Deloitte.

Интегрированный подход к управлению киберрисками

Обеспечение безопасности операционной деятельности в нефтегазовом секторе

2017

Предисловие

Данный отчет содержит результаты анализа, проведенного с использованием опыта работы на конкретных предприятиях, в том числе в ходе оказания нефтегазовым компаниям содействия в обеспечении безопасного функционирования систем управления производственными процессами.

Сегодня нефтегазовый сектор вступает на новый этап развития, которая подразумевает стремительную интеграцию роботизированных систем, цифровых инноваций и технологии Интернета вещей (IoT) в операционные процессы предприятий. На протяжении последних 10 лет интерес киберпреступников к промышленным операциям растет, что приводит к кибератакам, наносящим ущерб как производству, так и безопасности компаний. На фоне этих атак кибербезопасность стала предметом бурного обсуждения в корпоративных советах директоров по всему миру. В результате все больше организаций ведет разработку масштабных трансформационных программ с целью предотвращения новых операционных угроз.

Создание безопасных и гибких операционных процессов, а также подготовка к возможным угрозам — непростая задача, для выполнения которой нефтегазовые компании должны синхронизировать и скоординировать свои действия как в технической, так и в информационно-технологической сферах. К тому же операционная среда требует разработки специализированных технических решений, которые не всегда легко обеспечить.

Решение указанных проблем требует глубокого знания как технических дисциплин, так и информационных технологий, а также лучшей отраслевой практики в области управления киберрисками. Данный отчет содержит результаты анализа, проведенного с использованием опыта работы на конкретных предприятиях, в том числе в ходе оказания нефтегазовым компаниям содействия в обеспечении безопасного функционирования систем управления производственными процессами (ICS).

Мы надеемся, что этот отчет станет для вас полезным и информативным.

С уважением,

Пол Зонневельд
Руководитель Международной группы
по предоставлению консультационных услуг
в области управления рисками
предприятиям энергетики
и добывающей промышленности,
«Делойт» (Канада)

Введение

Основу безопасности и надежности функционирования наиболее важных объектов инфраструктуры составляют системы управления производственными процессами организации (ICS). Инженерно-технические специалисты успешно разрабатывают и внедряют ICS-системы с учетом требований безопасности труда и надежности, но не всегда — информационной безопасности. В чем же причина? Изначально потребность в обеспечении информационной безопасности таких систем была небольшой. Наибольшим спросом для управления производственными процессами пользовались изолированные, узкоспециализированные системы. Учитывая, что прежде такие системы не внедрялись в бизнес-процессы организаций и даже не были интегрированы между собой, риск возникновения масштабных каскадных аварий в случае виртуальных и иных атак рассматривался отдельно от прочих рисков организаций.

Всего 20 лет стремительного развития — и повсеместное распространение объединенных в сети IoT-устройств коренным образом изменило базовые представления об операционной безопасности. Сегодня все виды производственных активов, включая нефтяные месторождения, нефтепроводы и нефтеперерабатывающие предприятия, становятся уязвимыми для кибератак. В наше время операционные системы, вне зависимости от их локализации, подвержены внешним и внутренним рискам, которые могут привести к нарушениям безопасности или производственным сбоям и тем самым увеличить размер коммерческого риска. Несмотря на то что ICS-системы, как правило, призваны обеспечить безопасность в аварийных ситуациях, постоянное совершенствование методов, применяемых киберпреступниками, ведет к росту риска возникновения катастроф и масштаба их последствий, которые проявляются в виде затрат, нарушения безопасности, ущерба для репутации и коммерческих или финансовых потерь.

До сих пор нефтегазовому сектору удавалось избегать крупных производственных катастроф, однако если они не расширят свои программы по управлению рисками безопасности, это везение может вскоре закончиться.

В последнее время нефтегазовые компании, как и компании из других отраслей экономики работают над укреплением информационной безопасности, поскольку, по мнению высшего руководства и членов советов директоров, эта задача является одной из первоочередных.

До сих пор нефтегазовому сектору удавалось избегать крупных производственных катастроф. Но если они не расширят свои программы по управлению рисками безопасности, это везение может вскоре закончиться.

По сей день нефтегазовые компании в основном направляли свои усилия на защиту не производственных процессов, а бизнес-систем и данных. Это объясняется тем, что технология Интернета вещей, благодаря которой, например, можно управлять производством с помощью планшета или смартфона, — это относительно новая концепция, набирающая популярность на протяжении вот уже 10 лет. Кроме того, операционные системы имеют совсем иную специфику, а потому их защита требует не только знаний в сфере информационных технологий, но и особых инженерно-технических навыков.

