Kaspersky ICS CERT

kaspersky

Цифровые двойники и обеспечение кибербезопасности предприятий. Нефтегазовая отрасль

Александр Николаев

20.10.2022 Version 1.0

Необходимость модернизации 2
Внедрение ИТ и цифровизация 2
Цифровые двойники 4
Угрозы, связанные с цифровизацией предприятий 5
Обеспечение безопасности цифрового двойника. Кибериммунитет 8
Модели зрелости 9
Профиль зрелости 11
Заключение 12

Особенность нефтегазовой отрасли заключается в огромном разнообразии установок и технологических процессов. Предприятия и объекты отрасли в ходе жизненного цикла из-за адаптаций, ремонтов, модернизаций превращаются в уникальные, не схожие с другими. Например, установки первичной переработки нефти или гидроочистки, выполненные по одному первоначальному проекту и установленные на разных НПЗ в одно время, через несколько десятилетий по итогам эксплуатации будут серьезно отличаться друг от друга. То же самое можно сказать про оборудование, эксплуатируемое на скважинах. Даже с учетом того, что может использоваться один и тот же метод добычи, есть много факторов, влияющих на развитие систем. К таким факторам относятся территориальное расположение скважин, качество нефти и состав нефтепродуктов, характеристики пластов, дебит и т.д. Как результат, эти различия объектов приводят к разнице в организации процессов производства. Эта разница, соответственно, влияет на поддерживающее оборудование, используемое ПО, процессы ИТ и обеспечения кибербезопасности. Развитие экономической ситуации и конкурентное давление часто требуют дальнейшей модернизации предприятий и объектов, в том числе в области кибербезопасности. При этом модернизация не должна быть сверхсложной и дорогой, и должна проходить по максимально унифицированным, типовым проектам, где это возможно.

Необходимость модернизации

Месторождения, которые давно разрабатываются и где пройден пик добычи, а также НПЗ и отдельные их установки, введенные в эксплуатацию 30 и более лет назад, модернизируются компаниями крайне неохотно. Техническая сложность модернизации, большие денежные и временные инвестиции, потеря финансов из-за простоев в ходе работ — это вложения, которые окупаются десятилетиями. Вложения могут и не окупиться, к примеру, из-за излишнего обводнения нефтяного пласта, и, в результате низких количественных и качественных показаний добычи чистой нефти и т.п.

Если все-таки модернизация проводится, то требуются новые технологии. Исследования в области развития технологий в нашей стране в последние 30 лет были остановлены: предприятия отрасли пользовались советским наследием, минимально вкладываясь в то, что есть. Это в итоге привело к зависимости от импорта. Зависимость сильна и для технологических процессов и систем, например, в разработке трудноизвлекаемых углеводородов и горизонтальном бурении, и для цифровых технологий — электронного, компьютерного оборудования, ПО.

Санкции последних лет против России, а также большая волатильность рубля и высокая стоимость нефти удорожают эксплуатацию существующих систем и развитие новых.

В итоге новые технологии внедряются, но в незначительном объеме.

Вышесказанное приводит нас к следующим тезисам:

1. Историческая и текущая ситуация на мировой арене отбросили российские компании по сравнению с мировыми лидерами в части технологической зрелости далеко назад, разрыв нужно сокращать.
2. Сложность и невозможность изменения технологического процесса и замены основного полевого оборудования на более современное в ряде случаев можно компенсировать, модернизировав процессы управления и внедрив для этого новые информационные технологии, — это поможет снизить операционные издержки, уменьшить время простоя, тем самым повысив экономическую эффективность предприятия.

Внедрение ИТ и цифровизация

Про необходимость активного внедрения ИТ для модернизации предприятий и объектов говорят нефтяные компании и Минэнерго России. По оценке

государственного ведомства, внедрение ИТ в нефтегазовой отрасли может приносить государству до 700 млрд руб. в год.

СИБУР на «Томскнефтехиме» (дочернее предприятие) в 2020 году первым в России внедрил систему цифрового моделирования нефтехимического процесса. Цифровая модель реактора полиэтилена высокого давления позволила с высокой точностью моделировать физико-химические процессы, что в свою очередь позволило оптимизировать операционные издержки, в частности, при производстве полиэтилена высокого давления. По оценкам компании, прогнозная оценка ожидаемой экономии в масштабах предприятия составляет 50-60 млн. руб. в год.

