции, с другой — закладки и НДВ.

Если мы начинаем бороться с санкциями, то прежде всего должны сформировать стратегию импортозамещения как серьезную государственную программу. Для этого нужно не только определить критически важные области и приоритеты замещения, но и форсировать развитие российских технологий. Кроме того, поскольку мы не можем полностью отказаться от применения импортных средств, следует построить систему контроля над этими средствами для обеспечения нужного уровня безопасности. Наконец, необходимо категорировать зарубежных производителей по степени доверия к ним и сформировать список стратегических для РФ технологических поставщиков. Безусловно, не все вендоры будут соответствовать нашим требованиям, а значит, фокус внимания может сместиться к иностранным производителям, не связанным обязательствами по санкциям и ограничениям (Китай, Индия, Корея, Сингапур и пр.).

В рамках борьбы с закладками мы должны внедрять средства, позволяющие проводить мониторинг процесса обработки информации, выявлять аномальную активность и нестандартное обращение к командам. Многие западные продукты управляются извне, т. е. их обновление идет из внешней, неподконтрольной среды. И вопрос о том, можем ли мы поставить тот или иной канал под контроль, равносилен вопросу о возможности доверять этому каналу.

В каждом конкретном случае придется искать ответы на эти вопросы индивидуально, оценивая конкретные риски. Для одних компаний некоторая потеря управления не станет трагедией, и их бизнес будет продолжаться. Для других эта проблема окажется весьма болезненной, и ее придется ставить во главу угла.

Борьба с НДВ предполагает, что на случай возникновения «жестких» условий необходимо заранее разработать план действий. Он должен включать в себя все возможные меры, в том числе полное отключение от сети и переход на «ручное» управление.

Итак, в реальных условиях требуемый уровень ИБ может обеспечить лишь «гибридное» импортозамещение. При невозможности замены абсолютно всех импортных технологий на российские нужно разрабатывать и внедрять отечественные технологии, которые позволят контролировать реализацию важнейших функций безопасности зарубежными продуктами. Кроме того, следует отказаться от использования отдельных функций импортных продуктов, заменив их российскими решениями. И отметим: уже есть примеры реализации «гибридного» подхода в области ИБ.

В рамках борьбы с закладками мы должны внедрять средства, позволяющие проводить мониторинг процесса обработки информации, выявлять аномальную активность и нестандартное обращение к командам.

ПРИоткрытый рынок ИБ АСУ ТП

Если потребность в обеспечении ИБ АСУ промышленных предприятий вполне понятна, то популяризация этой задачи влечет за собой шлейф заблуждений у многих участников рынка. Так, на нем появляется много предложений средств защиты информации, которые на деле не выполняют требований к ИБ. Продавцы убеждают владельцев АСУ в том, что обеспечить безопасность информации АСУ можно с помощью предлагаемых ими типовых средств, например межсетевых экранов. Однако, стремясь всеми способами выполнить план продаж, эти поставщики не ставят покупателей в известность об остающихся угрозах. О том, каковы реальные условия реализации требований к ИБ, выдвигаемых федеральными и отраслевыми нормативными документами, рассказывает Игорь Душа, специалист по информационной безопасности НИЯУ МИФИ.

!БДИ: Тема ИБ АСУ ТП весьма многогранна. Каковы практические проблемы в данной области, например на КВО?

И. Д.: Критически важные объекты — это те объекты, которые числятся в государственном реестре. Регуляторы (в данном контексте — ФСБ и ФСТЭК России) не только разрабатывают нормы и требования к защите информации на таких объектах, но и отвечают за применение системного подхода к выполнению этих норм участниками рынка. Важен механизм обеспечения правового статуса установленных требований, который делает их обязательными для всех участников рынка.

Основным параметром, по которому классифицируются системы защиты информации АСУ, является степень критичности последствий от деструктивных воздействий на эту информацию. Наиболее важной информации присваивается тот или иной гриф секретности, имеется статус корпоративной информации и др. Данный вопрос хорошо освещен в нашем правовом поле, поэтому лишь подчеркну: критичность информации, обрабатываемой в АСУ ТП, — это один из базовых показателей, от которого нужно отталкиваться при оценке подходов к построению систем защиты информации АСУ ТП.

Все работы по обеспечению безопасности информации АСУ ТП КВО являются «закрытыми», поэтому вызывают удивление декларации поставщиков, заверяющих, что их решения способны эффективно защищать информацию этих систем. Компании, выступающие с саморекламой, должны отдавать себе отчет в том, что профессиональное сообщество их заявления может расценивать как антирекламу. А для предприятий, не имеющих отношения к КВО, но желающих обеспечить ИБ своих АСУ ТП, эти заявления могут служить индикатором возможности доверия к таким коммерсантам.

!БДИ: Каков подход к классификации объектов, на которых необходима защита информации АСУ ТП?

И. Д.: Давайте сосредоточимся на безопасной работе объектов, потенциально опасных и очень опасных для жизни и здоровья людей, для окружающей среды. Их беспроблемное функционирование во многом зависит от степени информационной защищенности АСУ и АСУ ТП, а инциденты на таких объектах могут иметь тяжкие или даже

катастрофические последствия. Соответственно, обеспечение ИБ АСУ ТП не должно быть предметом спекуляций в коммерческих интересах! А компаниям, которые предлагают средства поиска уязвимостей в ПО, нужно признать, что все фактически существующие уязвимости обнаружить невозможно (пока таких средств попросту нет).

Еще один существенный момент: знание о выявленных уязвимостях не повысит защищенность вашей АСУ, если нельзя предотвратить угрозы, исходящие от этих уязвимостей. Так, уязвимости в базовом ПО, разработанном иностранным вендором, могут быть устранены только самим вендором — при наличии у него желания и возможности. Поэтому при построении систем безопасности необходимо базироваться на модели защиты, предусматривающей комплексный подход: не отказываться от поиска уязвимостей, но и не останавливаться на этом.

То, как выстраивать систему защиты в условиях, когда все программно-технические средства АСУ ТП изначально признаны недоверенными, является предметом отдельного обсуждения. Одно могу сказать: это крайне сложно, но возможно...

!БДИ: Как Вы считаете, может, ажиотаж вокруг темы ИБ АСУ обусловлен ее новизной?

И. Д.: Новизна этой темы весьма относительна. Рассматривая ее с точки зрения оценки угроз безопасности, выявленных в последние годы, данную тему можно считать новой. Но можно и вспомнить о документах начала 1990-х гг., таких как сих пор действующий документ Гостехкомиссии 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Описанная в нем классификация систем распространяется на все действующие и проектируемые АСУ учреждений и предприятий, обрабатывающие конфиденциальную информацию. А в наше время трудно найти системы, в которых не используется эта информация.

Таким образом, требования к защите информации АСУ виде начали появляться больше 20 лет назад. Это факт. Но то, что многие владельцы АСУ до недавнего времени ими пренебрегали, — тоже факт. Значит, говорить о «новизне» темы можно лишь применительно к тем, кто не придавали ей значения все эти годы.

Проблемы безопасности АСУ существуют ровно столько, сколько существуют сами АСУ, и присущи любой такой системе. Главное для организации, ответственной за эксплуатацию АСУ, изначально правильно классифицировать ее в соответствии с требованиями к защите информации. Если допустить ошибки на этом этапе, они станут системными, окажутся причинами разработки неверной модели угроз и негативно отразятся на определении требований к системе защиты АСУ.

!БДИ: Кто и как выполняет процедуру классификации АСУ ТП по требованиям безопасности?

И. Д.: По-разному. Если классификация АСУ проводится в соответствии с Приказом ФСТЭК России № 31 от 14 марта 2014 г., то эту процедуру осуществляет владелец АСУ или оператор, отвечающий за ее эксплуатацию. Классификация может проводиться и на других основаниях — например, если АСУ входит в состав объекта, подлежащего обязательной аттестации по требованиям безопасности. В любом случае главное — правильно применять установленные методики, позволяющие определять степень критичности информации, обрабатываемой в АСУ. От этого должен зависеть выбор ИБ-решения.

Есть масса примеров того, что процедура классификации АСУ выполняется их владельцами формально, без применения специальных методик. Порой владелец АСУ не считает выполнение соответствующих требований необходимым — мол, раньше ими пренебрегали, и все обходилось. Возможно и умышленное занижение степени критичности информации АСУ, что является для ее владельца или оператора методом снижения затрат на систему защиты и выполнение всех требований. Гораздо проще не рассчитывать реальный уровень критичности информации, а установить приказом ее низкий уровень. Это вполне возможно в организациях, в которых расчеты не проверяются или формально проверяются комиссиями, назначенными самими владельцами.

!БДИ: Как избегать ошибок, принимая решения о создании или совершенствовании системы защиты информации АСУ?

И. Д.: Все опять сводится к тому, как заказчик оценивает критичность своей системы и соответствующие риски. Очевидно, что он может обосновать как минимальные, так и максимальные риски, а они всегда рассматриваются как эквивалентный показатель ущерба. И если оператор АСУ умышленно оценивает размер вероятного ущерба как низкий, то доказать ошибочность его расчетов и решений могут лишь независимые эксперты. Однако организации, имеющие аккредитацию в соответствующей области, работают отнюдь не бесплатно. И, естественно, оператор, который фальсифицировал показатели, оплачивать проверку не станет — как и владельцы АСУ, доверяющие операторам своих систем. Ну а контролирующие органы либо вовсе не проверяют, либо редко проверяют правильность расчетов критичности информации.

Этот пример показывает, что рынок, который считается открытым, на деле открыт ровно настолько и только там, насколько и где сами владельцы или операторы АСУ его открывают.

РЕГУЛИРОВАНИЕ ЗАЩИТЫ

ФСБ

По материалам блога
Алексея Лукацкого
«Бизнес без опасности»
(http://lukatsky.blogspot.ru/2013/01/blog-post_24.html)

ЗАКОНЫ И ЗАКОНОПРОЕКТЫ

Законопроект «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры» (снят с рассмотрения)

ФЗ от 21.07.2011 №256-ФЗ «О безопасности объектов топливно-энергетического комплекса»

ФЗ от 21.07.2011 №257-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения безопасности объектов топливно-энергетического комплекса»

Законопроект «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»

УКАЗЫ ПРЕЗИДЕНТА РФ

Указ от 11.08.2003 №960 «Вопросы федеральной службы безопасности Российской Федерации»

Указ от 16.08.2004 №1085 «Вопросы Федеральной службы по техническому и экспортному контролю»

«Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз» (от 28.09.2006)

Указ от 29.12.2012 №1711 «О составе Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям»

Указ от 15.01.2013 №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

ПОСТАНОВЛЕНИЯ И РАСПОРЯЖЕНИЯ ПРАВИТЕЛЬСТВА РФ

Распоряжение от 23.03.2006 №411-рс «Об утверждении Перечня критически важных объектов Российской Федерации»

Постановление от 05.05.2012 №458 «Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса»

Постановление от 05.05.2012 №459 «Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса, порядке его проведения и критериях категорирования»

Постановление от 05.05.2012 №460 «Об утверждении правил актуализации паспорта безопасности объекта топливно-энергетического комплекса»

КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

МИНЭНЕРГО

«Рекомендации по антитеррористической защищенности объектов промышленности и энергетики Российской Федерации» (утверждены Приказом №150 от 04.05.2007)

«Методические рекомендации по анализу уязвимости производственно-технологического процесса и выявлению критических элементов объекта, оценке социально-экономических последствий совершения на объекте террористического акта, антитеррористической защищенности объекта при проведении категорирования и составления паспорта безопасности объекта топливно-энергетического комплекса» (от 10.10.2012)

ГАЗПРОМ

СТО Газпром 4.2-0-004-2009 Система обеспечения информационной безопасности ОАО «Газпром». Базовая модель угроз информационной безопасности корпоративным информационно-управляющим системам

Р Газпром 4.2-0-003-2009. Типовая политика информационной безопасности автоматизированной системы управления технологическими процессами

СТО Газпром 4.2-2-002-2009. Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами

ФСТЭК

«Методические рекомендации по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период» (от 23.04.2011)

«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (от 18.05.2007)

«Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (от 18.05.2007)

«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (от 18.05.2007)

«Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (от 18.05.2007)

«Методические рекомендации по организации контроля состояния обеспечения безопасности информации в ключевых системах информационной инфраструктуры РФ» (от 18.11.2008)

СОВЕТ БЕЗОПАСНОСТИ РФ

«Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий» (от 08.11.2005)

«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (от 04.07.2012)

ДМИТРИЙ ДАРЕНСКИЙ

Руководитель направления АСУ компании «Информзащита»

Битва пяти воинств

Любой бизнес — это история взаимоотношений людей, так или иначе в него вовлеченных. Успех каждого предприятия и проекта во многом зависит от того, насколько эффективно взаимодействуют участники бизнес-процессов. Активное обсуждение в нашей стране темы информационной безопасности АСУ ТП породило множество вопросов, связанных с взаимоотношениями между отраслевыми специалистами по ИБ, АСУ ТП, ИТ, владельцами компаний и регуляторами.

Поле битвы

Большой интерес, проявляемый в последнее время к информационной безопасности автоматизированных систем управления технологическими процессами (ИБ АСУ ТП), привел к обострению и без того накаленных отношений между специалистами разных секторов ИТ-отрасли и АСУ ТП, представителями бизнеса и, в некоторой степени, государственными и отраслевыми регуляторами. На тематических конференциях, в СМИ, на панельных дискуссиях, в социальных сетях обсуждается множество вопросов — от того, насколько целесообразно заниматься защитой АСУ ТП, до вариантов и способов реализации конкретных технических решений по обеспечению защиты и повышению ее уровня. Последние пару лет ни одно мероприятие, посвященное информационной безопасности, не обходится без докладов и дискуссий о безопасности промышленных систем управления и автоматизации.

Такая активность, конечно, не может не радовать. Во-первых, ИБ АСУ ТП, похоже, становится реальным драйвером сразу нескольких технологических секторов отечественного рынка — ИТ, ИБ и АСУ. Во-вторых, интерес к этой теме способствует формированию единого понимания соответствующих задач и подходов. В-третьих, он подталкивает законодателей и регуляторов к развитию нормативно-правовой базы.

Кроме того, если сравнить темы дискуссий, которые были актуальны два года назад и актуальны сегодня, можно сделать однозначный вывод: обсуждения получили более качественную направленность. И хотя выяснение отношений между специалистами из секторов ИТ, ИБ и АСУ продолжается, и порой дело доходит до взаимных обвинений в некомпетентности, само «поле битвы» изменилось.

Еще до недавнего времени на отдельных российских промышленных предприятиях разворачивались ситуации, похожие «по сюжету» то на боевики с саботажем, ликвидацией подразделений и лишением финансирования, то на комедии положений с «переодеваниями» специалистов и покупками хлама за миллионы, то на политические триллеры с интригами и громкими отставками. С ростом интереса к ИБ АСУ ТП в нашей стране увеличивалось и напряжение в отношениях специалистов по ИТ, ИБ и автоматизации производственных процессов. Причин для разногласий — много, и находятся они сразу в нескольких плоскостях. Это — и особенности организационных структур предприятий, и принципы финансирования функциональных подразделений, и вопросы технической реализации решений по обеспечению ИБ АСУ ТП, и то, что у некоторых руководителей до сих пор находится под вопросом сама целесообразность повышения уровня защищенности АСУ ТП.

Текущий виток отношений между отраслевыми специалистами по ИБ и АСУ ТП очень напоминает развитие уже ставшего «каноническим» спора за место под солнцем между ИТ- и ИБ-подразделениями. В свое время «ИТ-шники»

и «ИБ-шники» сломали много копий в попытке доказать друг другу и владельцам предприятий значимость своей роли в повышении эффективности бизнес-процессов, увеличении капитализации компаний, обеспечении устойчивости и безопасности функционирования предприятия и т. п. «ИТ-шники» постоянно недоумевали, зачем «ИБ-шники» вставляют им палки в колеса: то доступ ограничивают, то сервисы режут, то в Интернет не пускают. А «ИБ-шники» в попытке завоевать их доверие были вынуждены заниматься просветительской деятельностью. С течением времени отношения нормализовались, большинство противоречий были сняты, и оба лагеря поняли необходимость деятельности друг друга.

Отметим, что с ростом уровня информатизации предприятий и «цифровизации» производства, с проникновением ИТ в область АСУ ТП взаимоотношения между ИТ- и АСУ-подразделениями тоже строились не так-то просто. В качестве примера можно упомянуть программу РАО ЕЭС, подразумевавшую замену устаревших аналоговых систем телемеханики на ГРЭС и ТЭЦ на новые цифровые системы сбора и передачи технологической информации. При ее реализации противодействие между специалистами по АСУ и ИТ было колоссальным. «АСУ-шники» тяжело расставались со старыми системами — доверия к новым у них не было. В итоге возникало противодействие функциональных заказчиков, технические решения не согласовывались, бюджеты проектов то раздувались, то схлопывались, а сроки реализации постоянно сдвигались.

Причины таких отношений понятны. Эти две области, АСУ и ИТ, развивались параллельно, и с течением времени между ними увеличивался технологический разрыв. Как следствие, росло непонимание между специалистами. «АСУ-шники» искренне недоумевали, зачем им все эти ИТ, если и без них предприятие перевыполняет план по производству. А специалисты по ИТ удивлялись: зачем, например, вручную заполнять ведомости в цехе, если можно послать данные в электронном виде, ускорить бизнес-процесс, повысить эффективность, сэкономить ресурсы и время!