Современный подход предполагает объединение информационных и инженерных технологий для обеспечения информационной безопасности за счет использования комплексных мер. Далее в отчете рассматриваются задачи, реализуемые в рамках указанного подхода, а также практические шаги для запуска процесса.

Для начала рассмотрим виды киберугроз, с которыми сталкиваются компании нефтегазового сектора, соответствующие угрозы для цепочки создания стоимости и возможные последствия.

Рис. 1. Влияние киберугроз на цепочку создания стоимости в нефтегазовом секторе

Киберугроза

Геологоразведка и добыча

Геологоразведка

- **Геофизическая оценка и моделирование**
- **Разработка месторождений**
- **Буровые работы**

Геологоразведка и добыча: сценарий 1

Незаконное присвоение служебной коммерческой информации о динамике эксплуатации пласта и скважин

Риски: утрата конкурентных преимуществ оператора на месторождении

Добыча

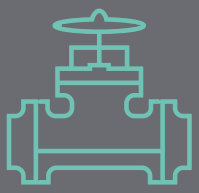
- **Извлечение нефти**

Геологоразведка и добыча: сценарий 2

Превышение стандартных эксплуатационных параметров или полная остановка работы ключевого оборудования, обеспечивающего управление работами в скважинах, и безопасность рабочих

Риски: риск остановки работ и возникновения финансовых потерь, а также инцидентов в сфере безопасности на месторождениях из-за неисправностей в работе оборудования

Транспортировка и хранение



Транспортировка

- **Сбор и транспортировка (трубопроводы, танкеры, грузовики)**

Транспортировка и хранение: сценарий 1

Несанкционированный доступ и управление системами трубопроводов

Риски: риск возникновения взрыва, утечки, нанесения ущерба окружающей среде и системам, а также создания опасных условий для персонала и населения близлежащих территорий

Транспортировка и хранение: сценарий 2

Нарушение или прерывание процесса мониторинга, создающее угрозу для бесперебойной работы оборудования

Риски: риск остановки функционирования системы, обеспечивающей проведение внутренних расследований, что может привести к сбоям при доставке продукции и финансовым потерям

Переработка и сбыт

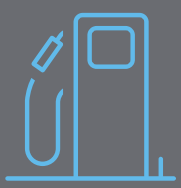
Переработка

- **Переработка сырой нефти для получения нефтепродуктов**
- **Смешение нефтепродуктов**

Переработка и сбыт: сценарий 1

Хищение данных о запасах сырой нефти и очищенных нефтепродуктов

Риски: риск несоблюдения деловых обязательств и утраты репутации



Сбыт

- **Розничные продажи**
- **Трейдинг**

Переработка и сбыт: сценарий 2

Нарушение/умышленное нарушение функционирования средств осуществления контроля за операционной деятельностью

Риски: риск несоблюдения условий эксплуатации и простоя оборудования, приводящий к сбоям в поставках и потере доходов

Понимание рисков

Одна из основных причин, затрудняющих обеспечение безопасности ICS-систем, заключается в том, что при их создании не предполагалась возможность их объединения в сети, однако сегодня происходит именно это. Дигитализация операционных процессов в нефтегазовом секторе привела к тому, что перед компаниями открываются новые возможности для повышения производительности и сокращения затрат. Однако слияние производственных и бизнес-процессов делает организации уязвимыми для широкого спектра новых киберрисков. Рассмотрим нижеследующие сценарии, которых несколько лет назад вовсе не существовало.

- Если организации пользуются незащищенным удаленным доступом для взаимодействия, это позволяет киберпреступникам получить контроль над системой, управляющей производственными процессами, и вызвать перегрузку производственного оборудования.
- Неэффективные методы обеспечения безопасности, применяемые сторонними контрагентами, позволяют вирусам проникнуть в производственную программную среду, что приводит к остановке работы ключевых систем SCADA (системы диспетчерского управления и сбора данных) и созданию небезопасных условий труда.
- Некорректное проведение тестирования информационных систем перед развертыванием приводит к их полному отказу и, как следствие, к сбоям или остановке производственных процессов.
- Если предприятие приобретает какие-либо технологические продукты без полноценного предварительного тестирования и оценки, то все имеющиеся в таком программном обеспечении ошибки остаются неисправленными, что делает предприятие уязвимым и позволяет враждебно настроенным лицам получить удаленный доступ к программируемым устройствам управления (PLC) и возможность умышленно дестабилизировать производственные процессы.

Приведенные примеры показывают, что существует множество источников киберугроз, в том числе в лице сотрудников компании, стремящихся организовать диверсию на производстве; конкурентов, желающих нанести ущерб бренду компании; а также третьих лиц (например, групп активистов, призывающих к остановке работ).