При этом стоит отметить, что СИБУР стал одной из первых компаний в мире, кто на базе собственного R&D подразделения провел эту работу на практике.

Однако построить интегрированную модель какой-либо установки в современном производстве — это хорошо, но мало. Она статична. Такая технология дает возможность различных моделирований и расчетов, экономии ресурсов, однако для современного производства этого недостаточно. Для оперативной и более качественной работы нужна «живая» и динамическая модель АСУ ТП \ всей установки\ цеха или даже всего производства. Данные вопросы помогают решать технологии цифровых двойников.

Несмотря на возможные угрозы и риски, использование передовых информационных технологий уже сейчас помогает добиваться целей, специфичных для производственных систем.

Так ПАО «Газпром нефть» в 2018 году взяло глобальный курс на цифровизацию всего своего производства. По информации компании, цифровая трансформация бизнеса — приоритетное направление деятельности для них. С помощью цифровых технологий и цифровых двойников в компании успешно решаются задачи по тестированию гипотез разработки месторождений, строительства и модернизации инфраструктуры, эксплуатации промыслов без рисков для людей и объектов. Для достижения целей этих задач в компании создаются цифровые двойники скважин, заводов, производственных площадок и месторождений.

По словам Дмитрия Шварца — руководителя направления отдела исследований и разработки центра цифровых инноваций ПАО «Газпром нефть» — в компании создается инфраструктура для работы цифровых двойников. При этом ПАО «Газпром нефть» одна из немногих компаний в

нефтегазовой отрасли, которая занимается решением вопросов информационной и кибербезопасности своей цифровой инфраструктуры.

Цифровые двойники

Цифровой двойник это виртуальная копия какого-либо объекта — системы (например, система гидроочистки дизельного топлива), установки (например, ЭЛОУ-АВТ), цеха (например, цех добычи нефти и газа), месторождения, НПЗ, — которая достоверно воспроизводит все происходящие на оригинальном объекте процессы в режиме реального времени, так что в каждый момент времени параметры состояния цифрового двойника соответствуют параметрам состояния физического объекта.

В такой системе все данные превращаются в цифровые продукты и начинают помогать выбирать и рассчитывать оптимальные режимы работы, прогнозировать показатели, проводить различные эксперименты с минимальными рисками для дорогостоящих физических активов компании и людей.

Цифровые двойники могут быть очень разными в зависимости от целей, которые компания хочет достичь. Уровень сложности цифрового двойника в каждом конкретном случае определяется индивидуально и зависит от уровня детализации, типа визуализации, выполняемого функционала и глубины аналитики.

Внедрение цифровых двойников дает дополнительные возможности оптимизации и процессов управления производственными активами предприятия, и процессов обеспечения его кибербезопасности.

Как известно, основной упор в обеспечении кибербезопасности предприятий нефтегазовой промышленности делается на операционные задачи — управление уязвимостями, мониторинг и обнаружение атак, реагирование на инциденты, восстановление нормальной работы систем после вызванных инцидентами сбоев. Все эти процессы могут быть оптимизированы с применением возможностей цифрового двойника.

Так, определенным образом спроектированный цифровой двойник поможет помочь определить оборудование, подлежащее обновлению в первую очередь, оценить возможные риски и последствия, связанные с обновлением, — с тем, чтобы правильно запланировать обновления реальных систем, минимизировать время простоя оборудования и время проведения работ.

Мониторинг безопасности, обнаружение и расследование инцидентов также могут быть оптимизированы с использованием цифровых двойников — например, для проведения тренингов персонала и киберучений, для анализа возможных последствий выявленной атаки и оценки возможного ущерба, в том числе, и прямо в ходе расследования на реальном объекте, пользуясь информацией об обнаруженных деталях атаки.

Цифровые двойники являются важным драйвером развития технологических предприятий. Но не стоит забывать о том, что, как и любые новые информационные технологии, цифровые двойники сами несут и новые угрозы информационной и кибербезопасности для предприятия. Боязнь новых кибератак и утечек данных — достаточно сильный сдерживающий фактор для руководства предприятий, который тормозит цифровизацию производства.