Похоже, в настоящее время разворачивается очередной эпизод с выяснением отношений, но уже между специалистами по ИТ, ИБ, АСУ и бизнесом.

Расстановка сил

Обозначился ряд проблем, мешающих развитию ИБ АСУ ТП, в отношениях между представителями ИТ, ИБ, АСУ, бизнеса и регуляторов. Вот — некоторые из таких болевых точек (перечень можно продолжить):

- специалисты по ИТ до сих пор убеждены в том (и часто не без оснований), что ИБ ограничивает возможности ИТ-инфраструктуры и сервисов предприятия, а соответственно, развитие бизнес-процессов, делает их менее гибкими;
- большинство специалистов по АСУ уверены (чаще всего — без оснований), что их системы хорошо защищены и нет никакой необходимости в дополнительной защите. Они ничего не понимают в обеспечении ИБ и зачастую не считают необходимым знать эту проблематику;
- многие специалисты по ИБ абсолютно не разбираются в особенностях АСУ ТП и не видят необходимости погружения в отраслевую специфику;
- специалисты по ИТ, ИБ, АСУ и представители бизнеса говорят на разных языках и плохо понимают друг друга;
- отсутствуют универсальные специалисты, одинаково хорошо знающие проблематику ИТ, ИБ и АСУ;
- бизнес зачастую не видит эффекта от инвестиций в ИБ, а уж тем более в ИБ АСУ ТП;
- регулятора не интересует эффективность бизнеса. Если вы имеете КСИИ (ключевые системы информационной инфраструктуры, в том числе АСУ ТП) или, того круче, являетесь КВО (критически важным объектом государственной инфраструктуры), то будьте добры исполнять!

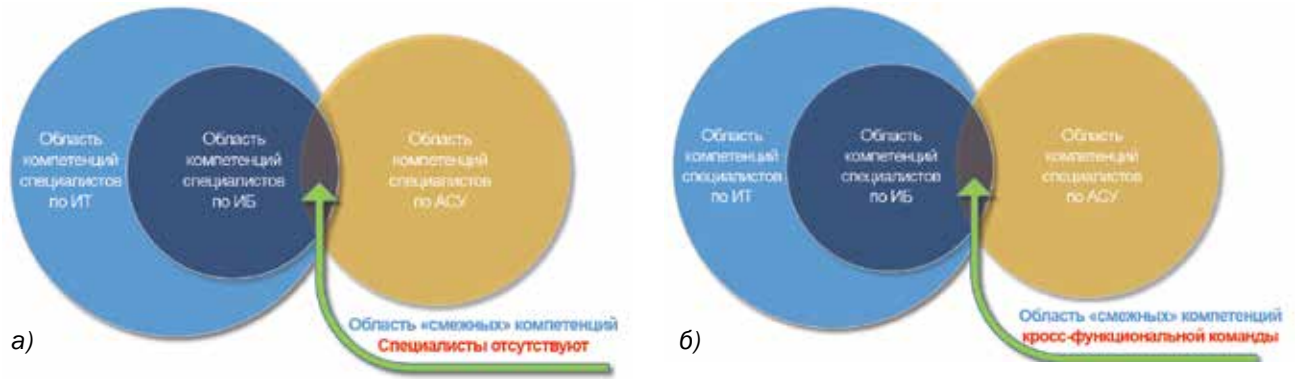


Рис.1. Взаимосвязь областей компетенций и наличие «смежных» компетенций у профильных специалистов (а) и в кросс-функциональных командах (б)

При этом всем с недавних пор стало понятно, что силами специалистов одного профильного направления (будь то ИТ, ИБ или АСУ) решить весь комплекс проблем, связанных с обеспечение информационной безопасности АСУ ТП, не получится. Во многих отраслевых презентациях встречается схема, наглядно демонстрирующая отсутствие у нас специалистов с необходимыми «смежными» компетенциями (рис.1, а). Однако в зарубежных стандартах, регулирующих обеспечение кибербезопасности технологических систем управления (например, в NIST 800), даются довольно подробные рекомендации по созданию кросс-функциональных команд специалистов из разных областей, в том числе технологов, и объясняется, для чего это нужно делать. В таком ракурсе приведенную на рис.1, а схему можно несколько изменить (рис. 1, б).

Развитие ситуации интересно и тем, что в головах руководителей и владельцев предприятий тема ИБ АСУ ТП пока присутствует лишь в виде тумана неопределенности. Они не понимают, для чего это нужно, какой «профит» от этого можно получить. Да, публикуется большое количество исследований по уязвимости и защищенности АСУ ТП, материалов, разъясняющих положения нормативно-правовых актов, описаний методик и решений по обеспечению ИБ, проводятся конференции и учебные курсы, посвященные тому, что и как защищать.... Однако, похоже, на языке бизнеса, то есть денег, объяснить необходимость защиты АСУ ТП пока никто не в состоянии.

Целесообразность инвестиций сначала в ИТ, чуть позже — в ИБ, а теперь — в ИБ АСУ ТП закономерно является краеугольным камнем в отношениях между бизнесом и представителями технологических подразделений предприятий. Ни для кого не секрет, что основные баталии разворачиваются в борьбе не за функциональные границы или штатные единицы технологических подразделений, а за бюджеты. И вполне понятно, что возможность увеличения бюджета одного подразделения, в данном случае ИБ, вызывает неоднозначную реакцию других подразделений (АСУ и ИТ).

Все против всех или все заодно?

Проиллюстрируем отношение специалистов по ИБ, ИТ, АСУ, представителей бизнеса и регуляторов к ИБ АСУ ТП (рис. 2). Закономерно, что представители профессиональных сообществ и бизнеса взаимодействуют примерно по такому сценарию, который приведен на рис. 3.

К счастью, данная картина сильно упрощена и потихоньку начинает устаревать, поскольку буквально в последние полгода-год ситуация на отечественном рынке стала

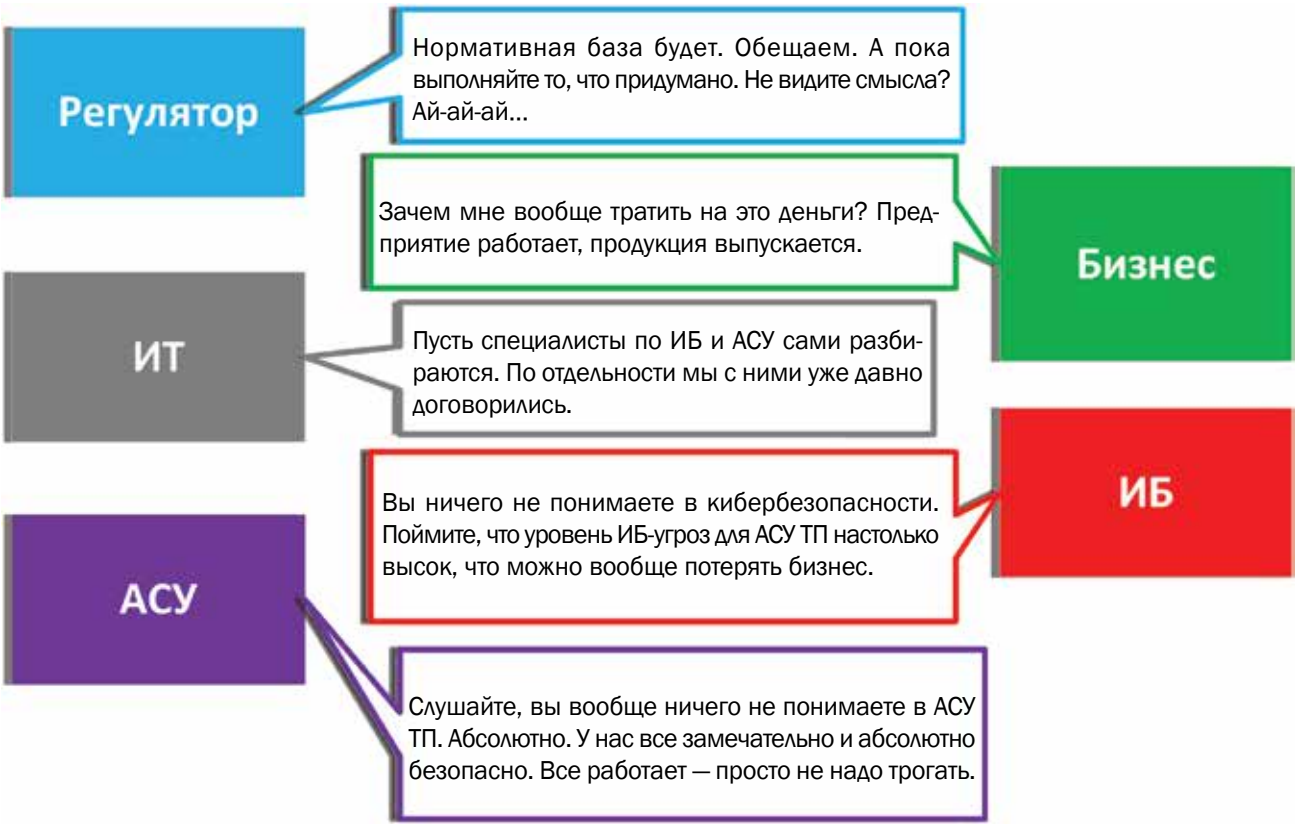


Рис. 2. Отношение специалистов по ИБ, ИТ, АСУ, представителей бизнеса и регуляторов к ИБ АСУ ТП

активно меняться в лучшую сторону. Отчасти это связано с тем тем, что регуляторы вплотную занялись нормотворчеством в области обеспечения безопасности АСУ ТП. Можно упомянуть Приказ № 31 ФСТЭК 2014 г., а также планируемые на 2015 г. публикации закона о безопасности КСИИ (КИИ) и на 2016 г. — методических документов по безопасности АСУ ТП. Да и объявленное ФСТЭК начало работы по формированию банка данных угроз и базы данных уязвимостей вселяет некоторый оптимизм.

Немаловажную роль играет и то, что за последние годы резко увеличилось как число инцидентов, связанных с кибератаками на промышленные объекты и системы технологического управления, так и количество выявля-

Комментарий

Игорь Решетников, заместитель начальника САИТиС ООО «Газпром центрремонт»

Появление в цехах информационных систем — это еще не АСУ ТП. Да, уже не уровень датчиков или контролеров, однако еще и не полноценная система управления технологическим процессом.

Статистика свидетельствует, что в мировой практике на первые места вышли следующие причины инцидентов:

- некорректная обработка входных данных — 47%;
- ошибки при настройке прав доступа — 18%;
- нарушения при аутентификации — 11%;
- пренебрежение проверкой источников данных — 8%.

По этому перечню видно, что среди причин инцидентов лидируют ошибки ПО и человеческий фактор.

Тот, кто связан с производством, знает, что грань между АСУ ТП и менеджментом, который отвечает за все происходящее на предприятии, смазана полностью. Это означает, что если в производственной цепочке происходит сбой, то плохо становится всем. Но больше всего проблем следует ожидать, тоже по статистике, на уровне MES-систем. За ними следуют инциденты на уровне локального управления корпоративной ERP-системы — в той ее части, где ERP связаны с производственными ИС. Если в управляющую ИС вводить некорректную информацию, то она некорректно и отрабатывает, и вся ценность этой информационной системы теряет смысл.

Сейчас на производстве все больше профильных и непрофильных задач «сваливаются» на цеховой уровень. Если раньше в цехе у сотрудника была установлена только одна система управления станком или технологическим процессом, то теперь приходится работать и с SAP, и с BI-системой, и с десятком других. Что в таком случае делает системный администратор? Устанавливает везде, где нужно и не нужно, дополнительное ПО — антивирусы. Но мне, например, известен случай, когда установленный на сервере антивирус «положил» систему Oracle, так как нашел в ней что-то похожее на вирус и перенес в карантин.

Кроме того, производственные системы работают не в псевдо-, а в реальном масштабе времени. А значит, такие системы крайне сложно администрировать, и для этого необходимы уникальные компетенции. Кто при этом отвечает за информационную безопасность на цеховом уровне? «Разделить между собой» систему АСУ ТП пытаются три центра компетенций — ИТ-служба, производственники и служба АСУ ТП. Как правило, ИТ-служба предпочитает ограничиваться сопровождением — все должно все работать, и больше ничего не надо. Производственники добиваются решения своих производственных проблем. А служба АСУ ТП вынуждена как-то выживать, лавируя между их интересами. Можно ли в таких условиях ожидать построения системы с нормальными уровнями надежности и безопасности?

Мне могут ответить, что «у нас есть регламенты, и они кровью написаны»... Верно, есть, но написаны они для того, чтобы находить крайних в случаях инцидентов, а не для того, чтобы этих инцидентов избегать. Но ведь критическую ситуацию надо предотвращать, не дожидаясь того, чтобы она произошла.

Безопасность АСУ ТП — вопрос неоднозначный. Мне, как практику, больше нравится, когда безопасность трактуется как «степень защищенности».

Рассуждая о защите КИС, мы не забываем о вирусах, доступе в серверные помещения и т. п. Хотелось бы, чтобы обеспечение безопасности систем АСУ ТП рассматривалось, в первую очередь, как обеспечение стабильной бесперебойной работы. И тут подходы к защите КИС и АСУ ТП полностью противоположны. Так, антивирусное ПО — уже не помощник, а враг № 1, его на терминалах АСУ ТП быть не должно.

емых уязвимостей в компонентах АСУ ТП. Естественно, рост деструктивной активности по отношению к промышленным системам никого не радует, но распространение данной информации способствует формированию единого взгляда на проблематику защиты АСУ ТП и единого вектора действий всех участников рынка.

Примерно с 2013 г. владельцы АСУ ТП стали предпринимать первые попытки повышения уровня защищенности своих систем. Они начали инициировать аудиты, изменение политик и организационно-распорядительной документации, проектирование организационных и технических мер защиты. Параллельно перестраиваются организационные структуры с учетом новых потребностей и задач обеспечения безопасности АСУ ТП. Например, на многих предприятиях электроэнергетики и ТЭК уже функционируют подразделения, занимающиеся защитой АСУ ТП. А кое-где (например, на крупных ГЭС и предприятиях нефтепереработки) реализованы первые проекты внедрения систем и средств защиты АСУ ТП.

Делая первые шаги в данном направлении при отсутствии полноценной отечественной нормативно-правовой базы, владельцы АСУ ТП в стремлении грамотно организовать взаимодействие подразделений берут на вооружение международные стандарты и методические документы зарубежных государств, которые лидируют по темпам развития данной области. Некоторые отечественные компании еще и заказывают у иностранных консалтинговых фирм, специализирующихся на безопасности АСУ ТП, аудит и анализ уровня защищенности своих систем.

Итак, буквально за последние полгода многие отечественные компании сделали первый, но очень важный шаг в верном направлении — начали налаживать взаимодействие между собственными подразделениями ИТ, ИБ и АСУ. Конечно, разногласия между ними остаются, а нужный объем компетенций по техническим и организационным вопросам по-прежнему отсутствует. Да и бизнес еще не до конца понимает, зачем ему за это платить. Но самое главное, что есть движение. И это обнадеживает.

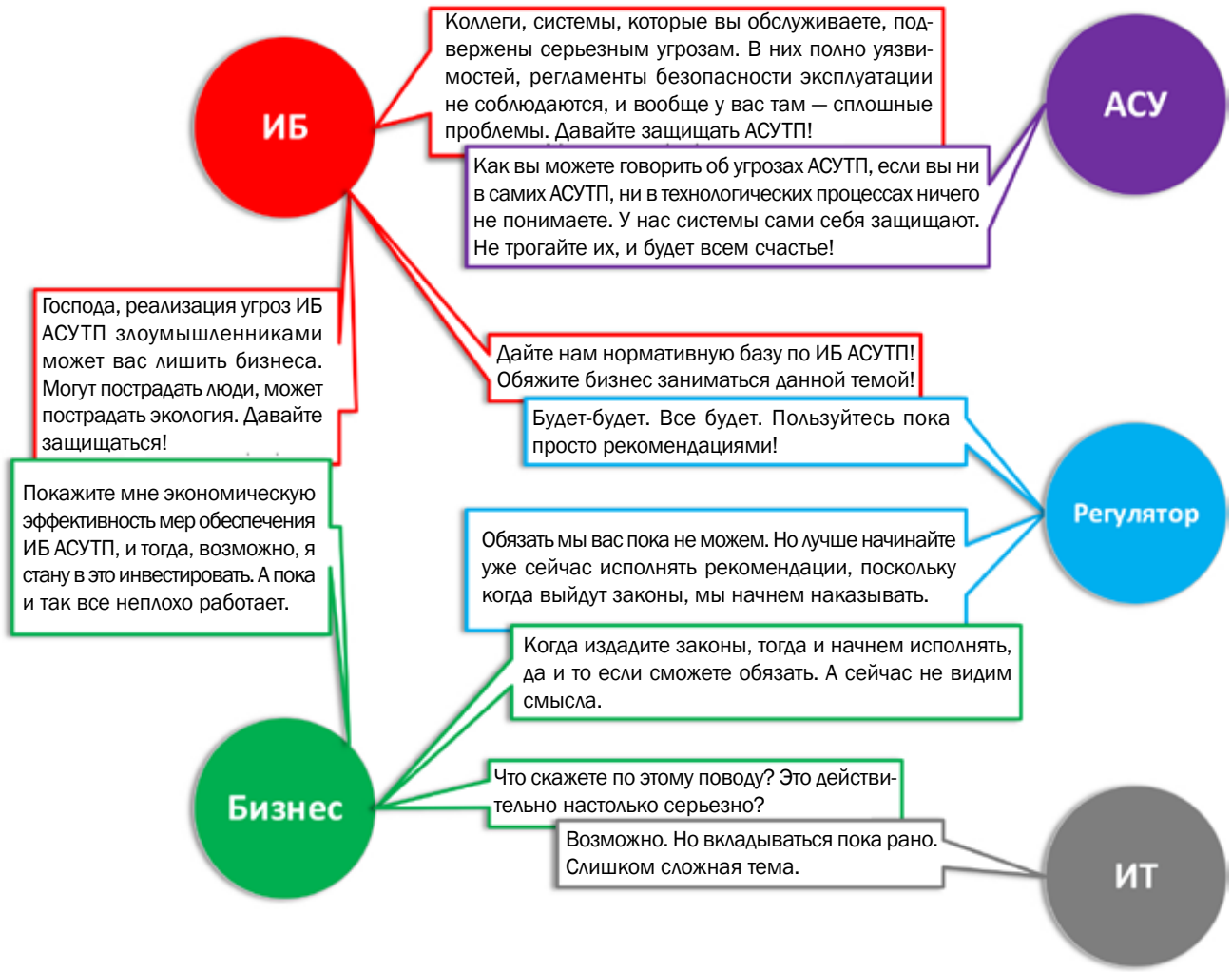


Рис. 3. Сценарий взаимодействия представителей профессиональных сообществ, бизнеса и регуляторов

Обеспечение информационной безопасности АСУ ТП

ДМИТРИЙ ИЛЬИН

Начальник отдела информационной безопасности компании «АйТи Таск»

Какие особенности работы АСУ ТП необходимо учитывать при обеспечении защиты информации в промышленных сетях? Какими нормативными документами при этом следует руководствоваться? В чем состоят различия западного и отечественного подходов к регулированию вопросов безопасности АСУ ТП? Постараемся ответить на эти вопросы.