Не все уязвимости обуславливаются исключительно использованием технологий. Поведенческие аспекты также могут играть свою роль. Так, недостаточное понимание значения мер по обеспечению безопасности в рамках организации может подвергнуть корпоративные системы риску возникновения кибератак (например, это может случиться, если сотрудники используют собственные мобильные носители информации, зараженные вредоносными программами). Более того, многие производственные работники полагают, что используемые ими системы не представляют интереса для злоумышленников, а потому неохотно признают необходимость изменения привычного образа действий и внедрения новых протоколов безопасности. В конце концов, еще недавно можно было с уверенностью предполагать, что все элементы оборудования заслуживают полного доверия. Сегодня все изменилось. Ведь показания цифровых сенсоров и контроллеров можно сфальсифицировать с целью предоставления ложной информации о состоянии оборудования. Другая устаревшая аксиома гласит, что сбои в процессах в основном объясняются погодными условиями, человеческим фактором и износом оборудования и не обязательно вызваны злонамеренным вмешательством в работу систем со стороны лиц, желающих причинить ущерб компании.

Вне зависимости от того, произошла ли утечка данных по недосмотру самой компании или в результате атаки злоумышленников, ее последствия могут быть очень серьезными: от нарушения конфиденциальности данных до отказа или полной остановки работы систем. А это может повлечь за собой уменьшение объемов выручки, нанесение ущерба репутации компании, происхождение экологической катастрофы, принятие правовых мер или — в худшем случае — гибель людей.

Легко понять, почему внедрение комплексных, эффективных средств контроля информационной безопасности в ICS-системы организаций в наше время становится насущной необходимостью, если не сказать обязательным требованием. Вместе с тем для выполнения этой задачи компании должны найти способ принять во внимание противоположные точки зрения на информационные системы и операционные процессы, поскольку специалисты по управлению производственными процессами не всегда в полной мере понимают специфику текущих рисков информационной безопасности, а специалисты в области информационной безопасности часто не разбираются в производственных процессах, управляемых ICS-системами.

Анализ типа bowtie — популярная концепция, широко используемая в инженерно-технической области для оценки отказов оборудования — может стать полезным инструментом для преодоления этого непонимания. Любой анализ можно провести с учетом специфики организации. На рис. 2 мы приводим пример проведения анализа киберрисков по методу bowtie применительно к нефтегазовой компании.

Рис. 2. Пример проведения анализа киберрисков по методу bowtie применительно к нефтегазовой компании

Источник: адаптированные материалы книги Дж. Талбота и М. Джейкмана Security Risk Management Body of Knowledge (RMIA, Карлтон Саус, 2008 год)

Дигитализация операционных процессов в нефтегазовом секторе привела к появлению новых возможностей повышения производительности и снижения затрат. Но при этом слияние производственных процессов и бизнес-процессов создало для организаций целый ряд киберрисков, с которыми они не сталкивались прежде.

Проведение оценки зрелости

После получения полной картины рисков нефтегазовая компания должна провести оценку зрелости существующих средств обеспечения контроля за информационной безопасностью производственных процессов.
И пусть не все риски можно минимизировать, важно понимать, какие виды контрольных процедур существуют в организации и над чем еще необходимо работать.
Речь идет о необходимости уделять достаточное количество внимания анализу взаимосвязей между рисками, связанными со взломом ICS-систем, и бизнес-рисками в целом.
Важно отметить, что с этой задачей может самостоятельно справиться и технический отдел, и ИТ-подразделение и что ее реализация требует привлечения специалистов из самых разных областей деятельности (производственных специалистов, инженерно-технических специалистов, специалистов в области информационной безопасности), перед которыми будут ставиться нижеследующие цели.

Проведение инвентаризации активов и оборудования и оценка степени их важности для организации

Здесь могут возникнуть следующие вопросы: существуют ли какие-либо факторы, делающие тот или иной объект особенно привлекательной целью для злоумышленников? Применяются ли корпоративные стандарты информационной безопасности, механизмы управления и мониторинга ко всем ICS-активам организации? Был ли проведен анализ всей совокупности уязвимостей систем перед киберугрозами и были ли определены и тщательно оценены возможные последствия?