Угрозы, связанные с цифровизацией предприятий

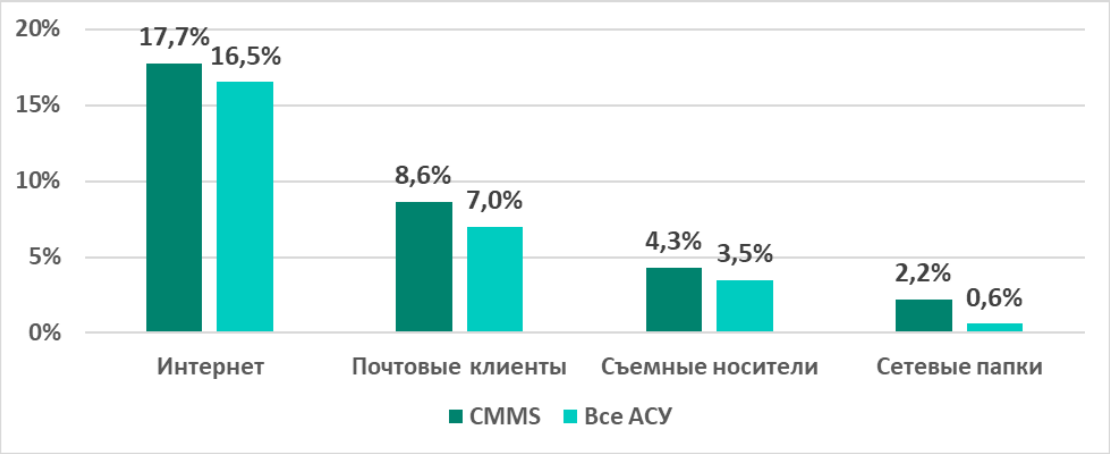
Новые передовые технологии всегда тянут за собой новые уязвимости, угрозы и риски, которые необходимо будет купировать «на горячую». Цифровизация с использованием технологий, проверенных временем и практикой эксплуатации, дарит шанс на более безопасное их внедрение с учетом полученного ранее опыта. даже если этот опыт отрицательный или нерелевантный — в таком случае получаем возможность исправить ситуацию.

Боязнь новых технологий не напрасна. Так, наши исследования ландшафта угроз систем АСУ показывают, что внедрение новых типов систем увеличивает поверхность атаки предприятия. Особенно это актуально для

систем, требующих одновременно и связи с интернетом, и доступа к системам АСУ.

Для примера взглянем на статистику по компьютеризированным системам управления техническим обслуживанием (CMMS, Computerized Maintenance Management System). Согласно нашему исследованию, в первом полугодии 2022 года 38,2% таких систем были атакованы, как минимум, один раз.

Процент CMMS, на которых были заблокированы угрозы из разных источников, получился следующим:



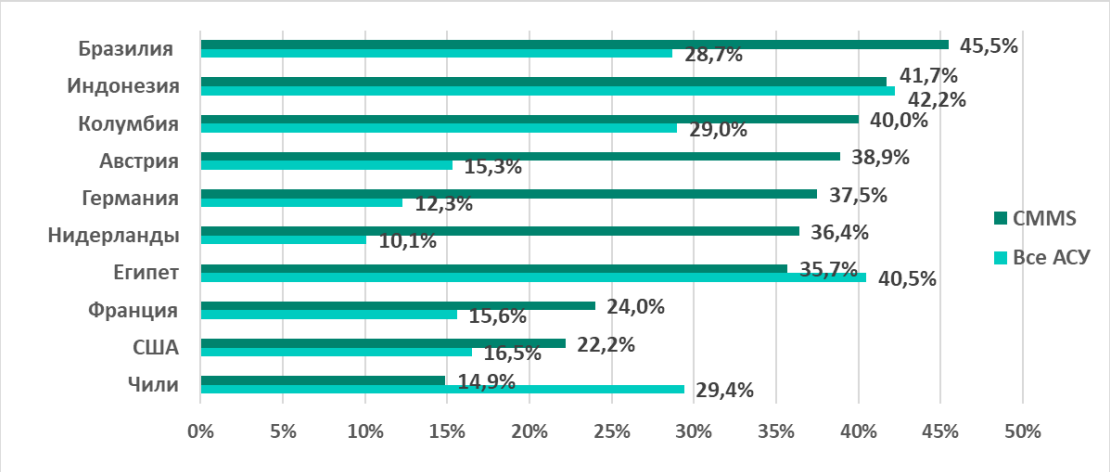
Как видно на графике выше, основная часть атак связана с доступом к интернет-ресурсам, на втором месте — атаки посредством электронной почты (фишинг), на третьем месте — использование съемных носителей (usb-flash, внешние жесткие диски и т.п.).