Российская нормативная база

В России действуют не менее трех десятков документов, в той или в иной степени затрагивающих тему информационной защиты АСУ ТП. Среди всего этого многообразия можно выделить четыре документа ФСТЭК России, с выпуска которых в 2007 г., собственно, и началось предметное развитие нормативной базы в сфере защиты АСУ ТП: «Базовая модель угроз безопасности информации в КСИИ», «Методика определения актуальных угроз безопасности информации в КСИИ», «Общие требования по обеспечению безопасности информации в КСИИ», «Рекомендации по обеспечению безопасности информации в КСИИ». Эти документы распространялись под грифом ДСП, который до сих пор с них не снят.

Новый виток развития нормативной базы начался в 2011 г., когда был принят Федеральный закон № 256-ФЗ «О безопасности объектов ТЭК», обязывающий проектировать и внедрять системы обеспечения безопасности объектов ТЭК. В соответствии с этим законом субъекты отрасли должны использовать системы защиты информации и информационно-телекоммуникационных сетей от неправомерного доступа, уничтожения, модифицирования, блокирования и иных неправомерных действий. Соответственно, требуется квалифицированный персонал, который обеспечивает функционирование таких систем. Процесс обеспечения безопасности информации на объектах ТЭК, как и в любой другой отрасли, включает в себя целый комплекс организационных и технических мер.

Очередная волна развития нормативной базы пришлась на 2014 г., когда был принят Приказ ФСТЭК России № 31, содержащий требования к обеспечению защиты информации АСУ ТП на критически важных, потенциально опасных и представляющих собой повышенную опасность объектах. Сейчас именно этот документ является главенствующим с практической точки зрения.

Таким образом, у ИБ-специалистов промышленных предприятий имеется в распоряжении достаточно полная и применимая на практике база нормативных документов. Следование их требованиям вкупе со знанием лучших отраслевых практик, описанных в зарубежных документах, позволяет обеспечивать ИБ-защиту производственных и технологических процессов.

Особенности АСУ ТП с точки зрения ИБ

При разработке большинства автоматизированных систем управления технологическими процессами подразумевалось, что они не будут изменяться в будущем. Другими словами, системы, сконфигурированные 20 лет назад, до сих пор функционируют «в первозданном виде». Программное обеспечение, используемое в АСУ ТП, зачастую не обновлялось годами. Мало того, многие производители даже рекомендуют не обновлять ПО, если система работает исправно. Дело в том, что любое изменение может повлечь за собой сбои в работе

системы управления, а для производства с непрерывным циклом (такого как металлургическое предприятие или объект топливно-энергетического комплекса) это означает возможность серьезных проблем, например отказа в обслуживании промышленного оборудования.

Кроме того, индустриальные сети зачастую создавались отдельно от корпоративного контура. С течением времени менялись системы, архитектуры, оборудование, и сегодня индустриальные сети либо напрямую связаны с другими информационными системами предприятий (в частности, интегрированы с системами SAP, с ERP-системами и т. п.), либо отделены от остальных контуров межсетевыми экранами и средствами обнаружения вторжений.

Принципиальное отличие АСУ ТП от привычных для специалистов по ИБ информационных систем заключается в том, что из триады «конфиденциальность — целостность — доступность» в данном случае наиболее критичной является доступность. В «классических» системах речь шла об обеспечении конфиденциальности информации, ее защите от перехвата и компрометации, а в индустриальных системах, в первую очередь, важно, чтобы управляющий сигнал был вовремя принят и оказал необходимое воздействие. Собственно, именно поэтому вопросам обеспечения информационной безопасности в индустриальных сетях не уделялось должного внимания даже на этапе проектирования архитектуры. Как правило, в них устанавливались стандартные пароли, которые, как и настройки оборудования, не изменялись годами.

Как бы то ни было, повторим, создание и работа подсистемы обеспечения безопасности АСУ ТП не должны мешать функционированию системы управления. Для обеспечения безопасности АСУ ТП крайне редко используются криптографические решения, поскольку они, как правило, порождают избыточность вычислений и могут замедлить или вовсе остановить отправку и получение управляющего сигнала. Стандартным механизмом, предлагаемым производителями решений для защиты АСУ ТП, является периметровая защита — разделение (логическое или физическое) сетей на сегменты, которое позволяет выделить или изолировать индустриальные решения. Большое распространение получили разработанные для АСУ ТП межсетевые экраны. В целом, подход к защите индустриальных систем во многом напоминает тот, который использовался 15 лет назад для обеспечения безопасности ИТ-систем.

Западный и российский подходы к защите АСУ ТП

Для того чтобы понять, в чем состоят сходства и различия западного и отечественного подходов к регулированию вопросов безопасности АСУ ТП, достаточно сравнить 31-й приказ ФСТЭК и стандарт NIST SP 800—82. Очевидно, что при разработке Приказа № 31 специалисты ФСТЭК изучали зарубежные стандарты и рекомендации по обеспечению безопасности автоматизированных систем управления, поэтому российский документ хорошо согласован с международной нормативной базой. Тем не менее имеются и серьезные различия в подходах.

В нашем представлении NIST SP 800—82 является не стандартом, а набором рекомендаций по комплексному обеспечению безопасности индустриальных систем, содержащим методические наработки практиков. В свою очередь, Приказ ФСТЭК России № 31 — формальный документ. Он создан по аналогии с Приказами ФСТЭК № 17 и № 21, и специалисты, которые знакомы этими двумя документами, легко в нем разберутся.

В Приказе ФСТЭК № 31 вся работа по обеспечению защиты информации АСУ ТП делится на пять больших этапов:

- формирование требований (в том числе определение уровня значимости системы, необходимого класса защищенности, возможных угроз и требований к системе защиты);
- разработка системы защиты на основе сформулированных требований;
- ее внедрение;
- обеспечение защиты в процессе эксплуатации системы;
- обеспечение защиты при выводе системы из эксплуатации.

Стандарт NIST не выдвигает каких-либо формальных требований, а лишь предлагает набор методик и рекомендаций. Он содержит:

- предметные рекомендации, дающие представление о том, с чего следует начать и как наиболее эффективно построить систему защиты в целом;
- упрощенные модели злоумышленника и угроз АСУ ТП;
- большой раздел по типовым угрозам и уязвимостям АСУ ТП;
- рекомендации по созданию и реализации программы обеспечения безопасности АСУ ТП;
- подробное описание архитектуры АСУ ТП и общее описание подсистемы безопасности;
- всеобъемлющий раздел, посвященный всем классическим подсистемам информационной безопасности (контроль над доступом, идентификация и аутентификация, антивирусная защита, сети, аудиты, криптография и пр.).

Подчеркнем, что NIST SP 800—82 и Приказ ФСТЭК № 31 не противоречат друг другу. И хотя стандарт NIST является не единственным документом, которым целесообразно пользоваться, он содержит все необходимые разделы и может применяться наряду с Приказом ФСТЭК при построении системы защиты автоматизированных систем управления (в России стало распространенной практикой одновременное использование этих документов и, соответственно, подходов).

ИБ—решения для АСУ ТП

Перечислим подсистемы обеспечения информационной безопасности АСУ ТП:

- подсистема сетевой безопасности. Иногда ее делят на две системы — межсетевого экранирования и обнаружения вторжений. В таких случаях подразумевается, что в АСУ ТП будет внедрено дополнительное оборудование — межсетевые экраны и система обнаружения вторжений;
- подсистема двухфакторной (многофакторной) аутентификации;
- подсистема обеспечения целостности;
- подсистема быстрого восстановления конфигураций и данных;
- подсистема предотвращения утечек конфиденциальной информации;
- подсистема управления патчами;
- подсистема управления мобильными устройствами;
- подсистема управления неструктурированными данными;
- подсистема анализа защищенности;
- подсистема криптографической защиты.

Первые три ИБ-подсистемы являются ключевыми в АСУ ТП, поскольку позволяют наиболее эффективно сохранять доступность автоматизированной системы управления. Чаще всего построение комплексной системы безопасности начинается с обеспечения целостности — соответствующие задачи регламентируются дополнительными стандартами и руководствами, в частности NIST SP 800—12, 800—40 и 800—94.

Нужно отметить, что российский рынок решений для информационной защиты автоматизированных систем управления и индустриальных сетей находится в зачаточном состоянии. Каждый конкретный проект подразумевает сугубо индивидуальное решение. Кроме того, обеспечить безопасность АСУ ТП исключительно с помощью серийных технических средств крайне сложно. Добиться максимального «эффекта» позволяет поиск уязвимостей путем построчного анализа кода.

Дело в том, что специфика АСУ ТП (приоритет доступности) не позволяет использовать ИБ-решения с большой интеллектуальной составляющей. Если для стандартной ИТ-системы приостановка какого-то процесса в случае подозрения на вредоносную активность является нормальной мерой, то в промышленных системах это может стать причиной техногенной катастрофы.

Приоритету доступности соответствует логика работы серийных ИБ-решений для АСУ ТП, которая принципиально отличается от логики соответствующих решений для ИТ-систем. Например, межсетевой экран для АСУ ТП, по сути, играет роль обычного ключа. В нем нет интеллектуальной составляющей, и он работает по заранее определенным правилам, которые настраиваются при внедрении. Так, можно настроить межсетевой экран на блокирование сигнала с неподходящими параметрами — скажем, при повышении температуры в котле более чем на 100 град. Однако межсетевой экран легко пропустит команду злоумышленника на повышение температуры до 99 град., ведь он не «умеет» отличать сигналы администратора от сфальсифицированных сигналов.

Одним из распространенных подходов к построению ИБ-системы АСУ ТП является эшелонированная защита, которая включает в себя следующие уровни:

- физической безопасности (ограничение физического доступа к панелям управления, диспетчерским и другим помещениям, устройствам, кабелям);
- сетевой безопасности — в него входят сетевая инфраструктура (например, межсетевые экраны со встроенными сенсорами систем предотвращения вторжения) и средства защиты, интегрированные в сетевое оборудование (коммутаторы и маршрутизаторы);
- безопасности рабочих станций и серверов (управление обновлениями ПО, применение антивирусного ПО, удаление неиспользуемых приложений, протоколов и сервисов);
- безопасности приложений (аутентификация, авторизация и аудит при доступе к приложениям);
- безопасности устройств (контроль над изменениями и ограничение доступа).

Особое внимание следует уделять сетевому уровню. Многие компоненты АСУ ТП подключены к сетевой инфраструктуре IP/Ethernet, но для них не всегда возможна установка средств обеспечения ИБ, таких как антивирусы или системы предотвращения вторжений на уровне хоста.

ДАНИИЛ ТАМЕЕВ

Руководитель направления по работе с ПиТЭК Центра информационной безопасности компании «Инфосистемы Джет»

Прежде чем защищать

«Инициатива наказуема исполнением и ответственностью за проявленную инициативу». В этой грустной шутке есть большая доля истины, которой можно было бы объяснить многие сложности реализации проектов, призванных обеспечить ИБ промышленных предприятий и критически важных объектов... Но на практике все намного сложнее.

Мотиваторы инициатив

Строго говоря, российская ИБ-область технологического сегмента промышленных предприятий, в том числе систем АСУ ТП, начала серьезно развиваться буквально в последние несколько лет. Сейчас можно с определенной долей осторожности утверждать, что руководство некоторых компаний из энергетического, топливно-добывающего и других секторов экономики постепенно приходит к пониманию важности такой задачи. И это нормально, поскольку потребовалось время на осознание того, что период строительства всей технологической инфраструктуры предприятий на базе аналогового оборудования уже закончился. Не сразу удалось принять и актуальность для промышленных предприятий тех рисков, которые ранее были характерны только для корпоративной инфраструктуры (в том числе угроз со стороны хакеров, конкурентов, а порой и просто нелояльных сотрудников).

Как правило, проекты обеспечения ИБ инициируются руководителями, которые по тем или иным причинам, наконец, осознали: предприятию есть что терять в случае инцидента. «Частичное наличие» и активная доработка регуляторами законодательной базы также заставляют руководителей понять, что рано или поздно с них будет спрос за невыполнение требований законодательства.

При этом одной из особенностей отечественных компаний является стремление умолчать о произошедших с ними инцидентах. И хотя в новостных лентах довольно часто встречается такая информация, все упоминаемые в ней объекты и персоналии неизбежно являются иностранными. За рубежом эти истории становятся публичными, поскольку утаить их довольно сложно. Если же внештатная ситуация возникает в России, она максимально замалчивается. Никто не признает, что злоумышленники извне совершили на его «территории» противоправные действия, — можно рассчитывать максимум на признание факта технологического сбоя.

Соответственно, представления об актуальности задачи обеспечения ИБ в зарубежных и российских условиях заметно различаются. Отчасти этим можно объяснить общее отставание отечественного ИБ-рынка промышленных предприятий.

Профессиональный союз

Постановка задачи обеспечения ИБ промышленного предприятия, озвученная любым руководителем, примерно одинакова: необходимо добиться той самой безопасности производства в полном соответствии с требованиями законодательства и документами отраслевых регулирующих органов (некоторые из них уже выпущены, а некоторые находятся в разработке). Задачу, сформулированную именно таким образом, ставят перед руководителями служб ИБ, и они узнают, что помимо классической корпоративной безопасности должны заниматься еще и ИБ в технологическом сегменте.

С одной стороны, грамотная постановка задачи — уже половина проекта. С другой, в данном случае важна и грамотная детализация, которая зависит от совместного участия руководителей ИБ-службы и «технологов», эксплуатирующих системы технологического сегмента. На разных производствах их должности могут называться по-разному, но это — те люди, которые следят за соблюдением технологических и производственных процессов.

Кто из них должен вести проект со стороны заказчика? Совместно те же две стороны: специалист по ИБ (обычно — руководитель отдела, который зачастую подходит к обеспечению защиты с «классическим» опытом построения корпоративных систем безопасности) и руководитель, отвечающий за штатное выполнение технологических процессов. Однако на практике этот союз нередко оказывается весьма конфликтным. «Безопасники» часто не понимают специфику работы производства, а производственникам кажется, что ИБ им мешает, поскольку может нарушить штатную работу систем, да и вообще, «без нее последние 20 лет жили и дальше проживем».

Казалось бы, в их словах есть доля истины, но, пока они «спокойно жили», мир изменился до неузнаваемости. Примером могут послужить использовавшиеся ранее лишь в области обеспечения корпоративной безопасности модели угроз и нарушителей — теперь эти термины стали полностью применимыми к производственным процессам, к конкретной промышленной инфраструктуре, и в ходе реализации проекта это обязывает к разработке соответствующих документов. Ранее, при разработке АСУ ТП, аспектам информационной безопасности внимание не уделялось. В этом, по сути, и не было необходимости, ведь тогда никому не могло прийти в голову, что какой-нибудь «школьник» сможет получить через Интернет доступ к управлению заводом. А сейчас это — вполне возможный сценарий.

Особенности промышленных ИБ-проектов

В отличие от «классических» ИБ-проектов, при организации защиты технологического сегмента во главу угла приходится ставить не обеспечение конфиденциальности или целостности, а доступность. Для поддержки технологических процессов зачастую используются системы реального времени, работа которых должна выполняться штатно и не подразумевает каких-либо задержек. Соответственно, ключевой задачей ИБ-проекта становится обеспечение штатной работы систем, что, в свою очередь, обуславливает необходимость защиты от нелигитимного доступа и выполнения «классических» задач ИБ.

Вспоминаю, как генеральный директор одной крупной компании вызвал к себе директора по ИБ и главного «технолога» и поставил перед ними задачу в формате «чтобы через год был защищенный завод». И уведомил, что отвечать за это будут они оба, а значит, с обоих — и спрос. Как бы они прежде друг к другу ни относились, проект должен был стартовать! При этом сам генеральный директор не намеревался вникать в тонкости проблемы обеспечения ИБ, и задача обретала детализацию уже в рамках сотрудничества разных департаментов.