Определение наличия/отсутствия в работе ключевых активов и оборудования детально изученных уязвимостей, которыми можно воспользоваться

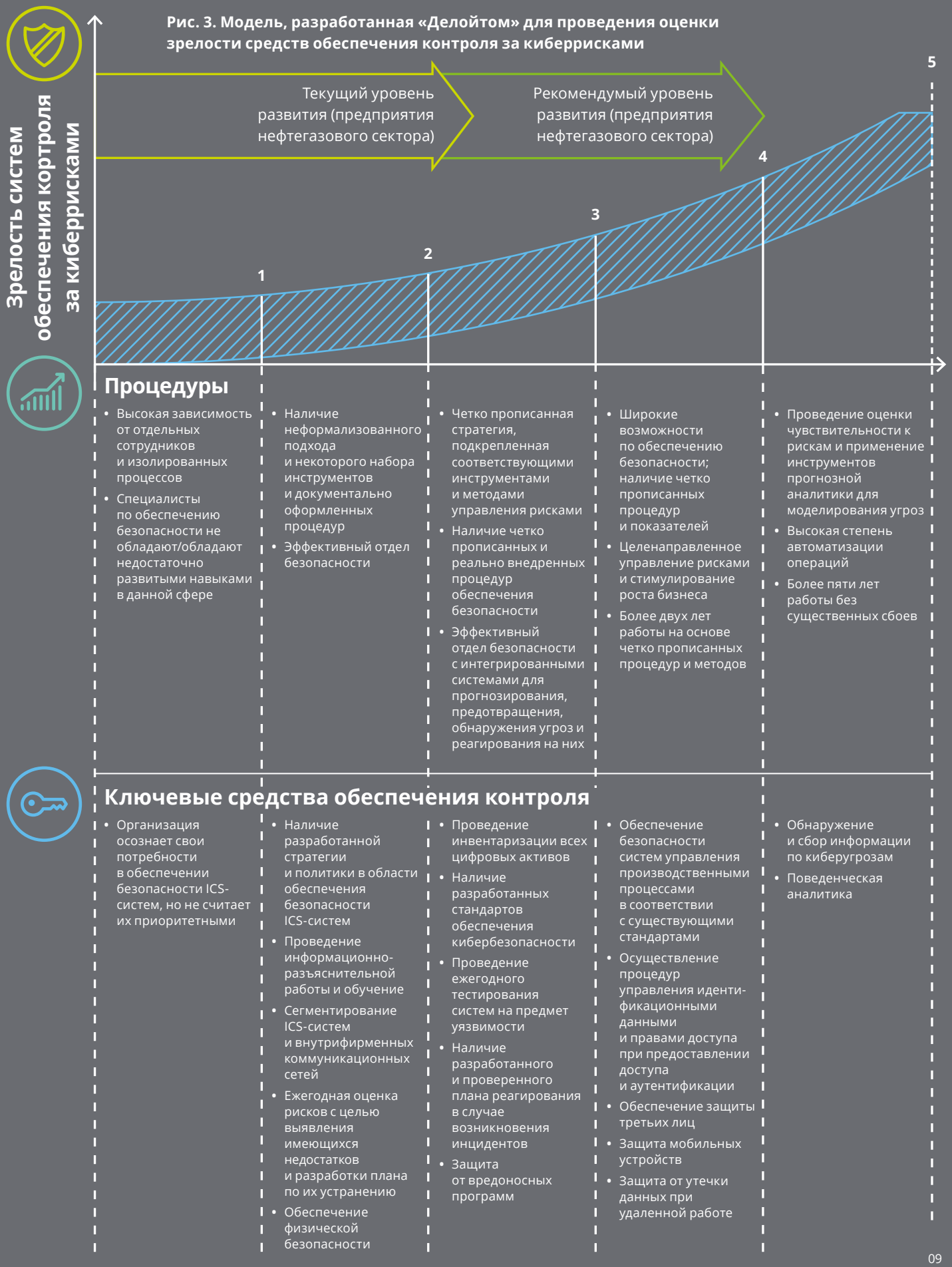
В нефтегазовом секторе такие уязвимости могут принимать различные формы в зависимости от внутриотраслевой специфики организации. К примеру, разведочные установки часто подвержены риску хищения корпоративных данных, таких как данные геофизических исследований, данные по добыче, статистические данные по скважинам, данные инженерных изысканий и данные по стратегическому планированию, то есть всех видов данных, утрата которых может грозить компании потерей конкурентных преимуществ.
С другой стороны, промышленные предприятия уязвимы перед угрозой злонамеренного вмешательства в работу их систем SCADA и прочих видов производственных систем, а также угрозой потери связи с отдаленными производственными площадками и остановки производственных процессов в результате проникновения в системы программных вирусов.
В данном случае последствия носят более осязаемый характер и проявляются в виде неблагоприятных условий работы и простоя оборудования, что, в свою очередь, может привести к финансовым потерям и человеческим жертвам. Сходным образом киберриски, характерные для транспортировки и хранения, также могут иметь как материальные, так и финансовые последствия (создание небезопасных рабочих условий, утечки и перебои в поставках или производстве продукции). Предприятия, работающие в сфере переработки и сбыта, также не застрахованы от манипуляций с системами управления производственными процессами и наступления таких же физических и финансовых последствий, с какими сталкиваются организации из других сегментов рынка.
Вместе с тем переработка и сбыт также подразумевают непосредственное взаимодействие с клиентами в рамках маркетинговых мероприятий, что создает возможность хищения клиентских данных и вмешательства в работу трейдинговых систем. Это может привести к потере доходов, нанесению ущерба репутации компании и нарушению нормативно-правовых требований.

