СОЮЗ НЕФТЕГАЗОПРОМЫШЛЕННИКОВ РОССИИ

Межотраслевой
экспертно-аналитический центр

КИБЕРБЕЗОПАСНОСТЬ И АНАЛИЗ РИСКОВ ЛОКАЛИЗАЦИИ

ноябрь 2018

Обзорно-аналитическое исследование

Анатолий Замрий
Сергей Черных

Материал опубликован в журнале «Oil&Gas Journal Russia», ноябрь 2018

Перед Вами обзорно-аналитическое исследование Межотраслевого экспертно-аналитического центра Союза Нефтегазопромышленников России – «Кибербезопасность и анализ рисков локализации»

В материале раскрывается место кибербезопасности в общем ландшафте информационных технологий, и отдельно анализируются риски локализации зарубежных компаний в России.

Концепция «Индустрия 4.0», или Четвертая промышленная революция, предусматривает сквозную цифровизацию всех физических активов предприятия и их интеграцию в единую экосистему. Вроде бы новая парадигма – новые возможности для всех, но история доказывает, что смена формации может стать началом конца для тех предприятий, которые к ней не были готовы. Только от нас зависит: дадут ли изменения новый толчок для роста компании или приведут к закату целых отраслей экономики. Эксперты говорят о «диджитал» как о способе выживания компаний (отдельная тема – это сами термины «цифровизация» и «диджитал» – очень много путаницы пока!).

По оценкам экспертов, российские производители стали в последнее десятилетие много инвестировали в свои активы. Вопреки стереотипам об устаревшем оборудовании советских времён, отечественные предприятия сегодня – самые эффективные и высокомаржинальные в мире. Так А.А. Мордашов считает, что «Северсталь» стабильно показывает лучшую рентабельность по показателю EBITDA среди глобальных конкурентов (32,2% по итогам 9 месяцев 2017 года – «HBR – Россия»).

Эксперты McKinsey оценивают потенциальный эффект от применения инструментов Индустрии 4.0 в металлургии более чем в $115 млрд. Среди основных источников дополнительных доходов они видят такие направления как:

- роботизация;
- удалённый контроль и управление оборудованием;
- увеличение эффективности труда сотрудников через цифровизацию;
- внедрение интегрированных платформ;
- глубокая аналитика данных и предиктивные инструменты.

Только благодаря цифровизации управления оборудованием отрасль может заработать более $40 млрд. В металлургии и горной добыче в целом дополнительные доходы прогнозируются на уровне 2,7% от выручки всех компаний отрасли или 9% от их прибыли. Если эти возможности не будут использованы сегодня, завтра возьмут верх конкуренты, и российским компаниям достанется печальная участь догоняющих, а проще говоря – отстающих.

Цифровизация как стратегический приоритет

Эксперты VYGON Consulting оценили будущие экономические эффекты цифровизации нефтяной отрасли. Далее коротко в изложении основные выводы, сделанные в исследовании «Цифровая добыча нефти: тюнинг для отрасли» в июне 2018 года.

Специалисты VYGON Consulting детально проанализировали финансовые и институциональные барьеры цифровой трансформации нефтегазовой отрасли России, сформировали прогнозы добычи российской нефти при сохранении текущих условий технологического развития и в случае раскрытия «цифрового» потенциала отрасли, а также оценили будущие экономические эффекты цифровизации нефтяной отрасли для государства и компаний.

В России на 2018 год насчитывается более 40 проектов интеллектуальных месторождений, суммарная добыча которых составляет 140 млн тонн или 27% от общего объёма в стране. Все крупнейшие отечественные компании выделяют цифровизацию как стратегический приоритет.

Потенциальный прирост извлекаемых запасов нефти в России за счёт технологического развития отрасли составляет 6,8 млрд тонн. Это может позволить нарастить добычу до 607

млн тонн к 2035 году с учётом экономических, финансовых и инфраструктурных ограничений – сценарий «Цифровая трансформация». При сохранении текущего уровня цифрового развития – сценарий «Status quo» – потенциальный уровень составляет около 525 млн тонн.