Детализация осуществляется в ходе реализации проекта, но первым шагом всегда является аудит, который позволяет выявить ключевые особенности исследуемых объектов. Дело в том, что взгляды на проект технологов и «безопасников» всегда будут разными, так как они воспринимают его через призму своих компетенций, формировавшихся на протяжении многих лет. Результаты аудита дают возможность понять, с чем именно предстоит работать, и сформулировать ряд требований, на основе которых в дальнейшем и будет создаваться система безопасности. Затем можно будет перейти непосредственно к поэтапному проектированию и построению системы. Но на каждом этапе неизбежны свои «подводные камни» и «сюрпризы».

В отличие от «классических» ИБ-проектов, зачастую типовых, защиту технологического сегмента нельзя рассматривать как разовый проект. Единожды вступив на этот путь, предстоит поддерживать весь цикл работы конкретного производства. Системы ИБ в данном случае нуждаются в такой же тщательной и внимательной поддержке, какая требуется для самих производственных процессов. И это — еще одна особенность, про которую часто забывают. В случае с АСУ ТП цикл сопровождения играет более важную роль, нежели в классических корпоративных проектах обеспечения безопасности.

Правила «жанра» ИБ, естественно, никто не отменяет, и этапы проектов обоих типов довольно схожи. Проводится обследование с выяснением всех деталей защищаемых объектов. Если речь идет о конкретном предприятии, описываются все технологические процессы. Часть информации поступает из технологической документации, а часть собирается непосредственно в ходе анализа — вживую, вручную. Затем начинается этап проектирования, на котором учитываются индустриальные ограничения (например, нельзя нарушать работоспособность предприятия, привносить в производственные процессы задержки или изменения).

Наконец, возникает вопрос, как и когда реализовать разработанный проект. Ответ на этот вопрос связан со спецификой защиты технологического сегмента: придется выполнять работы не вразрез со штатным функционированием действующих систем. Большинство подобных проектов реализуются строго в периоды технологических окон, причем на всех этапах, от аудита до внедрения. В корпоративном сегменте сотрудники ежедневно уходят домой по вечерам, есть выходные и праздничные дни, и в это время можно проводить работы по внедрению ИБ-решения. График технологических окон на любом производстве расписан минимум на полгода-год вперед. Соответственно, придется подстраивать свои действия под планы производственников.

Мониторинг аномалий сетевой активности в промышленных системах

АНТОН ШИПУЛИН

Руководитель проектов по информационной безопасности компании КРОК, автор блога «Безопасность АСУ ТП»

В сфере обеспечения ИБ промышленных систем важной задачей является выбор эффективных мер и средств защиты, которые должны предотвращать несанкционированный доступ к управлению технологическими процессами, но не создавать помехи для работы АСУ. Добиваться этого позволяют решения, обеспечивающие непрерывное пассивное наблюдение за активностью в промышленных системах и сетях, обнаружение потенциальных угроз и оперативное уведомление ответственных служб о возникающих проблемах. Среди таких решений можно выделить системы обнаружения аномалий сетевой активности (Network Behavior Anomaly Detection), применение которых в промышленных системах активно обсуждается экспертным сообществом.

Основным преимуществом систем анализа аномалий является их пассивное применение. Компоненты систем, отвечающие за сбор сетевого трафика, подключаются к зеркалирующим (SPAN) портам сетевых коммутаторов либо непосредственно к сети через TAP-устройства (это позволяет не создавать сетевые нагрузки и не порождает задержек в работе сервисов) и не взаимодействуют напрямую с промышленным оборудованием. Такие системы анализируют сетевой трафик и выделяют из него информацию о сетевых потоках (Flow). Анализ Flow-статистики более эффективен для обнаружения угроз, чем сигнатурные методы, поскольку дает возможность обнаруживать, в том числе, атаки на неизвестные (zero day) уязвимости, сигнатуры для которых еще не выпущены.

Есть и другие преимущества. С учетом того, что штатное взаимодействие устройств в промышленной сети должно быть статичным в течение продолжительного времени, развертывание систем обнаружения аномалий, их «обучение», запуск в «боевом» режиме и непрерывная эксплуатация значительно упрощаются, поскольку не требуются частые изменения профиля нормального поведения. Наконец, работа систем анализа аномалий позволяет оценить реальный уровень безопасности и выявить проблемы в системе обеспечения ИБ промышленной сети, причем результаты анализа могут стать основой ее совершенствования.

Системы класса Network Behavior Anomaly Detection (NBAD) хорошо зарекомендовали себя при защите офисных сетей и ЦОДов. Среди предложений есть как коммерческие (например, Lancope StealthWatch, Arbor Networks Pravail NSI, McAfee Network Threat Behavior Analysis), так и бесплатные (FlowMatrix, FlowBAT, Bro) решения.

Функционал этих систем включает в себя следующие возможности:

• обнаружение подключения сетевых устройств и построение карты сети;
• создание профиля нормального сетевого взаимодействия;
• мониторинг сетевой активности в режиме 24/7 для обнаружения аномального поведения (аномальные соединения, устройства, время и объемы трафика и другие показатели);
• обнаружение внешних и внутренних (связанных с преднамеренными или ошибочными действиями персонала) угроз;
• оперативное оповещение ответственных служб о проблемах и передача информации о них в смежные системы безопасности;
• ведение истории изменений сетевого поведения и помощь при расследовании инцидентов;
• формирование отчетов с разными уровнями детализации.

Эксперты утверждают, что своевременное применение решений, обеспечивающих мониторинг сетевой активности, позволило бы обнаружить активность вредоносного ПО Stuxnet, Havex и BlackEnergy, поскольку в таких случаях сетевое поведение выходит за рамки нормального взаимодействия устройств в сети. Например, не остались бы незамеченными попытки обновления прошивки контроллера по сети или сбора данных.

Несмотря на всю пользу и эффективность традиционных NBAD-систем, они не могут обнаруживать аномальное содержимое прикладных промышленных протоколов. Рост числа угроз для систем промышленной автоматизации привел к тому, что на рынке стали появляться решения, адаптированные для работы именно в промышленных сетях. Их работа основана на том же принципе пассивного сбора трафика, но они способны анализировать промышленные протоколы (deep packet inspection) и обнаруживать в них аномальные данные. В некоторых источниках этот класс решений получил название Industrial Network Anomaly Detection (INAD).

Сейчас известны следующие зарубежные решения: Dragos Security CyberLens, NexDefense Sophia, C4 Security Fides, SCADAfense. Среди российских продуктов такой функционал обеспечивают Kaspersky Trusted Monitoring System и InfoWatch Automated System Protector. Эти решения находятся на разных стадиях зрелости. Некоторые из них существуют уже несколько лет (например, NexDefense Sophia), а некоторые — только анонсированы (в частности, SCADAfense). В любом случае заметен интерес производителей и заказчиков к решениям этого класса.

Рассматриваемые системы поддерживают как открытые, так и проприетарные промышленные протоколы, в том числе DNP3, ModbusTCP, Profinet, ISO-TSAP, AB-PCCC, BACNet, Ethernet/IP и другие. В разных продуктах поддерживаемые протоколы и функциональные возможности различаются.

В общем виде системы данного класса позволяют обнаруживать следующие виды активности:

• нелегитимные команды и сетевой трафик, выводящие из строя системы управления;
• присутствие в промышленной сети вредоносного ПО, локализация очагов заражения;
• действия злоумышленников в промышленной сети без использования вредоносного ПО;
• управляющие команды, приводящие к нарушениям технологического процесса;
• команды на остановку/перезагрузку/перепрошивку/переконфигурацию контроллеров;
• команды, устанавливающие недопустимые/нежелательные значения ключевых параметров управления технологическим процессом.

Из особенностей применения таких систем отметим следующие. Им требуется значительное время на первоначальный сбор данных для построения профиля нормального поведения и задания базовой политики безопасности. Но это — плата за неиспользование активного сканирования, которое может создавать проблемы в работе промышленной сети. Кроме того, для подключения к SPAN-порту сетевого коммутатора или подключения TAP-устройства, что необходимо для пассивного сбора трафика, требуется активное взаимодействие с сетевым оборудованием (конфигурация, установка в разрыв). Однако вероятность того, что эти действия и дальнейшая работа системы приведут к проблемам, крайне мала. Эффективность систем безопасности в данном случае несравнимо выше риска от их применения.

Помимо систем, ориентированных на поиск аномалий в сетевом трафике промышленных сетей, стали появляться интересные решения, нацеленные на бесконтактное обнаружение аномалий в работе промышленного оборудования (такой функционал обеспечивает PFP Cybersecurity). Последняя задача реализуется путем наблюдения за энергопотреблением процессора.

Безусловно, выбор конкретного продукта должен осуществляться на основе анализа индивидуальных требований заказчика, особенностей промышленных систем и сетей, типа промышленного объекта. Крайне необходимо и тщательное тестирование продукта до его введения в эксплуатацию. Однако выбор решений на рынке однозначно есть.

О телепортации, мобильности и защите корпоративного пространства

Когда люди изобретут телепортацию, жить станет легче. Посиживаешь на домашнем кресле в тапочках, а потом нажимаешь кнопку — и ты уже в офисе. Никаких тебе пробок и толкотни в метро!

А ведь мы к этому уже близки, уже много всего напридумано. Например, концепция Bring Your Own Device (BYOD) дает возможность сотрудникам компаний использовать свои гаджеты как для работы, так и для личных целей. Не телепортация, но тоже удобно. Только неизбежны вопросы: как разделить свое и рабочее, как пользоваться соцсетями, не подвергая риску заражения корпоративную сеть, как не отправить письмо с секретной информацией по ненадежному каналу передачи данных?.. Конечно, работодатель может начать действовать по принципу «запретить и не пущать», но, опять же, возникнет вопрос о границах дозволенного. Кому понравится, если он станет вмешиваться в частную жизнь сотрудников, допустим вводить дресс-код в их квартирах!

К счастью, и в этом отношении прогресс не стоит на месте. О том, как сделать жизнь занятого человека удобнее, разделив личную и корпоративную информацию на одном мобильном устройстве, рассказывает Антон Разумов, руководитель группы консультантов по безопасности Check Point Software Technologies.

!БДИ: Расскажите, пожалуйста, как вы сумели решить проблему безопасного использования одного устройства для личных и корпоративных целей?

А. Р.: Мы разработали решение, которое защищает мобильные устройства и разделяет персональные и корпоративных данные. Мы и назвали его «капсулой», а точнее — Check Point Capsule, поскольку на нем создается изолированная защищенная бизнес-среда. Она позволяет защищать как корпоративные документы (причем на протяжении всего их жизненного цикла), так и само устройство — где бы оно ни находилось и к каким бы сетям ни подключалось. А значит, теперь сотрудник может полноценно работать с корпоративным документам, пользоваться электронной почтой и другими рабочими ресурсами, одновременно имея доступ к соцсетям, файлообменникам и прочей личной информации. Check Point Capsule отделяет личные данные и приложения от корпоративных, давая ИТ-службам возможность контроля только над корпоративной частью.

!БДИ: Давайте подробнее остановимся на защите документов и мобильных устройств.

А. Р.: Обмениваясь документами с коллегами, партнерами и заказчиками, компании фактически не имеют возможности контролировать, кто и куда их затем пересылает. Check Point Capsule обеспечивает секретность документа в течение всего его жизненного цикла — например, обеспечивая возможность его просмотра исключительно сотрудниками предприятия.

При использовании Check Point Capsule не требуется запоминать пароли доступа к документам. Авторизованные пользователи имеют прозрачный доступ ко всем документам, работа с которыми им разрешена. Разумеется, защиту можно перенастраивать, предоставляя права доступа отдельным партнерам и заказчикам. Эта возможность доступна как на традиционных компьютерах и ноутбуках, так и на мобильных устройствах.

Рассмотрим, как связанная с документом деятельность отображается в журнале консоли управления. В нашем примере (см. рисунок) сотрудник Джон открыл документ (internal memo), а затем сменил права доступа в соответствии с принятой политикой. Кликнув по конкретной строке журнала, можно узнать подробнее, что затем сделал Джон (например, распечатал документ и выложил файл на Dropbox). Обратите внимание на надпись Ask user: она означает, что система предупредила Джона о возможном нарушении корпоративной политики, связанном с его действиями. Он указал причину своих действий, и они были разрешены. А вот когда некий Майк попытался открыть файл, система заблокировала доступ.

С Check Point Capsule вы всегда можете узнать, кто обращался к тому или иному файлу, что с ним делал, как его менял, куда и каким образом пересылал. Наконец, с помощью Check Point Capsule можно управлять правами доступа, и это позволяет быть

уверенными в том, что только авторизованные пользователи получают доступ к документу и только в рамках их полномочий.

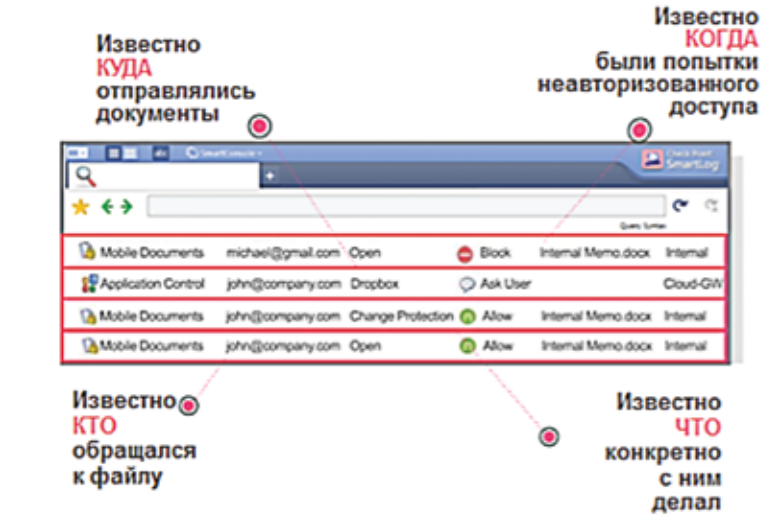
Кроме того, Check Point Capsule обеспечивает безопасность мобильных устройств на разных платформах (iOS, Android, PC и Mac), даже находящихся за пределами компании, причем к последним становятся применимыми политики корпоративной сети. Интернет-трафик перенаправляется по защищенному соединению в облако, где, собственно, и применяется корпоративная политика. Таким образом, обеспечивается защита пользователей и сети от угроз, предотвращается проникновение вредоносного ПО с мобильных устройств внутрь защищенного периметра.

Итак, Check Point Capsule позволяет применять единую корпоративную политику защиты данных, ресурсов и устройств, где бы они ни находились. В результате ИТ-службы получают мощный инструмент управления мобильными устройствами с интегрированной платформы, что дает им возможность полностью контролировать активность пользователей внутри компании и за ее пределами.

!БДИ: В условиях кризиса усиливаются риски, связанные с лояльностью сотрудников, кражей конфиденциальной информации и саботажем. Позволяет ли Check Point Capsule выявлять неблагонадежных сотрудников?

А. Р.: Да. Все действия пользователей проходят через корпоративный шлюз безопасности, фиксируются и хранятся. Можно узнать, какие письма пересылались по корпоративной почте, какие файлы скачивались и т. д. Если использовать интеграцию защиты документов, то будет зафиксировано, и какой документ открывался и просматривался. А дополнив возможности Check Point Capsule системой корреляции событий, можно будет

Отслеживаются все действия



настраивать реагирование на подозрительные действия, например слишком частую отправку писем за единицу времени. Возможно применение и других дополнительных механизмов. Допустим, если сотрудник попытается снять защиту с документа и отправить его за пределы защищенного корпоративного пространства на личный адрес электронной почты, шлюз безопасности DLP-системы это действие заблокирует.

!БДИ: Как этим всем управлять?

А. Р.: Если у заказчика уже есть решения Check Point, все просто. Заданная политика безопасности применяется и к локальным шлюзам, и к облачным, что автоматически обеспечивает одинаковые правила и механизмы защиты как внутри сети, так и вне — через облако. Если же у заказчика нет решений Check Point, и он просто хочет обезопасить работу своих мобильных сотрудников, можно воспользоваться упрощенным Web-интерфейсом.

!БДИ: Насколько сложен процесс внедрения Check Point Capsule?

А. Р.: Решение устанавливается за один день. На большое количество устройств действие «капсулы» распространяется с помощью QR-кода. Процесс достаточно прост и позволяет авторизовать и фиксировать те устройства, на которых установлен Check Point Capsule.

!БДИ: Кому бы вы порекомендовали Check Point Capsule? Насколько крупным должен быть бизнес, чтобы решение оказалось эффективным?

А. Р.: Наиболее популярно это решение у руководителей компаний. А величина бизнеса роли не играет: даже предприятию, имеющему лишь десяток сотрудников, наше решение принесет пользу. Предлагается оно на основе ежегодной подписки, месячная стоимость которой в расчете на одного человека составляет 5 долл. Согласитесь, приемлемая цена за безопасность!

!БДИ: А как вы определяете эффективность этого решения?

А. Р.: Если раньше пользователь не мог вечером ответить на письмо из дома и приходилось ждать решения важного вопроса до утра, то теперь все проблемы решаются оперативно из любой точки мира, где есть Интернет. Check Point Capsule позволяет быть быстрым, мобильным и защищенным, а это — существенные конкурентные преимущества в наше непростое время.