Проведение оценки зрелости средств и методов обеспечения контроля с целью упреждающего управления указанными угрозами

При оценке уровня развития средств корпоративного управления и внутреннего контроля часто бывает полезно использовать уже готовую, отлаженную систему, например, такую, как разработанная «Делойтом» модель для проведения оценки зрелости средств обеспечения контроля за киберрисками, представленная на рис. 3. При проведении такой оценки для большого числа различных компаний, занятых в сфере энергетики и добывающей промышленности, мы заметили, что в соответствии с нашей шкалой оценки в целом по отрасли зрелость внутрикорпоративных средств обеспечения контроля за киберрисками достигает отметки 2,5, тогда как рекомендуемый уровень зрелости — более 4.

На всех этапах анализа важно проводить различие между фактами и обстоятельствами, использующимися при оценке бизнес-систем и систем управления производственными процессами. Сегодня, в эпоху масштабной интеграции, стандарты и процессы обеспечения информационной безопасности должны отвечать потребностям как систем управления производственными процессами организации, так и вспомогательных систем, причем без создания каких-либо помех для функционирования существующих процедур, обеспечивающих безопасность и надежность рабочих процессов. Помимо оценки зрелости, организации в рамках текущего мониторинга должны регулярно реализовывать определенные активы, причем не только те, в которых были выявлены факторы уязвимости, но и те, в отношении которых обнаружены потенциальные угрозы безопасности, постоянные угрозы повышенной сложности (advanced persisent threats — APT) или подозрительные действия, а также заблаговременно отслеживать дискредитированные активы до возникновения реальной угрозы безопасности.

Рис. 3. Модель, разработанная «Делойтом» для проведения оценки зрелости средств обеспечения контроля за киберрисками



Разработка единой программы

На протяжении более чем 50 лет задача обеспечения безопасности была основным стимулом для разработки и внедрения средств осуществления внутреннего контроля за физическими угрозами эффективности производственных процессов. И хотя этот стимул сохранился до сих пор и помогает поддерживать процессы в защищенном и рабочем состоянии, перечень потенциальных угроз пополнился киберугрозами. Поэтому сегодня систематический подход к обеспечению кибербезопасности требует разработки единой программы защиты бизнес-процессов и производственных процессов. Создание программы такого рода подразумевает многолетнюю работу, однако на каждом этапе трансформации необходимо преследовать одну и ту же цель, постепенно повышая уровень развития внутренних контрольных процедур для создания безопасной, готовой к работе и защищенной контрольной среды.

Защищенность

Обеспечивать безопасность системы значит устранять нарушения и предотвращать взломы путем внедрения эффективных автоматизированных средств контроля и мониторинга. Однако обеспечить одинаковый уровень защищенности всех систем — это очень сложная задача. Очевидно, что важные активы и объекты инфраструктуры, а также соответствующие ICS-системы являются наиболее приоритетными целями. Однако необходимо помнить, что они не представляют собой разрозненные и изолированные компоненты. Это лишь часть масштабных цепочек поставок, и поэтому важно укреплять слабые места в рамках всего процесса. Это может подразумевать работу на многих уровнях и использование самых различных видов контроля: от использования защитных сенсоров на производственных объектах до установки программных брандмауэров. Необходимо разрабатывать системы с таким расчетом, чтобы предприятие, эксплуатирующее тот или иной актив, являлось не единственной организацией, имеющей доступ ксоответствующим данным. Сервисные компании, поставщики и производители оборудования также могут получить доступ к операционным данным и данным о работе оборудования в целях повышения качества своих услуг.

При отсутствии четкой структуры работы могут создаваться возможности для непредвиденной утечки данных или уязвимости систем, которые могут быть легко использованы в своих целях третьими лицами. При разработке систем осуществления контроля и мониторинга процессов важно обеспечивать четко определенные права доступа к данным и возможность отслеживать нарушение таких прав.