В случае снижения цен на нефть до $40 за баррель к 2035 г. цифровая трансформация позволит компенсировать 3,2 трлн руб дисконтированных выпадающих доходов государства и нарастить NPV нефтяного upstream на 3,3 трлн руб. в реальном выражении по сравнению с оптимистическим сценарием проекта Энергетической стратегии России до 2035 года.

Роман Самсонов указывает на интересную динамику роста количества цифровых месторождений за последние годы с учётом того, что их количество достигло в России уже сорока, ведь ещё в 2016 году их было всего 26, это уже тогда составляло около 12% от общего их количества в мире. При этом распределение было следующим: «Роснефть» – 10, «Газпром» – 7, «ЛУКОЙЛ» –4, «НОВАТЭК» –2, «Татнефть» – 1, «РИТЭК» – 1, «Зарубежнефть» – 1.

Если сравнить эту тенденцию роста числа цифровых скважин с мировой, то увидим следующие показатели: если на 1 января 2015 года их было 15 тысяч, то в России было не более 2 тысяч из общего количества. Далее темпы перехода на цифровые технологии в добыче стали существенно отличаться. Shell уже в 2016 году перешла на управление в режиме реального времени 24/7 практически всем своим фондом в 20 тысяч скважин. К этому уровню приближается и BP.

Российской нефтедобывающей отрасли для реализации сценария «Цифровая трансформация» необходимо инвестировать порядка 24 трлн руб в период с 2018 по 2035 гг. в реальном выражении. Для таких масштабных вложений необходимо создать благоприятные условия, в том числе в виде государственного стимулирования.

Основным препятствием цифровой трансформации российской нефтедобычи эксперты VYGON Consulting называют высокую зависимость от иностранных технологий на фоне действия санкций. Развитию собственных технологий мешает целый набор системных проблем: недостаточные стимулы у бизнеса для инвестиций в НИОКР, неразвитый рынок капитала, отсутствие венчурной инфраструктуры, слабая конкуренция на нефтесервисном рынке, наличие административных барьеров.

О трансформации бизнеса и экономики

В апреле 2018 года «Газпром нефть» утвердила цифровую трансформацию бизнеса в качестве одного из приоритетных направлений деятельности и объявила о создании профильной дирекции. Руководитель этой дирекции Андрей Белевцев говорит о разнице в понятиях цифровизация и цифровая трансформация. Цифровизация в его понимании – это как автоматизация. То есть использование цифровых технологий для повышения эффективности текущих организационных и бизнес-процессов. Цель «Газпром нефти» – именно трансформация всей компании с использованием тех возможностей, которые даёт технология, чтобы получить, возможно, принципиально иные бизнес-модели, изменения характеристик самой работы организации, порядка ведения бизнеса.

Поэтому цифровая трансформация – это переход к новой модели ведения бизнеса. При этом нужно иногда не бояться самостоятельно атаковать какие-то свои источники выручки или традиционные бизнес-модели, потому что, если этого не сделаешь ты, сделает кто-то другой.

Например, цифровая трансформация позволяет создавать то, что сейчас называют киберфизическими системами. Часто мы не можем ставить эксперименты над объектами

реального мира, это слишком дорого и сложно. Цифровые двойники позволяют создать виртуальную копию реального мира, ставить эксперименты недорого и безопасно, а в реальную среду переносить уже наработанный результат.

Инициированная правительством РФ в середине 2017 г. программа «Цифровая экономика РФ», призванная сформировать необходимую инфраструктуру и регуляторную среду для цифрового развития страны, не учитывает специфические особенности отдельных отраслей. Принимая во внимание важность нефтяного upstream для формирования доходов бюджета и роста российской экономики в целом, необходимо создание отраслевого центра компетенций в цифровизации и плана мероприятий по устранению барьеров развития уже сейчас, чтобы сохранить конкурентные позиции российской нефтянки на мировом рынке.