ВИТАЛИЙ МАЛКИН

Старший консультант компании PwC

Тестирование на проникновение АСУ ТП

Для современного бизнеса безопасность была и остается одним из важнейших аспектов. В конце XX — начале XXI вв. в связи с тенденциями информатизации общества и усложнением ИТ все большую роль стала играть защита информации. И если для компаний, не имеющих собственных производств, основными угрозами являются финансовые и репутационные риски, то на предприятиях производственной сферы проблемы обеспечения информационной безопасности могут привести к экологическим катастрофам и человеческим жертвам.

Для начала разберемся, что такое АСУ ТП и SCADA-система. Автоматизированная система управления технологическим процессом (АСУ ТП) — это комплекс технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях; АСУ ТП может быть связана с «более общей» автоматизированной системой управления предприятием (АСУП). В свою очередь, SCADA (от англ. supervisory control and data acquisition — диспетчерское управление и сбор данных) представляет собой программный пакет, предназначенный для разработки или обеспечения в режиме реального времени работы систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. Понятно, что SCADA-система не включает в себя оборудование и по отношению к АСУ ТП является лишь компонентом.

Сейчас проводится огромное количество исследований в области обеспечения информационной безопасности АСУ ТП, и их исполнители в один голос твердят: «Все очень плохо». По результатам исследования компании Positive Technologies, 54% всех АСУ ТП уязвимы к различным атакам (*http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf*). И причин столь плачевного положения дел — несколько. Во-первых, это консерватизм руководителей предприятий, которые нацелены на приоритетное обеспечение стабильности производственных процессов, а потому не желают рисковать, внося изменения (пусть даже связанные с безопасностью) в производственные системы. Во-вторых, это морально устаревшие решения, используемые в современных производственных комплексах. В-третьих, отсутствие высококвалифицированных специалистов в области обеспечения ИБ на производстве и КВО.

Но даже если в компании развернута система обеспечения информационной безопасности, это вовсе не означает, что она полностью защищена. Для того чтобы выяснить, каким реальным угрозам и рискам подвержено предприятие, рекомендуется провести на нем комплексное тестирование на проникновение (пентест).

Тестирование на проникновение

Что же такое тестирование на проникновение, и чем оно отличается от классического аудита ИБ?

Тестирование на проникновение — это вид аудита ИБ-системы, который основан на моделировании реальных действий хакера. Такое тестирование может проводиться по нескольким методикам — в зависимости от предоставляемой заказчиком информации:

- метод «черного ящика» лучше всего подходит для моделирования действий реальных злоумышленников. При его использовании специалистам, проводящим тестирования на проникновение, не предоставляется какая-либо информация о системе. Они сами собирают ее и проводят тестирование;
- метод «серого ящика» подразумевает, что специалисту предоставляется базовая информация о системе, ее назначении, а иногда даже — учетная запись для доступа в эту систему;
- метод «белого ящика» наиболее эффективен для обнаружения уязвимостей в системе. Специалистам обеспечивается полный доступ к ней, а если возможно, им еще и выдают исходный код и документацию.

Тестирование на проникновение обычно состоит из нескольких этапов.

1. Заключение контракта (в том числе о неразглашении). При тестировании АСУ ТП этот этап является одним из самых сложных. Согласование множества деталей, разделение рисков, возникающих при тестировании, составление уникального контракта для каждого случая — все это приводит к тому, что продолжительность первого этапа составляет до полугода.

2. Обнаружение компонентов системы и открытых сетевых сервисов. Данный этап проходит немного легче, поскольку все компоненты системы подробно описаны, и необходимо лишь подтвердить их наличие. Количество сетевых сервисов также весьма ограничено по сравнению с оными в офисных сетях.

3. Поиск уязвимостей в найденных компонентах и сервисах. Как и при тестировании корпоративных сетей, здесь многое зависит от того, насколько хорошо соответствующий специалист владеет навыками тестирования на проникновение. При этом основное отличие АСУ ТП от офисных сетей состоит в том, что в первых используется много низкоуровневого оборудования.

4. Эксплуатация уязвимостей. На этом этапе самой большой проблемой является эксплуатация уязвимостей на «живой» системе. Любой неверный шаг может не только нарушить производственный процесс, но и вывести из строя всю АСУ ТП.

Отметим, что этапы 2—4 могут выполняться циклически, если в процессе тестирования обнаруживаются новые системы.

5. Подготовка рекомендаций по устранению выявленных проблем. Этот этап очень важен, но зачастую оказывается бесполезным. Почему? Давайте разберемся.

Даже если в компании развернута система обеспечения информационной безопасности, это вовсе не означает, что она полностью защищена. Для того чтобы выяснить, каким реальным угрозам и рискам подвержено предприятие, рекомендуется провести на нем комплексное тестирование на проникновение.

От проблем к решениям

Тестирование на проникновение дает компании возможность оценить эффективность используемых ею механизмов защиты и обнаружения атак. При этом специфика АСУ ТП обуславливает гораздо большую, чем при проверке других систем, сложность их тестирования. Причин — сразу несколько.

Во-первых, АСУ ТП является ключевым звеном обеспечения работы промышленных объектов, и любой сбой такой системы может привести к серьезным проблемам. Классический подход к тестированию «живых» систем здесь не подходит. Вот, например, высказывание специалиста по обеспечению ИБ крупного государственного оператора АСУ ТП: «Пентесты проводят только на стендах, а на «боевую» систему вас никто не пустит. По поводу уязвимостей — да, находили, пока никто не исправил, но разработчик обещал это сделать в следующей версии. Другое дело, что создание новой версии — удовольствие дорогое и долгое. И точные сроки того, когда действительно исправят, неизвестны».

Выходом из ситуации может стать тестирование репликаций или покомпонентное тестирование системы. Правда, у этого решения есть ряд недостатков: оно является искусственным и не гаран-

тирует схожего поведения «живой» системы, а само воспроизведение полной репликации требует значительных ресурсов. Еще одно решение проблемы — проведение тестирования системы в период технологического перерыва в работе АСУ ТП. Но и в таком подходе есть свои недостатки: технологические перерывы ограничены по времени, что серьезно усложняет задачу.

Во-вторых, процесс тестирования на проникновение усложняется из-за необходимости многоуровневого тестирования системы. Можно выделить три основных направления, которые необходимо проверить при тестировании АСУ ТП: это безопасность PLC-контроллеров, проверка сегментации промышленной сети и возможных внешних связей, аудит программного обеспечения, установленного на оборудовании.

В-третьих, эффективность тестирования на проникновения страдает от консерватизма руководителей. К сожалению, на большинстве производственных объектов сейчас установлены АСУ ТП 15—20-летней давности, и работают они только с ПО, которое было написано в то же время. В лучшем случае это — Windows XP SP3, а в основном — MS DOS и Windows 98/2000/XP. Однако руководство, разумеется, предпочитает работающее, пусть и небезопасное, решение безопасному, но не работающему.

В результате основным способом защиты становится изоляция. Но изоляция в современном мире — понятие весьма размытое: как всегда, вмешивается человеческий фактор, например в виде подключенного flash-накопителя или USB-модема. И это — еще не все. Зная, что пользователи задействуют их систему как изолированную, разработчики АСУ ТП концентрируются на безопасности производственных процессов, но забывают о безопасности информационной. В результате эксперты ежедневно находят десятки новых уязвимостей в действующих SCADA-системах.

В-четвертых, фактор, серьезно затрудняющий тестирования на проникновение и обеспечение ИБ АСУ ТП — это отсутствие взаимопонимания между специалистами по ИБ и операторами АСУ ТП. Первые имеют хорошую квалификацию в области информационной безопасности, но не понимают специфику технологического процесса, а потому неправильно просчитывают риски, от чего страдает производство. Вторые ничего не знают про ИБ и считают, что их нетиповое решение взломать никому не удастся, да и вообще взламывать АСУ ТП никому не интересно.

Мы перечислили далеко не все факторы, усложняющие работу специалиста по тестированию на проникновение. Но даже они позволяют сделать вывод, что проводить такие тесты и что-то менять в соответствии с их результатами чрезвычайно сложно. Однако делать это необходимо, иначе рано или поздно нас ждет техногенная катастрофа. Так какие же решения указанных проблем можно предложить?

В первую очередь, необходим конструктивный диалог между операторами АСУ ТП и специалистами по ИБ, позволяющий эффективно обмениваться компетенциями. В таком случае ИБ-специалисты смогут повысить уровень осведомленности операторов о проблемах и задачах информационной безопасности, что обеспечит большую защищенность АСУ ТП. Операторы, со своей стороны, предоставят более детальную информацию о критически важных объектах, процессах и их слабых местах, что положительно повлияет на эффективность тестирования на проникновение и расчет рисков.

Кроме того, необходимо создание комплексной методики тестирования на проникновение АСУ ТП. Хотя системы могут очень сильно различаться, унифицированный подход поможет увеличить эффективность тестов и позволит разработчикам SCADA-систем тестировать защищенность решений еще на стадии их создания.

Необходимо и серьезно повысить уровень осведомленности о проблематике ИБ всех лиц, участвующих в принятии решения. Эта задача — общая для всей отрасли информационных технологий, но в отношении АСУ ТП она особенно актуальна. Отметим, что сейчас ситуация — намного лучше, чем несколько лет назад, и что проводится множество конференций на данную тему, но этого все равно недостаточно. Понимание серьезности проблемы руководящими лицами поможет компаниям смириться с затратами, необходимым для качественного тестирования на проникновение.

Еще одним решением является введение стандарта на ИБ АСУ ТП. В банковской сфере, например, действует огромное количество стандартов, регулирующих обеспечение информационной безопасности. Введение подобного стандарта в обсуждаемой области поможет обратить внимание руководителей на серьезные проблемы в области ИБ и, таким образом, повысить уровень защищенности производственных систем. Ну а поскольку принятие такого стандарта означает давление на производителя, при его разработке необходимо будет учесть и нынешнюю конъюнктуру рынка, и мнение самих производителей.

Аудит ИБ АСУ ТП: без резких движений

Проводится ли тестирование на проникновение (пентест) в реальных инфраструктурах АСУ ТП? Как оценивается защищенность АСУ ТП? Какие особенности АСУ ТП необходимо учитывать при таком аудите? Постараемся ответить на эти вопросы.

АЛЕКСАНДР БОЛЬШЕВ

Директор департамента безопасности АСУ ТП Digital Security

АЛЕКСЕЙ ТЮРИН

Директор департамента аудита защищенности Digital Security

Сразу подчеркнем: есть два направления работы — пентест КИС и оценка защищенности АСУ ТП предприятия. Проведение пентеста АСУ ТП является не очень хорошей затеей, поскольку элементы промышленных инфраструктур не рассчитаны на воздействия, сопровождающие пентест, и могут легко «упасть» даже от банального сканирования сетевых портов. А это повлечет за собой нарушение или даже остановку технологического процесса, что недопустимо в промышленности.

Выявление уровней инфраструктуры

Как правило, тесты на проникновение в реальных инфраструктурах АСУ ТП не проводятся. Вместо этого оценивается защищенность (security assessment) сетевой инфраструктуры АСУ ТП. А анализ КИС промышленного предприятия чаще всего не особо отличается от тестирования корпоративных сетей банков и других коммерческих организаций. Главная особенность — наличие «точки входа» из КИС предприятия в инфраструктуру АСУ ТП. Здесь находится зона повышенного риска, и при пентесте задача достижения сети АСУ ТП является одной из приоритетных.

Остановимся на оценке защищенности инфраструктуры АСУ ТП и выделим несколько ключевых задач аудитора. Типичная инфраструктура АСУ ТП сегментирована и состоит из следующих уровней:

- уровень полевых устройств, где находятся датчики, актуаторы и RTU;
- уровень программируемых логических контроллеров (PLC), или управления полевыми устройствами;
- уровень систем управления, серверов со SCADA- и DCS-компонентами, OPC-серверов и клиентов, систем HMI;
- верхний уровень контроля, или интеграции с бизнес-процессами, включающий в себя также серверы с системами MES и PAS, системы журналирования (data historian) и др. Именно с этого уровня данные попадают в КИС.

Обычно перечисленные уровни изолированы друг от друга при помощи маршрутизаторов или межсетевых экранов. Общий план оценки защищенности в этом случае выглядит как:

- анализ архитектуры системы АСУ ТП и выявление уровней;

- анализ потоков данных между уровнями;
- анализ каждого уровня в отдельности.

В некоторых случаях границы между уровнями отсутствуют, и все системы (не исключая КИС) находятся в одной подсети IP. Несмотря на явное удобство менеджмента, архитектурные слабости такой инфраструктуры тоже очевидны. Пентест получается одновременно сложным и простым: легко заключить, что все плохо, но очень трудно выявить весь спектр недостатков, ведь отсутствие уровней значительно затрудняет анализ.

Что можно порекомендовать в таком случае? Для начала — выделить основные потоки данных, провести минимальную сегментацию системы, а затем — повторную оценку защищенности. Напрасно утверждают, что работающую систему АСУ ТП невозможно сегментировать. Отделить (без какого-либо нарушения работы) системы 3-го уровня от 4-го, а 4-го — от КИС при помощи межсетевого экрана вполне реально. Кроме того, всегда можно использовать межсетевые экраны в режиме «моста» — логическое разделение на подсети не происходит, но удается постепенно вводить новые правила фильтрации и анализа трафика.

Исключение составляют лишь такие случаи, когда на одном сервере находится одновременно ПО SCADA, MES, PAS, ПО для программирования PLC и OPC в любых комбинациях. Но тогда аудитору информационной безопасности делать тут нечего: для начала инженеры АСУ ТП должны убедиться, что соблюдается хоть одно условие из одиозной триады «наблюдаемость, работоспособность, управляемость».

Исследование потоков данных

Итак, предположим, что мы оцениваем защищенность сегментированной сети. Основная задача при этом — выделение потоков данных и определение степени их критичности для технологического процесса. Необходимо составить таблицу и схему, описывающие потоки данных между уровнями и внутри них. Источники информации о таких потоках — проектная документация системы, инженеры АСУ ТП и собственные наблюдения аудитора. Последние представляют собой результаты как пассивного анализа, так и активного взаимодействия (сканирование, определение сервисов, атаки на перебор, фаззинг и т.д.). Необходимо помнить, что применение активных средств инвентаризации систем в сети, включая nmap, может привести к нарушению работоспособности отдельных компонентов. Лучше ограничиться пассивными средствами — использовать снифферы и анализаторы протоколов (e.g. Wireshark) или сканеры на базе протокола ARP.

Кроме того, учтите, что некоторые потоки данных не присутствуют в сети постоянно, а появляются с некоторой периодичностью или при определенных событиях/действиях. Важность потока данных для технологического процесса определяется после консультаций с инженерами и изучения документации. На основе полученной информации достаточно легко проанализировать конфигурации компонентов, отвечающих за сегментацию, а также выявить потоки данных, которые излишни для поддержки ТП и могут быть перенесены на другие уровни/удалены из системы.

Анализ компонентов АСУ ТП

Следующая задача — анализ компонентов на разных уровнях систем АСУ ТП. Этот процесс имеет существенные различия на каждом уровне. Анализ систем 4-го уровня практически не отличается от типичного пентеста КИС, лишь осуществляемого с большей осторожностью. Сбой работы систем на этом уровне не приведет к каким-либо нарушениям технологического процесса, но может существенно повлиять на сбор информации о нем и на бизнес-аналитику. Аудитор может применять практические любые средства сканирования и анализа сети, за исключением потенциально опасных методов воздействия (MiTM-атаки, изменение конфигурации, применение эксплойтов и др.). С некоторыми ограничениями можно использовать даже сканеры уязвимостей — естественно, только в режиме анализа.

Анализ уровней 1—3 необходимо проводить «в белых перчатках» и с особой осторожностью. Любое активное воздействие на систему может спровоцировать возникновение нештатной ситуации, не говоря уже о более серьезных последствиях. Тем не менее серверы, станции операторов и другие компоненты 3-го уровня можно проверить с помощью специальных средств сбора информации, получив данные о запущенных процессах и сервисах, установленных обновлениях, пользователях и политиках безопасности сервера, установленном ПО и др. Кроме того, анализу подлежат физическая безопасность консолей управления и станций операторов, доступные порты USB и др.

Самые сложные уровни инфраструктуры для пентестера — 1-й и 2-й. Здесь в большинстве случаем мы можем ограничиться лишь информацией из проектной документации и внешними наблюдениями. Применение каких-либо сканеров или осуществление активных воздействий может привести к нежелательным результатам. Большинство промышленных контроллеров — очень «нежные» системы, и они могут перейти в СТОП-режим от простого сканирования nmap при помощи FIN-пакетов или с использованием опции определения версии ОС/сервиса.

Тем не менее в некоторых случаях удается применять пассивные системы мониторинга трафика как Ethernet-систем, так и промышленных протоколов. В случае Ethernet это можно сделать при помощи wiretap — специального устройства, зеркалирующего Tx1 и Tx2 линии витой пары на сетевую карту аудитора. Такое устройство не влияет на работу системы, поскольку «не способно» передать информацию, но оно может выдать опытному специалисту массу полезных данных.

Для анализа трафика специфических промышленных протоколов, в том числе Modbus-RTU, HART, Profibus, FF H1, можно воспользоваться высокоимпедансным осциллографом, логическим анализатором, DAQ-системой или специализированным оборудованием. Кроме того, на этом уровне важно выявить не только документированные внешние связи системы, но и потенциальные. Например, такой связью (и потенциальной точкой атаки) может быть радиоканал или датчик мониторинга окружающей среды за пределами охраняемой зоны предприятия.