Готовность к угрозам

Однако просто обеспечивать безопасность недостаточно. Необходимо также подготавливать системы к возможным угрозам или же проводить непрерывный мониторинг, чтобы всегда иметь информацию о том, защищена ли система или же была взломана. Для того, чтобы меры по обеспечению готовности систем к угрозам давали реальные результаты, необходимо с самого начала понимать, от чего необходимо защититься. Применительно к киберугрозам в нефтегазовом секторе прослеживается четкая закономерность, которая позволяет получить базовое представление о том, какие виды атак могут производиться на ICS-системы нефтегазовых компаний. В то же время это представление должно дополняться пониманием специфики бизнес-рисков конкретной организации, чтобы спрогнозировать возможные происшествия и соответствующим образом спроектировать системы по обнаружению угроз.

Гибкость

Устойчиво функционирующая организация должна иметь планы и процедуры для обнаружения, сдерживания или нейтрализации последствий кибератак и оперативного восстановления штатного режима работы. Вкратце эти шаги можно обозначить следующим образом: «обнаружить», «среагировать» и «восстановить работу». Набор конкретных мер для обеспечения успеха будет зависеть от вида выявленной угрозы. На всех уровнях цепочки создания стоимости нефтегазовых предприятий, идет ли речь о подготовке устья скважины, переработке, транспортировке или же очистке и поставке продукции, необходимо проводить постоянный мониторинг состояния оборудования, чтобы обнаруживать любые отклонения

в его работе в режиме реального времени. Это подразумевает постоянное получение информации о состоянии насосного оборудования, трубопроводной арматуры, компрессоров и технологических узлов, включая данные о темпах добычи и движении жидкостей и газов. Постоянная осведомленность о динамике роста этих показателей позволит быстро принимать меры для устранения угроз окружающей среде и безопасности людей, возникающих при выходе оборудования из-под контроля, вплоть до остановки производственных процессов в случае такой необходимости.

При проведении операций по переработке или очистке нефти и природного газа обнаружить факты незаконного присвоения или изменения служебной коммерческой информации об эксплуатационных характеристиках скважин, текущих темпах добычи или использованию активов может оказаться сложной задачей. Поэтому очень важно внедрять средства защиты уже на этапе разработки систем по управлению такими данными. Даже если средства осуществления контроля не сработают и кибератака не будет обнаружена, способность системы обеспечить эффективное реагирование может помочь минимизировать производственные потери, а также финансовый, экологический и репутационный ущерб. На этапах реагирования и восстановления необходимо будет не только принять немедленные меры по коррекции работы пострадавшего оборудования и систем, но и провести тщательный анализ с целью понимания того, где и как произошла атака, какие недостатки системы создали возможность для ее возникновения и что требуется сделать, чтобы смягчить ее последствия и предотвратить риски в дальнейшем.

Важно отметить, что просто разработать планы и регламенты будет недостаточно. По аналогии с учебной пожарной тревогой, необходимо периодически проверять эффективность применения таких планов и регламентов путем моделирования и проигрывания чрезвычайных ситуаций, требующих совместной работы бизнес- и технических специалистов.

Создание программы такого рода подразумевает многолетнюю работу, однако на каждом этапе трансформации необходимо преследовать одну и ту же цель, постепенно повышая уровень развития внутренних контрольных процедур для создания безопасной, готовой к работе и защищенной контрольной среды.

Внедрение ключевых средств обеспечения контроля

Несмотря на то что показатели готовности к рискам и зрелости ICS-систем отличаются от компании к компании, существует несколько основополагающих средств обеспечения контроля за киберрисками, которые должна иметь в наличии практически любая нефтегазовая компания. Внедрение этих ключевых средств осуществления контроля может стать началом для разработки специализированной программы по обеспечению безопасности и гибкости корпоративных систем и их готовности к угрозам.

Проведение информационно-разъяснительной работы

Необходимо разъяснять опросы кибербезопасности различным специалистам организации, а также обучать их необходимым навыкам безопасного и ответственного использования систем.

Осуществление контроля за доступом

Обеспечивается физическая и логическая безопасность компонентов ICS-систем, включая аппаратное обеспечение, программные приложения и компьютерные сети; доступ предоставляется только после осуществления формализованных процедур аутентификации и авторизации.

Безопасность сети

Доступ к проводным и беспроводным коммуникационным сетям в рамках ICS-систем ограничивается и защищается с учетом передового опыта в области управления идентификационными данными и правами доступа, включая проведение непрерывного мониторинга процессов предоставления доступа и аутентификации, а также обеспечение безопасности удаленных соединений.

Переносные носители информации

Использование переносных носителей информации в рамках ICS-системы должно ограничиваться; все устройства должны проверяться на предмет наличия вредоносного программного обеспечения.

Реагирование в случае возникновения инцидентов

В организации разрабатываются политика и процедуры управления инцидентами, эффективность которых периодически проверяется на практике.