В рейтинге заблокированных угроз на первых местах — шпионское ПО и фишинг (фишинговые страницы и вредоносные документы из фишинговых писем), целью которого чаще всего является также установка шпионского ПО. Далее следуют банкеры, вымогатели и самораспространяющееся вредоносное ПО (черви и вирусы):

Как и для других типов IT- и OT-систем, большинство заблокированных угроз имеют случайный характер. Их успех объясняется, в основном, низкой осведомлённостью сотрудников и подрядчиков в вопросах кибербезопасности. Второй важный фактор — ошибки и недоработки IT-, OT- и ИБ-специалистов, в чьи обязанности входит обеспечение безопасности систем предприятия. Речь идёт о недостатках топологии и архитектуры сетей и конфигурации сетевых устройств; неустранённых уязвимостях в прошивках, ОС и ППО; небезопасно настроенных, оставленных без присмотра и неучтённых средствах удалённого доступа; недостаточном контроле соблюдения политик ИБ в отношении использования переносных и мобильных устройств и внешних носителей информации; отсутствии или плохих настройках средств защиты.

Неаккуратные и непрофессиональные действия сотрудников создают предпосылки и для попадания в технологическую сеть предприятия большинства случайных угроз, и для успешной реализации целевых атак.

Показательно, что в топ 10 стран по проценту CMMS, атакованных в первом полугодии 2022 года, вошли традиционно «благополучные» страны, не попадающие в топ по общим показателям процента атакованных компьютеров АСУ в стране:



Таким образом, мы видим, что использование новых «продвинутых» технологий, типа CMMS на промышленных предприятиях может заметно увеличивать поверхность атаки и соответствующие киберриски.

Обеспечение безопасности цифрового двойника. Кибериммунитет

Поскольку работа цифрового двойника требует «живых» данных из технологической сети, при внедрении цифровых двойников приоритетной задачей является обеспечение безопасной работы не столько самого цифрового двойника, сколько непосредственно объекта, который этот двойник моделирует. Ключевое значение приобретает безопасность технического решения для организации, развёртывания и подключения цифрового двойника.

Такие решения должны обладать «врожденной» защищенностью — кибериммунитетом. Кибериммунитет обеспечивается разделением IT-системы на изолированные части и контролем взаимодействий между ними таким образом, чтобы не дать злоумышленнику развить атаку в направлениях, несовместимых с целями безопасности системы даже при компрометации её отдельных компонентов.

В частности, шлюз, обеспечивающий получение данных из сети АСУ ТП для передачи их в системы, имеющие связь с интернетом (например, компоненты цифрового двойника), должен надёжно разграничивать промышленную и корпоративную среду, не допуская распространения атаки на оборудование АСУ ТП. Поэтому такой шлюз должен обладать соответствующим свойством киберимунности: при любой компрометации его компонентов, доступных из внешней сети (например, при эксплуатации уязвимости в сетевом стеке или драйвере сетевого интерфейса), злоумышленник не сможет получить доступ к сетевому интерфейсу, подключённому к защищённой технологической сети. Обладающий таким свойством киберимунности шлюз может быть построен на основе ОС, предоставляющей гарантии разделения доменов безопасности («безопасной ОС»). Экземпляры драйверов, сетевые стеки, файловые системы и ПО прикладного уровня будут для разных сетевых интерфейсов разнесены по разным доменам безопасности. В качества примера подобного решения можно рассмотреть Kaspersky IoT Secure Gateway.

Для обеспечения безопасности цифрового двойника могут потребоваться дополнительные меры и средства защиты. Например, расположение цифрового двойника в отдельном изолированном от корпоративной сети передачи данных сегменте сети, использование классических средств обеспечения безопасности (таких как антивирусное ПО) и специализированных средств — например, средств защиты сред виртуализации — и прочие средства защиты. Конкретный перечень мер и средств защиты для каждого случая будет свой.