Исследование взаимодействия с внешними системами

Еще одной важной «точкой» проверки является связь между КИС и инфраструктурой АСУ ТП, а также с внешним миром. Под последним следует понимать различные дополнительные каналы связи, которые могут появляться при эксплуатации системы. Например, полное отсутствие доступа к Интернету может значительно усложнить процессы обновления какого-либо ПО (хотя бы для компонентов 4-го уровня), что заставляет использовать дополнительные устройства (3G-модемы, например) либо настраивать пути через корпоративный прокси-сервер. Любое из решений является потенциальной брешью для злоумышленника, и его работу необходимо проанализировать.

Также отличной «точкой входа» для злоумышленника могут быть WiFi-сети, которые, как ни странно, используются в инфраструктурах АСУ ТП — пусть и в качестве дополнительного канала связи для технического обслуживания. Бывает, что WiFi-сети появляются «случайно». Например, современные МФУ корпоративного уровня имеют встроенные WiFi-точки (активированные по умолчанию), к которым можно подключиться, чтобы распечатать данные. Если такое оборудование попадет в «защищенный периметр» персонала систем 4-го уровня, то через МФЦ потенциальный злоумышленник сможет добраться до части инфраструктуры АСУ ТП. Выходит, варианты связей с внешним миром имеются, и обнаружить их и проанализировать очень важно.

Если же говорить о типовых взаимосвязях КИС и инфраструктуры АСУ ТП, можно выделить две области.

Первая — связь на уровне потоков данных: какие-то системы бизнес-аналитики в КИС получают данные о производстве (из MES систем, например). Опять-таки, здесь возможно проведение атаки. Функционал многих MES широк и мало изучен с точки зрения безопасности, что делает захват контроля над системой делом довольно простым. В таком случае задача аудитора — выявление потоков данных между КИС и инфраструктурой АСУ ТП. Аудит MES, как мы упоминали, является отдельным этапом.

Отметим также, что иногда в ходе работ появляется возможность развернуть тестовый контур MES или систем других уровней и проанализировать их активными методами. Так заказчик может получить представление об уязвимых местах, привлекательных для хакера. И результатом будут уже не общие формулировки про ролевые модели и реальные векторы атак на приложение, а практические советы. Зная, как тебя могут атаковать, можно к этому подготовиться.

Вторая область, которой стоит уделить внимание, — сетевое оборудование. Все логично: если есть связь между КИС и АСУ ТП, то должно быть и сетевое оборудование, которое ее реализует (обычно это — межсетевой экран либо маршрутизатор). Вне зависимости от его типа злоумышленник может получить над ним контроль. Отметим, что возможны атаки как на само оборудование и его административные интерфейсы, так и на хосты администраторов. Завладев учетными записями нужного маршрутизатора, злоумышленник может получить доступ и к сети АСУ ТП. Стоит помнить, что серверы мониторинга, необходимые для управления большим количеством сетевого оборудования (для многих КИС это — типовая ситуация), также могут являться привлекательным каналом атак.

Функционал многих MES широк и мало изучен с точки зрения безопасности, что делает захват контроля над системой делом довольно простым. В таком случае задача аудитора — выявление потоков данных между КИС и инфраструктурой АСУ ТП.

Итак, подытожим. В зависимости от инфраструктуры АСУ ТП конкретного заказчика необходимо подобрать оптимальную комбинацию частей системы, которые подвергнутся пентесту и уровень защищенности которых будет оцениваться. Развертывание тестовых стендов систем дает более точные данные о возможных атаках. Желательно анализировать защищенность всех уровней инфраструктуры, не забывая уделять внимание выявлению и аудиту всех «точек входа» в инфраструктуру АСУ ТП.

Перекосы сознания «ИБ-шника»

МИХАИЛ САВЕЛЬЕВ

Директор Учебного центра «Информзащита»

«Есть ли разница между специалистами по информационной безопасности, защищающими разные секторы экономики?» — такой, на первый взгляд, странный вопрос задали мне недавно. Понятно, что кто-то специализируется на технических каналах утечки, кто-то — на электронной подписи, а кто-то — на персональных данных... Но вот типы мышления, подходы к решению задач, уровни осведомленности в предметных областях — должны ли они быть одинаковыми?

Перекосы сознания

В последнее время я все отчетливее вижу перекос в том, что информационную безопасность рассматривают как самостоятельное направление деятельности. Безусловно, есть соответствующие индустрия и отрасль, есть целая прослойка специалистов, есть профессиональные стандарты, которые пишутся для этой области... Но ведь не очень-то правильно рассматривать информационную безопасность как вещь в себе — она существует лишь как часть общей задачи защиты предприятия или организации! Да, это — особая часть, да, она специфическая, да, для успешного противодействия злоумышленникам на киберполе нужны особые знания и умения. Но эту специфику нельзя путать с обособленностью ИБ!

Если посмотреть, кто является основными потребителями товаров и услуг, предлагаемых индустрией информационной безопасности, то можно сделать вывод: в пул таких пользователей входят предприятия из финансового сектора, телекома и госструктуры. И это легко объяснимо. Для одних обязательным является соответствие их информационных систем определенным требованиям, для других безопасность — неотъемлемая часть всех бизнес-процессов, связанная с обеспечением непрерывности бизнеса, третьим совсем не хочется, чтобы через информационные системы у них напрямую воровали деньги. Ну а к тому же перечисленные отрасли — «рабы лампы» Закона о персональных данных.

К слову, по статистике Учебного Центра «Информзащита» (https://sdo.itsecurity.ru/UCV3/obzor_portret_specialista_po_IB.pdf), учиться чему-либо, имеющему отношение к области ИБ, приходят специалисты именно из этих секторов экономики. И именно в них информационная безопасность стала довольно самостоятельным направлением, а точнее, направлением с некоторыми специфическими задачами. При этом со временем отрыв ИБ от задач обеспечения общей безопасности предприятий начал быстро увеличиваться. В какой-то момент он стал настолько большим, что компании, продающие DLP-решения (исторически — ИТ-решения), некоторое время назад поменяли тактику продаж и стали предлагать продукты для решения задач корпоративной безопасности.

Быть ближе к жизни

Рассмотрим ситуацию, в которой информационная безопасность не является самоцелью. Например, имеется некое производственное предприятие, представитель-

ство которого в Интернете ограничено сайтом-визиткой, а корпоративная сеть — пределами административного здания. Вы скажете, что это предприятие еще не дозрело до решения задач ИБ? Что ему рано иметь выделенного специалиста? С одной стороны, да, тут нет простора для внедрения масштабных систем корреляции событий и противодействия атакам. С другой стороны, задачи обеспечения безопасности здесь более четко выражены, и хорошо видно то, о чем стали забывать специалисты из ТОП-овых отраслей.

Начнем с того, что на таком предприятии все задачи сводятся к обеспечению именно корпоративной безопасности. Даже защита персональных данных — всего лишь раздел подзадачи, подразумевающей защиту предприятия от возможных претензий со стороны государственных инстанций. Именно поэтому специалист по безопасности (давайте называть его так во избежание путаницы с более узким специалистом по ИБ) подобных компаний должен, в первую очередь, быть... бизнес-аналитиком!

Без понимания того, чем именно занимается предприятие, каковы его внешнее бизнес-окружение и конкурентная среда, какие процессы идут внутри компании и что для нее является критически важным, невозможно даже приступить к решению задач обеспечения безопасности. Не зная, от чего зависит прибыль предприятия, каковы его критически важные процессы и что является даже не коммерческой тайной, а предметом интереса со стороны конкурентов, невозможно проанализировать риски и выбрать оптимальное решение для организации защиты. Даже просто понять, где хранится, как обрабатывается и от чего именно должна быть защищена та самая критически важная информация, нереально без тщательного анализа бизнес-процессов.

А значит, затруднительно и применить подход универсального «ИБ-шника», расставив повсюду средства разграничения доступа и начав рулить правами на файловом сервере. Если специалист все же пойдет по этому пути, он, скорее всего, достаточно быстро столкнется с тем, что руководство его не понимает и денег на необходимые, с его точки зрения, вещи не выделяет. В ближайшей перспективе этот специалист, в лучшем случае, будет вынужден посещать семинары на тему «Как общаться с руководством».

Об умении общаться

К слову, умение общаться с руководством — весьма важный навык специалиста по безопасности. Но только дипломатических навыков для него недостаточно — еще больше нужны навыки психолога. Необходимо понять, что собой представляет руководитель, каковы его интересы, приоритеты и болевые точки. Еще следует осознать, что помимо тебя, безопасника, у руководителя имеются технологи, кладовщики, специалисты по безопасности производства и т. п., а всем этим людям тоже нужны деньги, и среди них, возможно, есть «более любимые жены». Убедить руководителя в необходимости выделения денег на решение каких-либо задач обеспечения безопасности (иногда припугнув его, иногда немного преувеличив, а иногда польстив) — тонкое искусство.

Именно поэтому я не применяю расхожую формулировку «говорите с бизнесом на одном языке». Это — скорее, западный подход, подразумевающий, что «бизнес» представляет собой серую толпу менеджеров с MBA, речь которых перенасыщена терминами «прибыль, затраты, маржа, возврат инвестиций» и т. п. Руководитель — такой же человек со своими страстями и слабостями, проблемами и радостями, наконец, со своим прошлым. Согласитесь, что разница между стоящими во главе предприятий бывшим конструктором, бывшим технологом и бывшим «реальным пацаном» — огромная. Кого-то нужно убеждать логикой, кого-то цифрами, а кого-то припугивать, и тут нет и никогда не будет универсальных советов.

Остальные навыки

Ну а как же навыки информационного «безопасника»? Они нужны для того, чтобы грамотно выбрать то или иное решение по защите, подобрать квалифицированного интегратора для построения и внедрения каких-либо систем и т. п. Но эти навыки вторичны по отношению к перечисленным навыкам бизнес-аналитики и общения. И если навыки убеждения руководства — во многом, дар, то освоение навыков бизнес-аналитики прибавляет большое количество очков «к карме» специалиста по ИБ, что особенно важно в наше беспокойное время.

К огромному сожалению, ни тому, ни другому не учат в подавляющем большинстве ВУЗов и учебных центров. При этом информационная безопасность является, скорее, инженерной специальностью, а истоки ее возникновения — неким замесом «ИТ-шника» и офицера по охране государственной тайны.

И еще раз повторю: превращение ИБ в довольно самостоятельное (специфическое) направление понятно в тех областях деятельности, где сами процессы обязательны, а защищать их важно любой ценой. Но, к сожалению, потом специалистам бывает очень нелегко расставаться с иллюзией своей исключительности.

АЛЕКСЕЙ ЛУКАЦКИЙ

Бизнес-консультант по безопасности Cisco Systems

Специалист по ИБ КВО — кто он?

На государственном уровне проблемой обеспечения ИБ КВО в России стали заниматься еще в 2006 г., когда появился первый законопроект в этой области, но к решению кадрового вопроса так до сих пор и не подошли. Ждут, когда бабахнет?..

В России насчитывается чуть меньше 4500 критически важных объектов (КВО), на абсолютном большинстве которых работает минимум одна АСУ ТП. Но по данным МВД в России — примерно 57 000 критически важных объектов. Как возник такой разрыв в цифрах? Как гласит русская пословица, у семи нянек дитя без глаза. Так и у семи отечественных регуляторов (Совет Безопасности, ФСБ, ФСТЭК, Ростехнадзор, МЧС, Минэнерго и МВД) нет единого определения КВО и, соответственно, единой статистики. Однако это не так-то и важно с учетом скорого принятия законопроекта «О безопасности критических информационных инфраструктур», который не только установит новые определения и термины, но и изменит дефиницию понятия «критически важная инфраструктура».

По версии его авторов из ФСБ, под действие данного законопроекта могут попасть не только традиционные отрасли, но и банки, госорганы и прочие организации. Правда, часть отраслей вряд ли столкнется с чем-то совсем новым, и требования по обеспечению их безопасности, скорее всего, будут мало отличаться от СТО БР ИББС Банка России или стандартов ISO 270xx. Интерес представляет ИБ «традиционно» критически важных отраслей — автомобильной, радиоэлектронной, химической, пищевой, машиностроительной, нефтегазовой, металлургической, энергетической, транспортной, водоснабжения и канализации.

Очевидно, что перечень этот неполон, но он достаточен для понимания проблематики. В каждой из упомянутых отраслей — свои технологические процессы и системы их автоматизации и управления, свои условия информатизации, ограничения и особенности. Грести всех под одну гребенку не получится: необходимо разделять ИБ процессов, скажем, приготовления продуктов питания, добычи электроэнергии, транспортировки нефти по трубопроводу и управления авиационным транспортом. И хотя базовые знания в области ИБ (криптография, сегментация, разграничение доступа, регистрация событий, аутентификация, управление инцидентами и пр.) остаются неизменными, их применение в конкретных ситуациях и в конкретных отраслях может сильно варьироваться.

Кого готовят ВУЗы?

Возникают закономерный вопрос: а есть ли у нас специалисты по ИБ традиционных КВО? Если рассмотреть государственные образовательные стандарты (ГОСы) первого и второго поколений (издаются в России с 2000 г.), а также федеральные государственные образовательные стандарты (ФГОСы) третьего и четвертого, последнего, поколений, можно увидеть, что тема информационной безопасности КВО и АСУ ТП в них практически не представлена. В стандартах первых двух поколений — уж точно!

По данным учебно-методического объединения ВУЗов России по образованию в сфере ИБ (http://www.isedu.ru/), сегодня в УМО входят 74 высших учебных заведения, готовящих специалистов по информационной безопасности. Из наиболее близких к специфике КВО есть лишь специальность 090303 «Информационная безопасность автоматизированных систем» (ранее — 075500 «Комплексное обеспечение информационной безопасности автоматизированных систем»), причем из указанных ВУЗов только 39 выпускают специалистов по безопасности АС. Получается, в идеале, что за последние 5 лет (прежде интерес к «нашей» тематике почти не проявлялся) было примерно 5000 выпускников данного профиля.

Стоп-стоп, но это же не наш профиль, ведь АС и АСУ ТП — две большие разницы, скажете вы, и будете правы! Поэтому давайте рассмотрим специализации, которые входят в специальность 090303. Их насчитывается 10, и 8 из них предполагают работу с разными типами автоматизированных и информационных систем: АИС специального назначения, высокопроизводительные вычислительные системы специального назначения, ИБ автоматизированных систем КВО, ИБ открытых информационных систем, ИБ автоматизированных банковских систем, защищенные автоматизированные системы управления, обеспечение ИБ распределенных информационных систем, ИБ автоматизированных систем на транспорте. Как мы видим, только две специализации имеют отношение к критически важным объектам — ИБ АС КВО и ИБ АС на транспорте. Если предположить, что по каждой из 10 специализаций обучается одинаковое число студентов, то на выходе мы получим всего 1000 человек, которых можно называть специалистами по ИБ АСУ ТП (которые, к слову, не все работают по специальности).

Но и это — лишь в теории… Задумаемся о том, что должен знать выпускник специальности 090303 и ее специализаций, связанных с КВО. Для ответа на этот вопрос обратимся к документу ФГОСа, в котором указаны следующие знания специалиста по ИБ АСУ ТП (выборочно):

- методы статистической радиотехники;
- методы расчета и измерения параметров основных линий передачи высокочастотного диапазона;
- основные тенденции развития теории и техники антенн и сверхвысокочастотных устройств;
- основные нормативные правовые акты в области метрологии;
- способы нормирования и формы задания метрологических характеристик средств измерений;
- языки описания цифрового автомата с памятью и методы синтеза схем цифрового автомата произвольного назначения на элементах различного базиса и степени интеграции;
- основные машинные алгоритмы и характеристики их сложности для типовых задач, часто встречающихся и ставших «классическими» в области информатики и программирования;
- влияние способов кодирования на сложность структуры цифрового автомата, его быстродействие, устойчивость и надежность работы.

Среди основных умений специалиста по ИБ АСУ ТП числятся:

- умение дифференцировать функции комплексного переменного, строить конформные отображения простейших областей, вычислять комплексные интегралы, раскладывать функции в ряды Тейлора и Лорана, вычислять вычеты функций;
- умение определять структуру оптимальных устройств обработки сигналов информационных радиотехнических систем и оценивать эффективность их работы;
- умение синтезировать логические схемы блоков операционного и управляющего автоматов с использованием методов синтеза цифрового автомата.

Наконец, выпускник должен владеть:

- методами комплексного анализа для вычисления определенных и несобственных интегралов, решения других задач алгебры и анализа;
- методами проектирования, удовлетворяющими заданным требованиям надежности;
- навыками разработки алгоритмов и программ, структур данных, используемых для представления типовых информационных объектов.

А теперь ответьте: что из перечисленного необходимо на практике? Думаю, если выпускник ВУЗа по ИБ-специальности и обладает хотя бы половиной перечисленных знаний и умений, то на практике он не будет их использовать в 99% случаев. В упомянутом ФГОСе нет ни слова о специфике защиты информации в АСУ ТП и обеспечения ИБ КВО.

Однако помимо специальных ФГОСов по ИБ имеется и множество ФГОСов для специалистов, которые будут работать в разных отраслях экономики, в том числе на КВО. Например, это «Теплоэнергетика и теплотехника», «Атомные станции: проектирование, эксплуатация и инжиниринг» или более общий «Автоматизация технологических процессов и производств». Но и тут похвастать особо нечем. Почти все ФГОСы, как под копирку, без какой-либо конкретизации сообщают, что выпускник должен обладать «способностью понимать сущность и значение информации в развитии современного информационного общества, осознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны». А упомянутый ФГОС по автоматизации технологических процессов содержит еще одно «вкрапление» темы ИБ: выпускник должен знать, как создавать и применять «алгоритмическое, аппаратное и программное обеспечение систем автоматизации, управления и контроля технологическими процессами и производствами, (…) освобождающих человека полностью или частично от непосредственного участия в процессах получения, трансформации, передачи, использования, защиты информации и управления производством».