Рис. 4. Ключевые средства обеспечения контроля

Управление	Безопасность	Готовность к угрозам	Гибкость
Управление киберрисками	**Защита информации**	**Управление угрозами**	**Управление инцидентами**
Управление рисками и соблюдение требований	Управление жизненным циклом информации	Проверка готовности к кибератакам	Реагирование в случае возникновения инцидентов
Политики и стандарты	Шифрование данных		Управление непрерывностью деятельности
Информационно-разъяснительная работа и обучение	**Управление идентификационной информацией и правами доступа**	**Управление инцидентами**	
Управление отношениями с поставщиками	Аутентификация	Мониторинг событий в системе безопасности	
	Управление ролями и правами пользователей		
	Управление жизненным циклом идентификационных данных пользователей		
	Защита инфраструктуры		
	Безопасность сети		
	Физическая безопасность		
	Безопасность системы		
	Выявление и исправление недостатков систем		
	Защита от вредоносного программного обеспечения		

Обеспечение эффективных механизмов управления

Четкое определение круга лиц, ответственных за обеспечение безопасности ICS-систем, имеет фундаментальное значение. При этом должны быть четко прописаны функции и обязанности всех участников процесса: от менеджеров до операторов оборудования и третьих лиц. В конечном итоге должен быть создан единый порядок подотчетности. В противном случае будет сложно не только определить единые требования для всей организации, но и понять, в каких случаях следует отдать предпочтение централизованным, а в каких локальным решениям.

Прежде производственная среда, включая процессы управления производственными операциями и обеспечения безопасности, находилась в ведении производственных и инженерно-технических специалистов. Сегодня вопросы безопасности ICS-систем все чаще рассматриваются в контексте всей организации, попадая в сферу ответственности директора по информационной безопасности. Однако речь не идет о том, что ИТ-службам нужно вмешиваться в управление, например, нефтяным месторождением или нефтеперерабатывающим заводом. Даже с учетом ответственности, которую несет директор по информационной безопасности, за разработку надлежащих решений и их внедрение на местах по-прежнему отвечают инжиниринговые компании.

Внедрение программ информационной безопасности при управлении производственными процессами сопряжено с дополнительными сложностями, связанными с управлением кадровыми ресурсами. Должностные обязанности часто вынуждают людей работать на одном и том же объекте долгое время. Если не дать им четкого представления о карьерном росте, возможны два сценария развития событий:

1. Специалисты в области информационных технологий, вынужденные заниматься обеспечением безопасности ICS-систем, будут рассматривать эти обязанности как нечто дополнительное и второстепенное и относиться к ним без энтузиазма.
2. Специалисты по обеспечению безопасности быстро достигнут карьерных высот в рамках отведенного им участка и отправятся на поиски другого работодателя.

В идеале организация должна разработать программу информационно-разъяснительных мероприятий, чтобы преодолеть непонимание между ИТ-специалистами и специалистами по ICS-системам, а также обеспечить возможности карьерного роста для тех работников, которые желают специализироваться в области информационной безопасности ICS-систем. Карьерный рост в данной области часто начинается с начальной позиции аналитика и для успешного сотрудника может закончиться на должности руководителя международного отдела безопасности организации.

Внедрение программ информационной безопасности при управлении операционными процессами сопряжено с дополнительными сложностями, связанными с управлением кадровыми ресурсами.

Заключение

За прошедшие несколько лет в нефтегазовом секторе практически стерлись привычные границы между корпоративными ICS-системами и информационными системами. Благодаря дигитализации нефтегазовых компаний эта эволюция продолжается. По мере того как взаимосвязь между указанными видами систем будет укрепляться, продолжат расти частотность и изощренность кибератак. Тем не менее, до сих пор большинство компаний не справляется с задачей подготовки систем к кибератакам.

А начинать нужно с оценки зрелости средств осуществления внутреннего контроля, обеспечивающих безопасность операционных процессов. Для нефтегазовых компаний выйти за рамки традиционного подхода к обеспечению безопасности операционных процессов и внедрить надежные, гибкие и готовые к атакам механизмы — это не просто важное условие для более эффективной защиты операционной целостности перед лицом растущего числа киберугроз, но и возможность оптимизировать бизнес-процессы за счет наращивания производительности путем дигитализации и полной интеграции ICS-среды.

В свете растущей осведомленности общественности о киберпреступлениях и их катастрофических последствиях для ключевых инфраструктурных элементов, задача подготовки к кибератакам никогда не была столь актуальной.

Контактная информация

«Делойт» может оказать содействие при проведении оценки зрелости системы обеспечения контроля за киберрисками операционной деятельности в вашей организации. Для получения более подробной информации обратитесь к любому из наших специалистов в области управления рисками.