Приоритетные технологии:

- большие данные;
- нейротехнологии и искусственный интеллект;
- системы распределённого реестра;
- квантовые технологии;
- новые производственные технологии;
- промышленный Интернет;
- компоненты робототехники и сенсорика;
- технологии беспроводной связи;
- технологии виртуальной и дополненной реальности.

Как мы видим, обозначенные технологии в возможностях применения охватывают практически все виды экономической деятельности и управления. То есть цифровая экономика – это совокупность технологий, обеспечивающая практически мгновенный обмен информацией, прозрачность процессов на всех уровнях, доступность государственных и частных сервисов в онлайне и автоматизацию большинства профессий.

Промышленная автоматизация

Одним из важнейших направлений автоматизации является промышленная автоматизация в широком смысле этого слова. Далее, заглянув в историю вопроса, более подробно остановимся на тех рисках, которые возникают или могут возникнуть в связи с цифровизацией этих процессов.

Автоматизировать производственные процессы индустриальные гиганты начали ещё в середине 30-х годов прошлого века. На протяжении многих десятилетий комплексы аппаратных и программных средств непрерывно совершенствовались и усложнялись. Автоматизация производственных процессов – например, в нефтепереработке – продвинулась далеко вперёд. Например, работу современного нефтеперерабатывающего завода контролируют сотни тысяч датчиков и приборов, а поставки топлива в режиме реального времени отслеживаются системами спутниковой навигации. Каждый день средний российский НПЗ производит более 50 000 терабайт информации. Для сравнения, 3 миллиона книг, которые хранятся в цифровом хранилище Российской государственной библиотеки, занимают в сотни раз меньше – «всего» 162 терабайта.

История промышленной автоматизации имеет несколько важных вех. Если проследить, как развивались все основные направления в автоматизации, можно обнаружить несколько ключевых людей и инноваций. Первая распределённая система управления (DCS) была

разработана в 1970-х командой инженеров Honeywell, а программируемый логический контроллер изначально был детищем изобретателя Дика Морли. Результатом нескольких инновационных стартапов стало программное обеспечение для человеко-машинного интерфейса и модули ввода/вывода. Некоторые крупные компании вложились в разработку современных датчиков и исполнительных устройств. Многие новаторы, работающие в этом бизнесе, в своём развитии рано или поздно упираются в потолок и продают свои наработки. Но некоторые продолжают успешно развиваться.

Сфера промышленных приборов и средств управления всегда была благодатной почвой для появления новых продуктов – усовершенствованных датчиков, усилителей, регистраторов, клапанов, элементов управления и прочих приспособлений и гаджетов. Но рынки их сбыта относительно малы, специализированы и разрозненны, что не позволяет обеспечить сколько-нибудь значительный объем продаж конкретного продукта.

Многие компании, работающие в промышленной автоматизации, выросли на инновационных разработках для узких, нишевых приложений. Заказчиками в этом случае были местные конечные пользователи, которые имели специфические потребности и были не против опробовать новые идеи. Успешные решения выходили на новые рынки в том случае, если новый продукт имел реальную ценность, и, если основателю удавалось найти подходящий персонал для управления, продаж и маркетинга, чтобы перешагнуть этап индивидуального предпринимательства и выйти на новый уровень.

Автоматизация может играть важную роль в повышении производительности в любой сфере производства или услуг. На сегодняшний день автоматизация управления производством наиболее распространена в обрабатывающих отраслях, в области добычи углеводородного сырья. В последние годы на производственных предприятиях используются следующие типы автоматизации:

- информационные технологии (ИТ);
- автоматизированное производство (CAM);
- оборудование с числовым программным управлением (NC);
- роботы;
- гибкие производственные системы (FMS);
- компьютерное интегрированное производство (CIM).