Кто нужен Минтруду и Минздраву?

Получается, что выпускников, способных трудится на ниве ИБ КВО, в России нет. Что по этому поводу думают те, кому по должности положено определять квалификацию специалистов, работающих на производстве? В 2009 г. Минздравсоцразвития выпустило Приказ №205, утвердивший единый квалификационный справочник должностей руководителей,

специалистов и служащих. В нем есть характеристики должностей специалистов по обеспечению ИБ в ключевых системах информационной инфраструктуры, специалистов по противодействию техническим разведкам и технической защите информации, но нет ни слова о компетенциях, которыми должен обладать специалист по ИБ АСУ ТП. Кстати, в приказе Минздрава используются понятия не «АСУ ТП» и «критические информационные инфраструктуры», а «ключевые системы информационной инфраструктуры», и это в очередной раз вносит путаницу в представление о том, что именно должен защищать выпускник ВУЗа, приходящий работать на критически важный объект.

В попытке устранить несоответствие между тем, кого готовят по ФГОСам, и тем, кто действительно нужен бизнесу, родилась идея профессиональных стандартов. Они должны описывать квалификации, необходимые для осуществления определенной профессиональной деятельности. Профессиональный стандарт является новой формой определения квалификации работника по сравнению с единым квалификационным справочником должностей руководителей, специалистов и служащих.

В 2013 г. была предпринята попытка разработать под эгидой Минтруда такой стандарт и для отрасли ИБ. Увы, не получилось… В результате работы, которую критиковало большинство специалистов отрасли, появился лишь один профессиональный стандарт ИБ-специалиста, «покрывающий» все возможные области его деятельности — от защиты государственных информационных систем и гостайны до безопасности АСУ ТП на КВО и защиты персональных данных на коммерческом предприятии.

В пояснительной записке к этому стандарту было написано, что необходимы не один, а минимум 10—15 профессиональных стандартов для разных отраслей и сфер деятельности. Правда, среди таких стандартов, предложенных УМО, места специалистам по ИБ АСУ ТП тоже не нашлось — дело ограничилось специалистом по ИБ автоматизированных систем. К сожалению, Минтруда не прислушался и к этому мнению, и ситуация стала даже более сложной, чем до 2013 г.: принятый Минтруда единственный профессиональный стандарт не стыкуется с несколькими ФГОСами, утвержденными Минобрнауки и описывающими специализации по ИБ.

В попытке устранить несоответствие между тем, кого готовят по ФГОСам, и тем, кто действительно нужен бизнесу, родилась идея профессиональных стандартов.

Что делать?

В утвержденных Президентом РФ в 2012 г. основных направлениях государственной политики в области защиты АСУ ТП КВО Российской Федерации прямо указывается, что «недостаточный уровень образования и профессиональной подготовки персонала, обслуживающего автоматизированные системы управления КВО, снижение технологической культуры производства» входят в число ключевых проблем государства в данной сфере, однако пока никто из уполномоченных органов не занялся вопросами подготовки кадров. И это несмотря на то, что в основах госполитики явно прописано среди основных задач «совершенствование системы подготовки, переподготовки и аттестации кадров (в том числе руководящих) в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры на базе профильных образовательных учреждений».

Что делать в такой ситуации? Я вижу два возможных пути решения кадровой проблемы.

Первый — долгий, но наиболее эффективный — заключается в доработке ФГОСов и включении в них дисциплин, связанных с реальной защитой информации в АСУ ТП, вместо теоретических умений раскладывать функции в ряд Тейлора. Правда, на подготовку и принятие изменений в ФГОС потребуется не менее года, а первый выпуск специалистов появится не ранее чем через пять с половиной лет. Иными словами, ранее 2021 г. первых выпускников, которые хоть что-то знают в области ИБ КВО, нам не дождаться. Вопрос квалификации действующих преподавателей оставим за кадром.

Второй путь заключается в переподготовке специалистов, работающих на КВО и имеющих отношение к защите АСУ ТП. В России такая переподготовка ведется как производителями АСУ ТП (например, Schneider Electric и Siemens) и средств защиты («Лаборатория Касперского»), так и специализированными учебными центрами. Последние, в свою очередь, делятся на обучающие по согласованным с ФСТЭК программам дополнительного профессионального образования специалистов по безопасности информации в КСИИ (НПП «Гамма», АНО УМЦ «ХимИнформЗащита») и на более приближенные к реальной жизни (такие как курсы АИС).

В частности, АИС предлагает вводный курс «Стратегия обеспечения информационной безопасности индустриальных решений», в котором рассматриваются ключевые вопросы, интересующие специалиста по ИБ АСУ ТП. И, видимо, не важно, какой из двух указанных путей выбрать — главное, начать продвигаться вперед.

Специалист по ИБ промышленного масштаба

ЮРИЙ МАЛИНИН

Ректор «Академии Информационных Систем»

ИГОРЬ ЕЛИСЕЕВ

Эксперт-аналитик «Академии Информационных Систем»

Подготовка специалиста по информационной безопасности промышленных предприятий — нетривиальная задача. Функции ИБ-специалиста в промышленности нельзя свести лишь к защите офисной сети заводоуправления и индустриальной сети передачи данных производственных цехов. В информационных системах крупных производственных предприятий циркулирует самая разная информация, потеря или искажение которой может привести к серьезным последствиям. Следовательно, подходы к защите информации тоже должны различаться.

Отраслевое многообразие

Несмотря на заявленный правительством курс на ускоренное развитие отечественного производства, импортозамещение, подготовку квалифицированных кадров для ОПК и т. д., есть стойкое ощущение, что вопросам ИБ в промышленности уделяется меньше внимания, чем в банковской сфере.

В финансовом секторе процедуры защиты информации жестко регламентированы нормативными документами, отраслевыми стандартами и требованиями регуляторов. С одной стороны, зарегулированность увеличивает бюрократическую нагрузку на службы ИБ и роль так называемой «бумажной» безопасности. С другой стороны, упрощается обучение специалистов, поскольку вдобавок к стандартным техническим знаниям по работе с СЗИ им достаточно изучить свод четко прописанных нормативно-правовых актов.

В реальном секторе экономики все гораздо сложнее. В силу того, что на предприятиях производственные и технологические процессы существенно различаются, а обсуживающая ИТ-инфраструктура является критически важной, создание единого свода правил или стандарта защиты информации для всех отраслей невозможно в принципе. В критически важных отраслях (атомная энергетика, ТЭК, транспорт) действуют разные федеральные законы и подзаконные акты в области обеспечения безопасности. И хотя они не устанавливают правила защиты информации на подведомственных предприятиях напрямую,

каждый сотрудник службы ИБ обязан знать их и принимать во внимание при оценке угроз и рисков.

Неким «общим знаменателем» в системе нормативного регулирования вопросов информационной безопасности является Приказ № 31 ФСТЭК России. Он утверждает требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах и объектах, представляющих собой повышенную опасность для жизни и здоровья людей и для окружающей среды. Однако требования этого Приказа распространяются только на АСУ ТП и только на объекты критической важности и потенциальной опасности, которая, в свою очередь, определяется другими законодательными актами РФ. А ИКТ-инфраструктура промышленных предприятий, как мы уже отметили, не ограничивается АСУ ТП, и в других ее сегментах применяются иные требования.

Помимо федеральных законов отраслевой направленности, регулирующих обеспечение ИБ, некоторые системообразующие корпорации приняли внутриведомственные стандарты информационной безопасности, в которых учитываются особенности их технологических и бизнес-процессов, характерные угрозы и риски. Такие стандарты есть, к примеру, у «Газпрома», «Роснефти», «Ростатома», РЖД. С учетом сложностей комплексного методичного выполнения требований ФСТЭК к защите АСУ ТП можно утверждать, что ведомственные стандарты ИБ являются едва ли не единственным ориентиром для построения политик и осуществления практических мер по обеспечению корпоративной ИБ.

Наличие у крупных корпораций ведомственных стандартов, как и в банковской сфере, упрощает процесс подготовки ИБ-специалистов для собственных нужд. При этом изучение таких документов явятся хорошим подспорьем и для всех прочих специалистов и менеджеров по информационной безопасности, так как ведомственные стандарты можно трактовать как лучшие отраслевые практики построения промышленных ИБ-служб. Аналогично, изучение рекомендаций международных институтов стандартизации (ISA, NIST, IEC, NERC, ENISA и др.) позволяет отечественным специалистам быть в курсе современных тенденций и подходов к защите автоматизированных систем управления, применять их при решении конкретных практических задач.

Повышение квалификации: теория и практика

Отсутствие в России единых стандартов обеспечения информационной безопасности в промышленности привело к тому, что в области дополнительного профобразования практически нет соответствующих комплексных программ повышения квалификации специалистов и менеджеров по ИБ. При этом в условиях актуальности угроз кибертерроризма и западных санкций потребность в подготовке промышленно-ориентированных специалистов по защите информации не вызывает сомнений.

Как разобраться в многообразии документов, стандартов и требований, чем отличается традиционная корпоративная ИБ от ИБ индустриального объекта, как выполнить последние требования ФСТЭК, каков передовой отечественный и зарубежный опыт защиты индустриальных активов? Ответы на эти и другие вопросы дают возможность определить основные подходы к обеспечению информационной защиты промышленных предприятий, выработать общее направление действий. Такие знания особенно важны для руководителей служб ИБ, так как позволяют им выйти за рамки привычной парадигмы защиты информации в корпоративной сети, в которой во главу угла ставится конфиденциальность. В случае АСУ ТП, как мы знаем, на первый план выходит поддержка целостности и доступности информации, что требует определенных изменений в стратегии обеспечения ИБ.

На наш взгляд, «теоретический» блок вопросов следует изложить в отдельной, пусть и краткой учебной программе. По заказу «Академии Информационных Систем» весной 2014 г. соответствующий курс разработал Алексей Лукацкий, известный эксперт в области информационной безопасности. Двухдневный семинар «Стратегия обеспечения информационной безопасности индустриальных решений» проводит только его автор и только в АИС.

Разумеется, даже самая тщательная теоретическая подготовка ИБ-специалистов не заменит необходимости получения практических навыков защиты АСУ ТП с детальным разбором задач и примеров их решения. Именно таким аспектам уделяется основное внимание в рамках другого авторского курса, «Практические аспекты защиты АСУ ТП и промышленных сетей», который разработан АИС совместно с компанией NGS Distribution. Этот курс адресован руководителям и специалистам служб информационной безопасности промышленных предприятий, а также интеграторам и консультантам, выполняющим у заказчиков работы по обеспечению защиты АСУ ТП.

Разработчики курса постарались учесть традиционные расхождения во взглядах между теми, кто защищают информацию, и теми, кто эксплуатируют технологические сети. Слушателям даются комплексные знания на стыке областей АСУ ТП, информационной безопасности и информационных технологий. Другим важным

Что должен знать и уметь ИБ–специалист промышленного предприятия

Алексей Волков, начальник отдела ИБ компании «Северсталь»

Помимо собственно обеспечения ИБ он должен знать производство, разбираться в используемых АСУ и уметь договариваться с теми, кто их обслуживает. А для того, чтобы с ними договориться, потребуется признание его авторитета, поэтому задача — не из простых. Идеальный вариант — вырастить «ИБ-шника» из «АСУТП-шника». Кроме того, хорошие специалисты по ИБ получаются, как и в области классической ИТ-безопасности, из «айтишников».

Для защиты конкретного производства достаточно знания специфических угроз и умения им противодействовать. А уж как это осуществлять, технически или организационно, — дело десятое. Можно привлечь консультантов, и они разработают документы, поставят систему и потом будут ее обслуживать. Но контролировать проект и говорить, где и что устанавливать, должен штатный специалист заказчика. И за любую ошибку отвечать ему!

Рустем Хайретдинов, глава Appercut Security, бывший советник генерального директора «РТ-Информ» (дочерней компании «Ростех»)

Промышленные предприятия имеют по несколько периметров защиты информации, поэтому спектр требований к их ИБ-специалистам — довольно широкий. Конструкторская и производственная документация, отражающая ноу-хау компании и составляющая основу ее конкурентоспособности, требует одной процедуры защиты, коммерческая тайна (условия контрактов, закупочные и отпускные цены) — другой, а персональные данные сотрудников — третьей. Если предприятие входит в список критически важных объектов, то к этим процедурам добавляются требования ФСБ, если выполняет гособоронзаказ — требования к защите государственной тайны.

В общем, работы в промышленных компаниях — начать и кончить, хотя на них средняя зарплата безопасника — гораздо ниже, чем в банках, а вникать в детали производства нужно гораздо глубже. И если технические навыки настройки оборудования одинаковы в любой компании, то требования к руководителям ИБ-служб в промышленности — более жесткие в силу более сложной юридической базы и нормативных требований.

Юрий Ипатов, руководитель департамента информационных технологий компании «Трансмашхолдинг»

В машиностроительном бизнесе, в котором используется большое количество самой разной информации ограниченного доступа, специалист по ИБ должен уметь четко разделять информационную систему на подсистемы по принципу уровня защищенности, концентрируясь на критичных для технологического процесса «местах». В связи со сложностью и многообразием информационных систем в машиностроении от ИБ-специалиста требуется целостный подход к обеспечению безопасности, углубленное знание сетевых и серверных технологий. Кроме того, в машиностроительной отрасли желательно, чтобы специалист по ИБ имел представление о производственных процессах и применяемых автоматизированных системах управления такими процессами, а также хорошо знал российскую правоприменительную практику в области законодательного регулирования вопросов ИБ — для соблюдения соответствующих законодательных и нормативных требований.

аспектом является то, что преподаватели ссылаются на «живые», реализованные компанией проекты и демонстрируют ряд решений в «боевом» режиме. Представитель NGS Distribution Алексей Комаров отмечает: «Современный специалист не может обойтись без практического опыта, но для его получения требуется достаточно длительное время, к тому же необходим доступ к всевозможному оборудованию систем АСУ ТП и средств их защиты. Именно поэтому мы фокусируемся на практических аспектах и делимся со слушателями наработками, которые появились у нас в ходе каждодневной практической деятельности на реальных объектах при реализации реальных проектов».

Наконец, квалифицированному специалисту по ИБ промышленного предприятия не в последнюю очередь необходимы и такие личные профессиональные качества, как умение брать на себя ответственность за принимаемые решения, работать в команде и, конечно же, крепкая нервная система. По мнению Алексея Комарова, способность находить общий язык с представителями разных команд очень важна для успеха проекта, поскольку защита АСУ ТП находится на стыке зон ответственности нескольких корпоративных подразделений.

АНДРЕЙ ВЛАСОВ

Аспирант Финансового университета

Страхование инфорисков как часть системы риск-менеджмента

В условиях бурного развития информационно-коммуникационных технологий, активной деятельности предприятий в Интернете, постоянно растущей «интенсивности» киберугроз компаниям следует обращать внимание на защиту прав собственности от киберрисков с помощью страхования.

Применение современных технологий кибернетики и связи, Интернета вещей (IoT), больших массивов данных (Big data) для реализации стратегических и операционных задач предприятий приводит к появлению новых киберугроз для бизнеса — таких как киберкражи, целенаправленные атаки (Advanced Persistent Threat, APT), распределенные атаки типа «отказ в обслуживании» (Distributed Denial of Service, DDoS), кибершпионаж, кибертерроризм и хактивизм. Значительный рост числа атак через Интернет, огромное количество утечек и компрометированных данных заставляют компании уделять все больше внимания защите их информационных систем и искать дополнительные инструменты управления рисками ИБ.