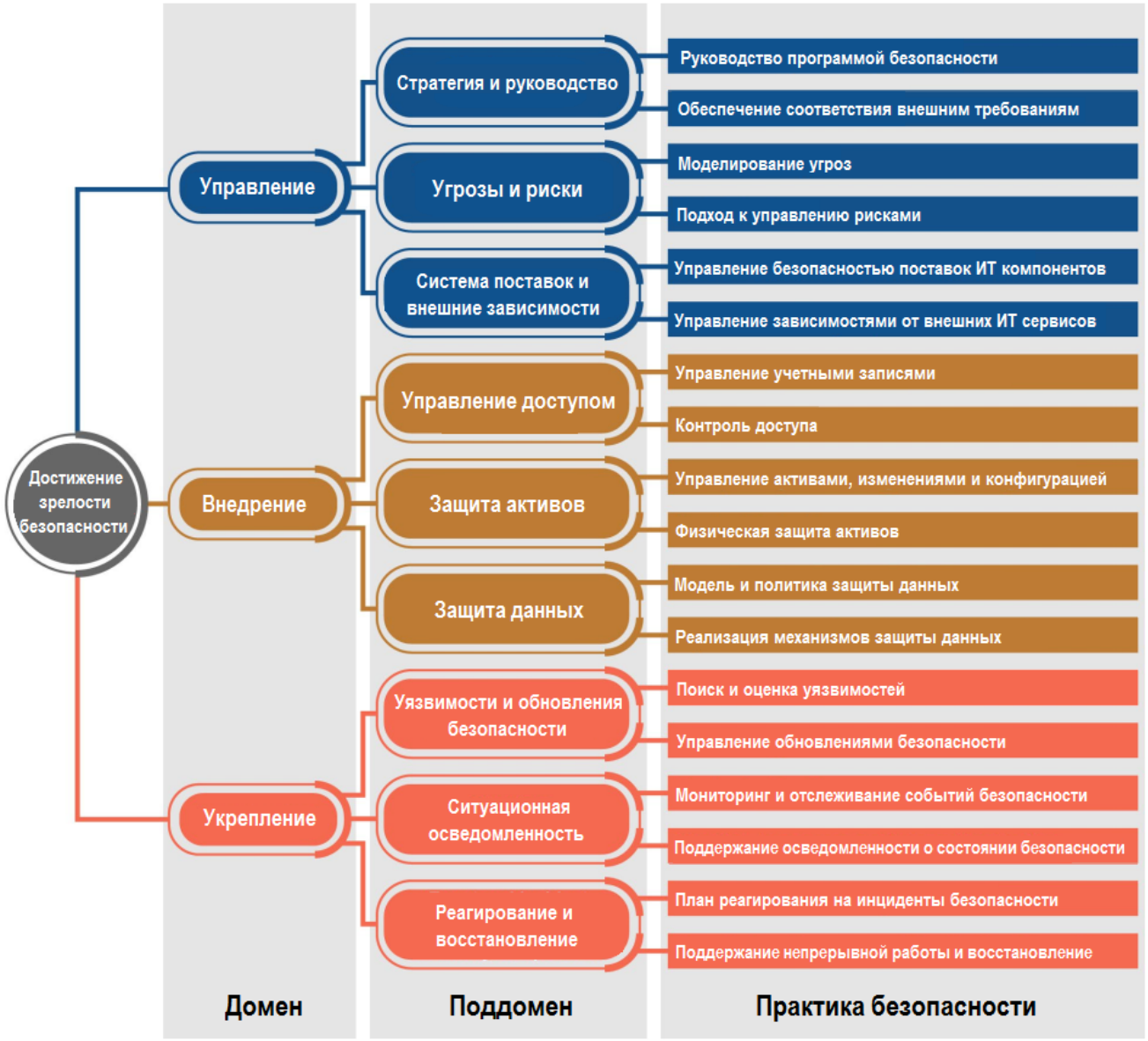
Модель зрелости IoT и разработанный на ее основе профиль зрелости безопасности предоставляют инструмент для формирования требований информационной и кибербезопасности, а также помогут определить уровень «достаточной безопасности» для каждого случая.

Модели зрелости

Для расстановки приоритетов при планировании и организации процессов обеспечения кибербезопасности и для оценки качества реализации всех запланированных в их рамках мер хорошо помогают практики модели зрелости безопасности интернета вещей.

Цель модели зрелости безопасности интернета вещей (IIC IoT Security Maturity Model, IoT SMM) — обеспечить выбор способов защиты от киберугроз, которые соответствуют реальным бизнес-потребностям организации. Модель зрелости безопасности интернета вещей равным образом может применяться к более или менее технологически сложным устройствам, компонентам IoT устройств и инфраструктур, и к самим инфраструктурам.