В лаконичной форме промышленная автоматизация может быть определена как использование установленных технологий, систем и устройств автоматического управления, которые обеспечивают автоматическую работу, контроль производственных процессов – без значительного вмешательства человека и достижение высокой производительности.

Промышленную автоматизацию можно охарактеризовать как совокупность технических и программных средств, включающих в себя средства измерения и средства автоматизации отраслевого (промышленного) назначения, предназначенные для выполнения функций:

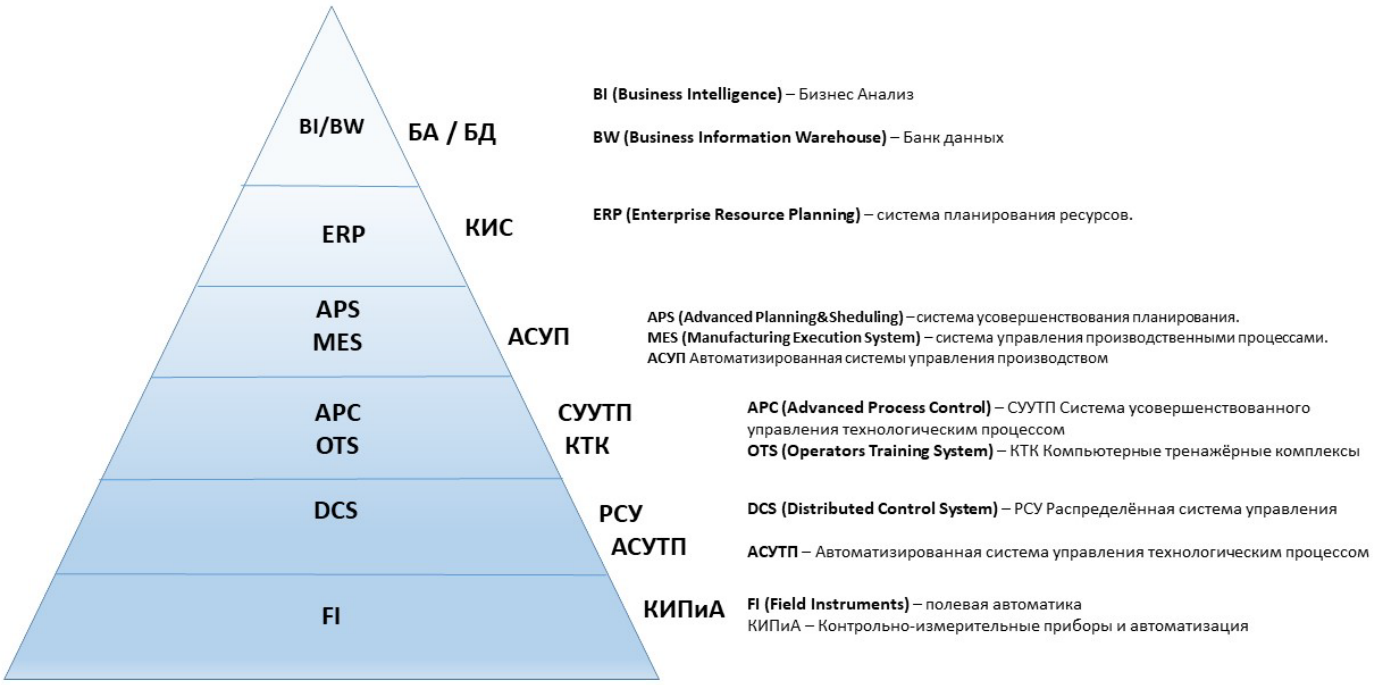
- восприятия информации, данных;
- преобразования;
- хранения;
- контроля;
- регулирования;
- формирования прогнозов и сценариев;
- управления процессами.

Основными преимуществами промышленной автоматизации принято считать:

- повышение производительности процессов;
- оптимизация затрат на эксплуатацию;
- повышение качества продукции;
- уменьшение ручных проверок;
- повышение уровня безопасности.