Авторский коллектив

Пол Зонневельд
Руководитель Международной группы по предоставлению консультационных услуг в области управления рисками предприятиям энергетики и добывающей промышленности
«Делойт», Канада
+1 403 503 13 56
pzonneveld@deloitte.ca

Эндрю Слотер
Исполнительный директор Центра решений «Делойта» для предприятий энергетического сектора
«Делойт», США
+1 713 982 35 26
anslaughter@deloitte.com

Для международных контактов:

Антон Боутс
Руководитель Международной группы по обслуживанию предприятий нефтегазового сектора
«Делойт Туш Томацу Лимитед»
+27 11 806 51 97
abotes@deloitte.co.za

Пол Зонневельд
Руководитель Международной группы по предоставлению консультационных услуг в области управления рисками предприятиям энергетики и добывающей промышленности
«Делойт», Канада
+1 403 503 13 56
pzonneveld@deloitte.ca

Дина Камаль
Руководитель Локальной группы по предоставлению консультационных услуг в области управления рисками предприятиям энергетики и добывающей промышленности
«Делойт», Канада
+1 416 775 74 14
dkamal@deloitte.ca

Амир Белхеллади
Партнер по предоставлению консультационных услуг в области управления рисками
«Делойт», Канада
+1 514 393 70 35
abelkhelladi@deloitte.ca

Тиаан ван Шалквык
Помощник директора по предоставлению консультационных услуг в области управления рисками
«Делойт», Африка
+27 11 806 51 67
tvanschalkwyk@deloitte.co.za

Раджив Чопра
Руководитель Международной группы по обслуживанию предприятий энергетики и добывающей промышленности
«Делойт Туш Томацу Лимитед»
+44 20 7007 29 33
rchopra@deloitte.co.uk

Стив Ливингстон
Руководитель Локальной группы по предоставлению консультационных услуг в области управления рисками предприятиям энергетического сектора, инфраструктуры и коммунальных услуг
«Делойт», США
+1 206 716 75 39
slivingston@deloitte.com

Рамси Хаджи
Старший менеджер по предоставлению консультационных услуг в области управления рисками
«Делойт», США
+1 561 962 78 43
rhajj@deloitte.com

Марко Ван Цвам
Партнер по предоставлению консультационных услуг в области управления рисками
«Делойт», Нидерланды
+31 88 288 08 90
mvanzwam@deloitte.nl

Стюарт Дэвидсон
Директор по предоставлению консультационных услуг в области управления рискми
«Делойт», Великобритания
+44 20 7303 21 78
stdavidson@deloitte.co.uk

Роб Хэйз
Директор по предоставлению консультационных услуг в области управления рисками
«Делойт», Великобритания
+44 20 7007 26 06
rjhayes@deloitte.co.uk

deloitte.ru

О «Делойте»

Наименование «Делойт» относится к одному либо любому количеству юридических лиц, включая их аффилированные лица, совместно входящих в «Делойт Туш Томацу Лимитед», частную компанию с ответственностью участников в гарантированных ими пределах, зарегистрированную в соответствии с законодательством Великобритании (далее — ДТТЛ). Каждое такое юридическое лицо является самостоятельным и независимым юридическим лицом. ДТТЛ (также именуемая «международная сеть «Делойт») не предоставляет услуги клиентам напрямую. Подробная информация о юридической структуре ДТТЛ и входящих в нее юридических лиц представлена на сайте www.deloitte.com/about.

«Делойт» предоставляет услуги в области аудита, консалтинга, финансового консультирования, управления рисками, налогообложения и иные услуги государственным и частным компаниям, работающим в различных отраслях экономики. «Делойт» — международная сеть компаний, в число клиентов которой входят около четырехсот из пятисот крупнейших компаний мира по версии журнала Fortune. «Делойт» имеет многолетний опыт практической работы при обслуживании клиентов в любых сферах деятельности более чем в 150 странах мира и использует свои обширные отраслевые знания и опыт оказания высококачественных услуг для решения самых сложных бизнес-задач клиентов. Более 244 тысяч специалистов «Делойта» по всему миру привержены идеям достижения результатов, которыми мы можем гордиться. Для получения более подробной информации заходите на нашу страницу в Facebook, LinkedIn или Twitter.

Настоящее сообщение содержит информацию только общего характера. При этом ни компания «Делойт Туш Томацу Лимитед», ни входящие в нее юридические лица, ни их аффилированные лица (далее — «сеть «Делойт») не представляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Прежде чем принять какое-либо решение или предпринять какие-либо действия, которые могут отразиться на вашем финансовом положении или состоянии дел, проконсультируйтесь с квалифицированным специалистом. Ни одно из юридических лиц, входящих в сеть «Делойт», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящее сообщение.

© 2017 ЗАО «Делойт и Туш СНГ». Все права защищены.