Архитектурой выбора и ядром модели зрелости безопасности интернета вещей является иерархия практик обеспечения безопасности:



В терминах модели зрелости безопасности интернета вещей (IIC IoT SMM), а также модели зрелости цифровых двойников (IIC Digital Twin Consortium IoT SMM), речь идет о практиках домена «Укрепление безопасности». Реализация этих практик на предприятиях нефтегазовой промышленности может требовать различных затрат в зависимости от того, к какой категории это предприятие относится. Внедрение обновлений безопасности для предприятий отрасли может занимать значительное время, особенно на устаревшем оборудовании и устаревших IT\OT-продуктах, а также с учетом передачи ответственности (инженеры АСУ ТП и инженеры по ИБ) — эти процедуры могут затягиваться до бесконечности.

Уровень зрелости цифрового двойника должен коррелировать с назначением, физическими ограничениями и спецификой работы

предприятия, и уровнем зрелости моделируемой системы. Не во всех случаях имеет смысл строить дорогостоящий цифровой двойник всего добывающего предприятия. Например, уровень зрелости системы (АСУ, установки и т.п.) в целом может быть низок для подобных работ или до определенного куста может быть проще добраться физически на автомобиле, или установка может не являться значимым и\или критически важным объектом (например, ДНС с куста, дающие слабые показатели по добыче нефтепродукта). В таких случаях имеет смысл рассматривать проектирование функций цифровых двойников выборочно, то есть только необходимых и достаточных функций.

То же и с определением уровня информационной и кибербезопасности. Необходимо явно определить уровень «достаточной безопасности». Этот уровень будет различаться на каждом объекте и зависеть от многих факторов. Для достижения достаточного уровня безопасности нельзя жертвовать производительностью объекта, а также необходимо соотносить затраты на сервисы информационной безопасности и полученную выгоду от их будущего применения.

Использование модели зрелости позволяет оптимизировать постановку задачи безопасности интернета вещей, то есть определить уровень «достаточной безопасности», провести оценку и планирование объема работ, которые необходимо провести для её достижения с требуемой детализацией, начиная с уровня доменов безопасности вплоть до отдельных практик.

Профиль зрелости

«Профиль зрелости безопасности интернета вещей для цифровых двойников», является отраслевым расширением документа «Модели зрелости безопасности IoT: руководство для практиков».

Профиль определяет специфичные для цифровых двойников параметры зрелости. Например, для практики «управление обновлениями» (patch management) минимальный уровень зрелости не определяет необходимости соотношения между обновлением безопасности и активом (оборудованием) в представлении цифрового двойника. Для второго и третьего уровня такое соотношение уже определено, а четвертый, самый высокий уровень зрелости, требует общего представления, согласования и координации устанавливаемых обновлений между цифровым двойником и физическим производством. Т.е. использование технологии цифровых двойников в целях повышения кибербезопасности становится актуальным

для предприятий, начиная уже со второго уровня зрелости, то есть подходит для большинства технологических предприятий.

Профиль зрелости безопасности IoT для цифровых двойников, таким образом, может применяться для согласования требований к процессам обеспечения кибербезопасности при проектировании сервисов, например, на MES уровне. При этом территориальная распределённость, физическая защищенность, технологические особенности производства могут быть учтены для будущей оптимизации этих процессов. Также необходимо отметить, что для разных типов предприятий (разведка и добыча, переработка и реализация, транспортировка и логистика) требования к зрелости процессов будут различаться.

Заключение

В современном технологичном производстве для поддержания конкурентоспособности, снижения затрат на поддержание имеющейся инфраструктуры и увеличения чистой прибыли не обойтись без внедрения ИТ и масштабной цифровизации и, следовательно, без внедрения новых технологий в сфере кибербезопасности.

Примером технологий, которые дают существенное преимущество, могут быть цифровые двойники. Примером необходимых для их интеграции новых технологий ИБ могут стать киберимунные системы на основе безопасных ОС, в частности, коммуникационное оборудование, дающее необходимые гарантии безопасности.

Выбор достаточных мер и средств защиты может упростить использование методологии SMM (Security Maturity Model). Эта методология принятия решений по обеспечению безопасности систем промышленного интернета вещей развивается высокими темпами, следуя за развитием ИТ. Так, в её рамках уже разработан фреймворк для построения профиля безопасности цифровых двойников.

В свою очередь, внедрение безопасных цифровых двойников может открывать в дальнейшем дополнительные возможности не только для решения задач оптимизации управления производственными активами предприятия, но и для решения задач информационной безопасности, в частности, задач управления уязвимостями программных и программно-аппаратных компонентов систем OT, что придаёт технологии дополнительную ценность для современных предприятий нефтегазовой отрасли.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com