В настоящее время для автоматизации промышленных процессов разработано множество приборов, оборудования и систем управления производством, предприятием. Схематично их можно отобразить в виде условной пирамиды уровней автоматизации, где внизу будет размещаться контрольно-измерительное оборудование, дающее исходные данные и параметры работы основных элементов оборудования, и выше системы, вбирающие в себя информацию нижних уровней и позволяющие осуществлять все более и более сложные функции контроля и управления жизненным циклом.

Парадигма уровней автоматизации



Функционирование столь сложных систем неизбежно поднимает проблемы информационной безопасности, устойчивости функционирования, надёжности.

Устраняя человеческий фактор из управления всё более сложными технологическими процессами на производстве, и получая от этого вполне ощутимую выгоду (см. цифры выше), компании создают для себя новые риски, а именно риски вмешательства в управление производством извне, через цифровые системы автоматизации. Здесь сделаем небольшое отступление и изложим, насколько проблема киберпреступности – относительно новый вид преступности для человечества серьёзно рассматривается международным сообществом.

Киберпреступность – опасность в электронной среде

Согласно рекомендациям экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде.

Кстати, первое упоминание об использовании компьютера с целью совершения преступления было обнародовано в 1960-х годах, когда компьютеры представляли собой большие универсальные компьютеры, так называемые ЭВМ, как пишут А.Б. Николаева, М. В. Тумбинская в своём исследовании «Киберпреступность: история развития, проблемы практики расследования».

Они рассматривают преступление, совершенное в киберпространстве – как противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.

Сегодня киберпреступность – масштабная проблема, а вредоносные программы пишутся с целью незаконного получения денег. Развитие интернета стало одним из ключевых факторов, определивших эти перемены. Компании и отдельные пользователи уже не мыслят без него свою жизнь, и все больше финансовых операций проводится через интернет. Киберпреступники осознали, какие огромные возможности для «зарабатывания» денег с помощью вредоносного кода появились в последнее время, и многие из нынешних вредоносных программ написаны по заказу или с целью последующей продажи другим преступникам.

Конвенция Совета Европы говорит о четырёх типах компьютерных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

- незаконный доступ – ст. 2 (противоправный умышленный доступ к компьютерной системе либо её части);
- незаконный перехват – ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с неё либо в её пределах);
- вмешательство в данные – ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
- вмешательство в систему – ст. 5 (серьёзное противоправное препятствование функционированию компьютерной системы путём ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

В концепции «Стратегии кибербезопасности», разработанной Комиссией по информационной политике Совета Федерации РФ даны следующие важные определения.

1. Информационное пространство – сфера деятельности связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

2. Информационная безопасность – состояние защищённости личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

3. Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства);

4. Кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Таким образом, кибербезопасность – область информационных технологий, а точнее информационной безопасности, занимающаяся защитой сетей, компьютеров, программ, устройств от атак, повреждения или несанкционированного доступа.

Основу кибербезопасности составляют три основных процесса:

- предотвращение угрозы,
- обнаружение угрозы,
- реагирование.

Сегодня в большей степени распространены следующие виды киберугроз:

- программы типа Wiper, выводящие из строя и затирающие информацию на дисках;
- программы-шифровальщики;
- эксплойты;
- ботнет-агенты;
- атаки бэкдор (от англ. back door – «чёрный ход»);
- DDoS атаки, направленные на отказ в обслуживании;
- атаки прямого доступа;
- подслушивание;
- подмена данных, фальсификация;
- фишинг (от англ. fishing – выуживание);
- кликджекинг (англ. Clickjacking);
- майнеры криптовалют;
- ошибки, халатность пользователей,
- предумышленные утечки через сотрудников, имеющих доступ.