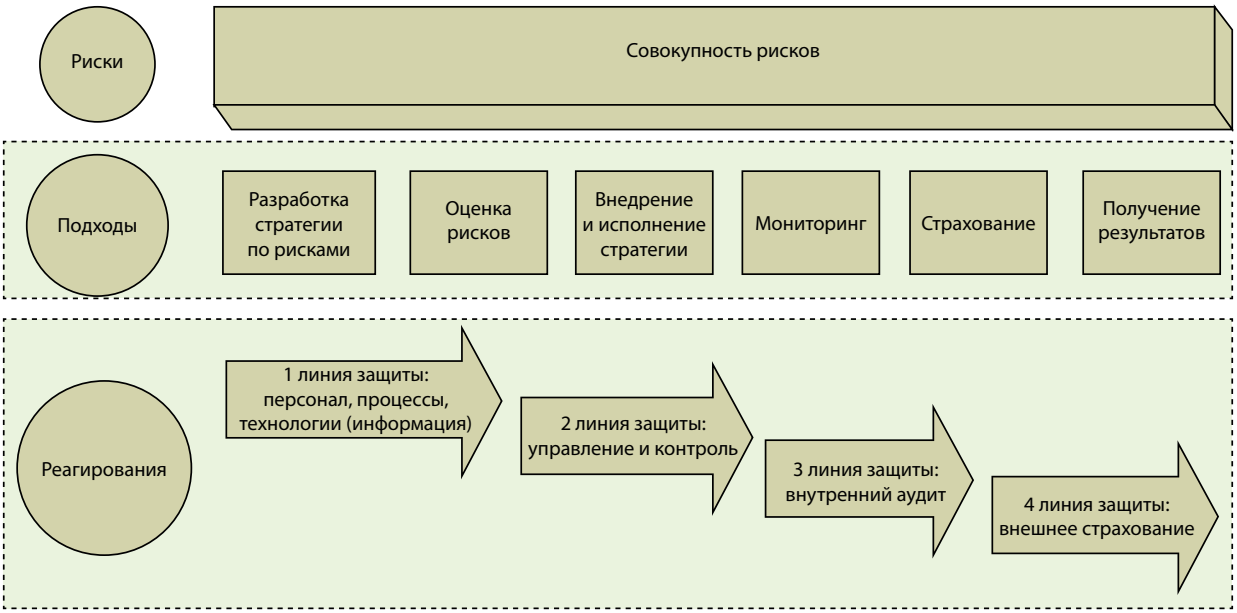


Рис. 1. Классификация рисков современной организации

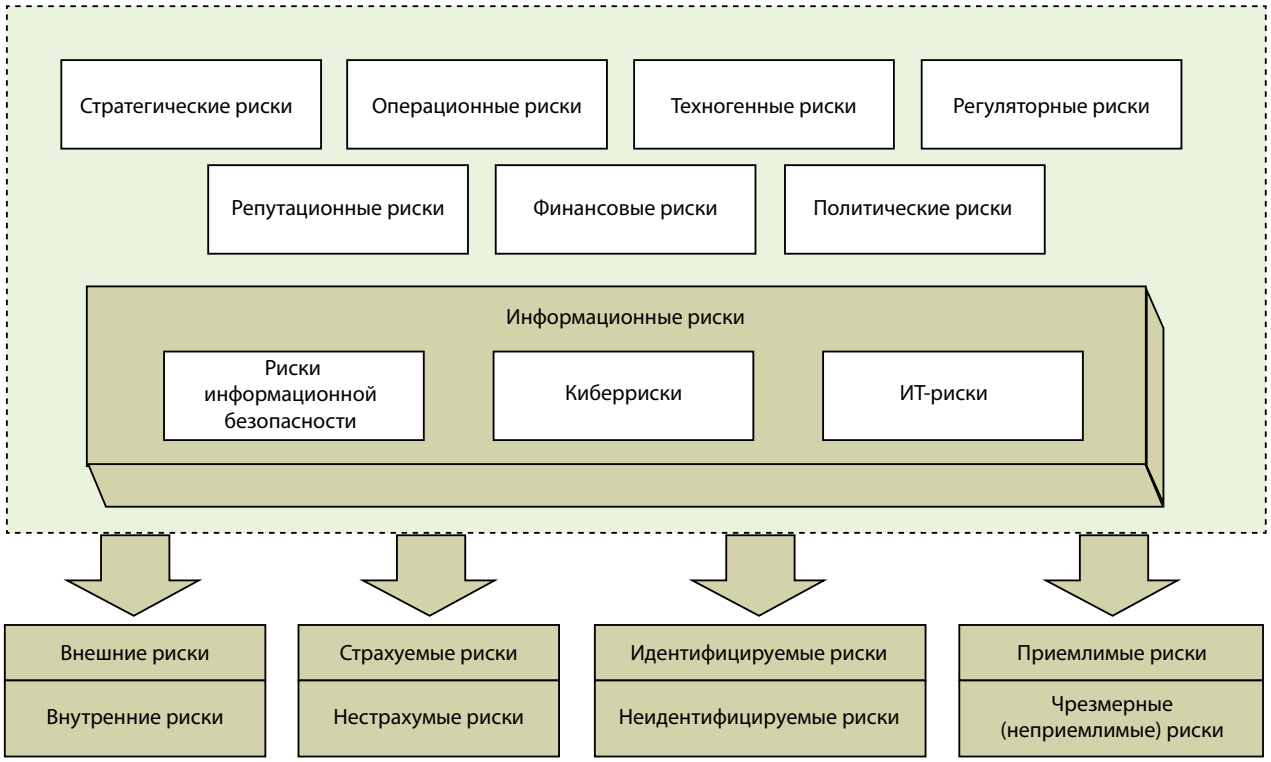


Рис. 2. Роль директора по информационной безопасности в системе риск-менеджмента

Инфориски и виды страхования

В контексте нашего обсуждения под понятием «информационные риски» (инфориски) мы подразумеваем риски информационной безопасности, киберриски и ИТ-риски компаний (рис. 1). Однако информационные риски можно понимать и шире, включая в их состав риски интеллектуальной собственности, диффамацию, дискредитацию, политические риски и т. д.

Одним из инструментов управления инфорисками является страхование. Соответствующие программы обеспечивают компаниям страховую защиту возможных убытков при возникновении инцидентов в области информационной безопасности, при интеграции бизнес-процессов организации и Интернета вещей. Страхование должно быть частью системы риск-менеджмента, в решении задач которого должен участвовать директор по ИБ организации (рис. 2). Если такой должности в компании нет, это может быть сотрудник, курирующий вопросы информационной безопасности.

В комплексную программу страхования помимо инфорисков могут быть включены следующие виды страхования:

• страхование электронного оборудования (Electronic Equipment Insurance);
• страхование ответственности директоров (Directors and Officers Liability);
• страхование от преступлений, совершенных служащими (Infidelity of Employees Insurance).

Для финансовых организаций (банков) дополнительно возможны:

• комплексное банковское страхование (Bankers Blanket Bond);
• страхование от компьютерных преступлений (Bank Computer Crime Insurance);
• страхование от мошенничества с кредитными карточками (Crime Card Insurance).

Управление инфорисками при страховании

Основой любой программы страхования является андеррайтинг (underwriting), то есть «подписание под чем-либо», под какими-то условиями, принятие решения. Андеррайтинг — это процесс отбора и классификации степеней рисков с точки зрения возможности принятия их на страхование (или принятие страховой ответственности за убытки с позиции страховщика).

«Упрощенный» вариант управления рисками с точки зрения компании как потенциального страхователя показан на рис. 3 (страхователь оценивает, снижает риски и поддерживает их на приемлемом уровне). Дополнительно для детальной оценки инфорисков предприятиями могут быть использованы метрики PCR-риска (perceived composite risk).

Программа страхования инфорисков, или страхования киберответственности, может состоять из следующих элементов:

• ответственность компании за утечку данных (Privacy Liability). В данном случае под ними подразумеваются персональные данные и данные, которые имеют материальную ценность для организации (в том числе «ноу-хау»), торговые секреты, конфиденциальная и приравненная к конфиденциальной информация;
• расходы по реагированию компании на ситуации, связанные с нарушением безопасности корпоративной сети и процессов организации, с восстановлением их работоспособности и непрерывности (Network Security);
• расходы на Интернет-активность и работу с социальными группами (Media Liability);
• расходы, связанные с кибервымогательством (Cyber Extortion);
• расходы на расследование ИБ-инцидента при возникновении его признаков и наступлении страхового события (Forensic Investigation);
• убытки от перерыва в деятельности (сбоя в работе корпоративной сети и процессов) предприятия (Business Interruption);
• расходы на уведомление об утечке информации (Notification Costs);
• расходы на работу со СМИ (Crisis Management/PR Expenses);
• расходы на восстановление данных (Data Restoration);
• расходы на кредитный мониторинг (Credit Monitoring Costs);
• расходы на покрытие штрафов и неустоек (Regulatory Action, или Fines Costs).

Этапы принятия решения страхователем

С точки зрения страхователя (компании-клиента) процесс принятия решения по страхованию инфорисков состоит из шести этапов (рис. 4):

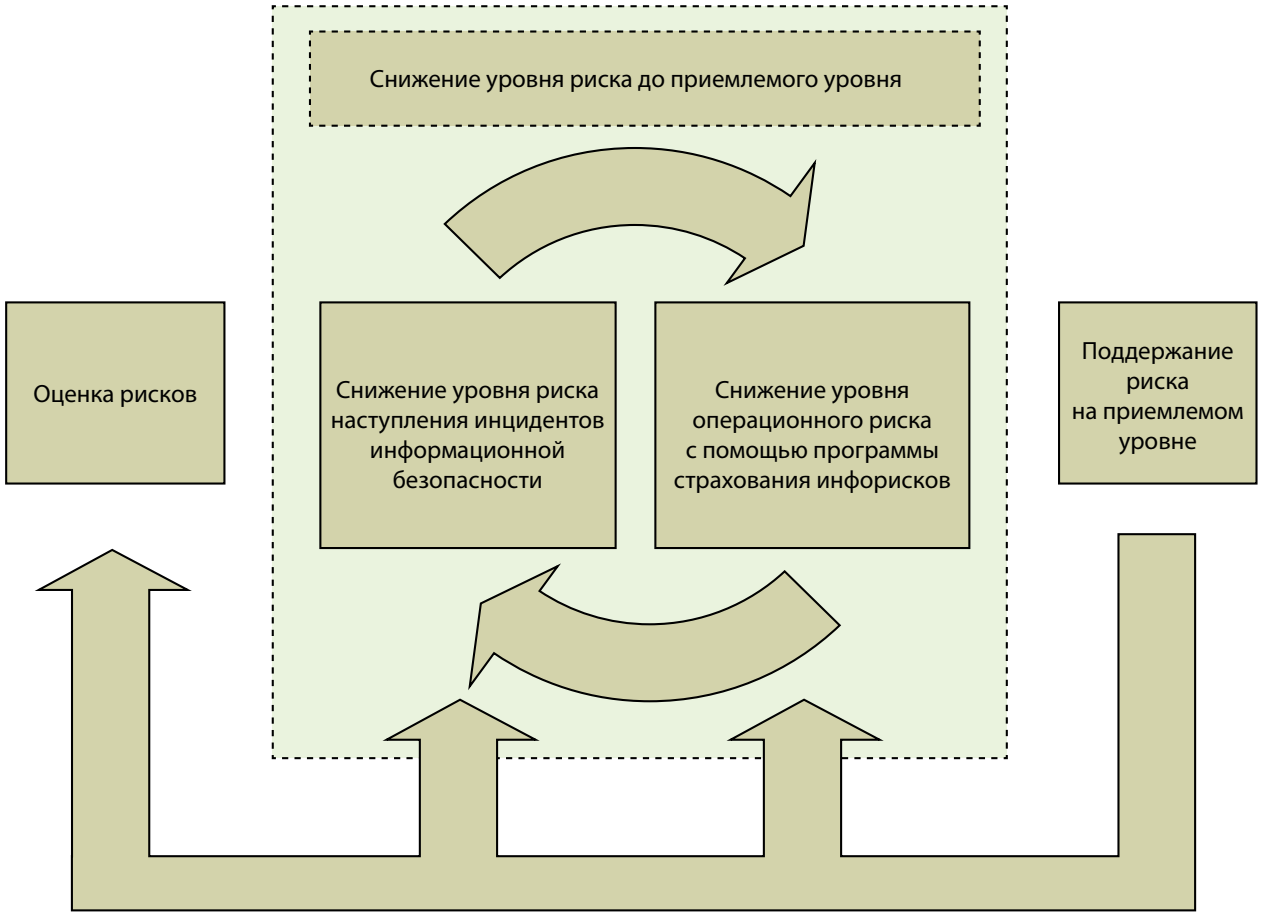


Рис. 3. Управление рисками в целях обеспечения информационной безопасности

Рис. 4. Процесс принятия решения по страхованию инфорисков

1) проведение аудита инфорисков;
2) оценка текущей программы страхования (при ее наличии);
3) заполнение опросного листа (заявления на страхование);
4) рассмотрение и оценка возможностей страхования, в том числе оценка предложений от страховых брокеров;
5) выбор программы страхования;
6) сопровождение программы страхования, мониторинг информационной безопасности.

Предприятиям рекомендовано проходить все стадии последовательно. Для предварительной оценки стоимости программы страхования необходимо лишь заполнить опросный лист.

Как советуют консультанты по страхованию инфорисков, при выборе страховщика и программы страхования предприятиям необходимо обращать внимание на следующее:

- размер страховой суммы в договоре страхования, включая размер сублимитов по отдельным страховым рискам;
- методика оценки максимальной стоимости возможного ущерба при наступлении событий, потенциально относимых к ИБ-инцидентам;
- исключения из страхового покрытия договоров «классического» страхования;
- расширение страхового покрытия за счет включения дополнительной секции по страхованию инфорисков в договор страхования;
- исключения из страхового покрытия, в которых упоминаются «терроризм», «военные риски», «территории страхования»;
- юрисдикция, в рамках которой будет действовать договор страхования;
- процедура урегулирования убытков, формирование доказательной базы по факту наступления страхового случая, методика расчета стоимости ущерба;
- собственное удержание страховщика и его партнеров по перестрахованию;
- возможность увеличения страховой суммы в период действия договора страхования;
- включение в страховое покрытие косвенных расходов при реализации киберугрозы;
- возможность проведения аудита по информационной безопасности в период действия договора страхования;
- условия предъявления требований к страховой выплате при перезаключении (или окончании) договора страхования.

Анализ российской практики заключения договоров страхования инфорисков позволяет констатировать, что уровень доверия предприятий к страховым компаниям, прозрачность деловой среды страхового рынка и степень готовности российских организаций к заключению договоров страхования киберответственности пока нельзя считать высокими. Однако стоит отметить появление страховых продуктов, которые ориентированы на потребности современного «цифрового» общества и появление активных участников страхового рынка в России.

Проблемные зоны развития страхования инфорисков могут заключаться в отсутствии следующих факторов:

- оценки политических рисков и рисков «кибертерроризма»;
- оценки инфорисков как катастрофических и системных;
- статистики по ИБ-инцидентам;
- модели количественной оценки утечек информации;
- контроля над состоянием застрахованного объекта, факторами развития рисков и выполнением мероприятий по снижению рисков;
- опыта страхования у андеррайтеров российских страховщиков;
- пула перестраховщиков на локальном рынке России;
- взаимосвязей между участниками страхового рынка и готовой инфраструктуры для страхования инфорисков;
- определения таких понятий, как «инцидент информационной безопасности», «кибервойна» на законодательном уровне;
- адекватных штрафов за несоблюдение законодательства о персональных данных.

Журнал «!Безопасность Деловой Информации»

Авторы

Виталий Лютиков, начальник 2-го управления ФСТЭК
Андрей Духвалов, руководитель Управления перспективных технологий «Лаборатории Касперского».
Наталья Касперская, генеральный директор InfoWatch
Артем Сычев, заместитель начальника ГУБиЗИ Банка России
Василий Окулесский, начальник Управления ИБ Банка Москвы
Рустем Хайретдинов, глава Appercut Security, президент ассоциации BISA
Сергей Вихорев, заместитель по развитию генерального директора «ЭЛВИС-ПЛЮС»
Михаил Емельянников, управляющий партнер консалтингового агентства «Емельянников, Попова и партнеры»
Игорь Душа, специалист по информационной безопасности НИЯУ МИФИ
Дмитрий Даренский, руководитель направления АСУ компании «Информзащита»
Игорь Решетников, заместитель начальника САИТиС ООО «Газпром центрремонт»
Даниил Тамеев, руководитель направления по работе с ПиТЭК Центра информационной безопасности компании «Инфосистемы Джет»
Антон Шипулин, руководитель проектов по информационной безопасности компании КРОК, автор блога «Безопасность АСУ ТП»
Виталий Малкин, старший консультант PwC
Александр Большев, директор департамента безопасности АСУ ТП Digital Security
Алексей Тюрин, директор департамента аудита защищенности Digital Security
Михаил Савельев, директор Учебного центра «Информзащита»
Алексей Лукацкий, бизнес-консультант по безопасности Cisco Systems
Юрий Малинин, ректор «Академии Информационных Систем»
Игорь Елисеев, эксперт-аналитик «Академии Информационных Систем»
Алексей Волков, начальник отдела ИБ компании «Северсталь»
Юрий Ипатов, руководитель департамента информационных технологий компании «Трансмашхолдинг»
Андрей Власов, аспирант Финансового университета

Информация

Номер журнала: № 9, I квартал 2015 г.
Тираж: 1000 экз.
Распространяется бесплатно
Номер свидетельства: ПИ № ФС 77 – 54908
Свидетельство о регистрации СМИ: ПИ № ФС 77 – 54908
Зарегистрировавший орган: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
Главный редактор: Олег Седов
Ответственный редактор: Наталья Мутель
Литературный редактор: Наталья Соболева
Верстка: Илья Залыгин
Дизайнер: Дарья Кирше
Адрес редакции: 123022, Москва, 2-я Звенигородская ул., д. 13, стр. 41
Дизайн и печать – типография «ЮСМА»: 109316, Москва, Волгоградский пр-т, д. 42, корп. 5
Интернет-версия издания: http://bis-expert.ru/bdi

Контакты по вопросам рекламы и размещения материалов

E-mail: pr@bis-expert.ru, тел.: 8-903-724-33-10
Рукописи не возвращаются и не рецензируются.

Наши выпуски

Журнал о трендах, знаниях и личномопыта
в области защиты информационных активов

Приглашаем к сотрудничеству!

По вопросам размещения статей и рекламных материалов
просим обращаться к ответственному редактору издания Наталье Мутель
тел: **8 909 724–33–10** email: **pr@bis–expert.ru**

INFOWATCH TRAFFIC MONITOR

А ВЫ УВЕРЕНЫ, ЧТО ВАШИ СОТРУДНИКИ НЕ ВЕДУТ ДВОЙНУЮ ИГРУ?

Поможем выявить злоумышленников,
сговоры, нелояльных сотрудников,
лиц, занимающихся промышленным шпионажем

INFOWATCH®

+7 (495) 22-900-22

sales@infowatch.ru

www.infowatch.ru