В качестве мер защиты применяются:

- специальное ПО для сканирования и обнаружения возможных угроз;
- процедуры аутентификации;
- «лёгкие» и надёжные средства защиты узлов;
- сегментация сетей (межсетевые экраны);
- резервное копирование;
- тщательное и непрерывное управление доступом;
- профессионально подготовленный персонал и специализированные центры реагирования;
- обучение и тестирование знаний пользователей;
- политика установки обновлений в индустриальной сети;

• средства мониторинга уязвимостей и патч-менеджмента;

• использование средств поведенческого анализа пользователей и сущностей в процессе мониторинга событий информационной безопасности и др.

Константин Саматов, руководитель направления в Аналитическом центре Уральского центра систем безопасности, член Ассоциации руководителей служб информационной безопасности, предлагает ещё один путь защиты. Это Penetration Test – метод оценки безопасности компьютерных систем или сетей передачи данных посредством моделирования атаки нарушителя, как правило, являющийся частью аудита информационной безопасности организации.

Тестирование на проникновение, как правило, является частью аудита информационной безопасности и относится к так называемому активному анализу, дополняющему «пассивный» анализ уязвимостей информационной системы, осуществляемый при помощи инструментальных средств – сканеров безопасности. Целью тестирования на проникновение является оценка возможности успешного проведения злоумышленником атаки (в т. ч. целевой) на информационную систему и её последствий.

А его задачи следующие:

- выявление недостатков в применяемых в информационной системе мерах безопасности и оценка возможности использования их нарушителем;
- получение на основе объективных свидетельств оценки текущего уровня защищённости;
- практическая демонстрация возможности использования уязвимостей; выработка рекомендаций по устранению выявленных уязвимостей и недостатков для повышения уровня защищённости.

При этом моделирование поведения нарушителя применительно к реально функционирующей информационной системе, как правило, не используется. Отсюда давно известная проблема: применяемые меры безопасности во многих случаях не могут обеспечить эффективную защиту информационной системы, несмотря на то, что по документации все идеально (преобладание "бумажной безопасности"). С учётом этого, по мнению К. Саматова, проведение тестирования на проникновение необходимо для любой информационной системы, но прежде всего для информационной системы, являющейся объектом критической информационной инфраструктуры.

Так, в соответствии со ст. 1 и ст. 4 Федерального закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», целью данного федерального закона является устойчивое функционирование критической информационной инфраструктуры Российской Федерации при проведении в отношении неё компьютерных атак, а одним из принципов обеспечения безопасности – приоритет предотвращения компьютерных атак. Таким образом, несмотря на то, что в настоящее время обязательного требования по проведению тестирования на проникновение в действующем законодательстве пока не сформулировано, без проведения учебного моделирования атаки на информационную систему и успешного её отражения вряд ли можно говорить о достаточности принятых мер защиты.

В вопросах защиты исключительно промышленных систем – АСУТП – интересное структурирование этого процесса предлагает один из лидеров автоматизации компания Хоневелл.

Комплексные решения Honeywell по защите АСУ ТП.

Более подробно решения для типичных ситуаций киберугроз АСУТП можно увидеть в таблице, предлагаемой одним из лидеров в вопросах ИБ и КБ компанией Касперский Лаб.

Решения Касперский Лаб для устройств

Риски и угрозы	Технологии Лаборатории Касперского
Запуск нежелательного ПО	Белые списки; два режима – только обнаружение или обнаружение и блокирование
Вредоносное ПО	Передовые технологии сигнатурной защиты, облачные средства защиты с помощью репутационной базы Kaspersky Security Network или репутационной базы для изолированных сетей Kaspersky Private Security Network
Блокировщики и шифровальщики	Анти-шифровальщик
Сетевые атаки	Сетевой экран на уровне хоста
Подключение нежелательных устройств	Контроль устройств
Неавторизованные соединения с сетями Wi-FI	Контроль беспроводных сетей
Подмена программ ПЛК	Контроль целостности ПЛК
Особенности АСУ ТП - воздушные зазоры, ложные срабатывания и проч.	Доверенные обновления, которые тесируются с ПО ведущих производителей, сертификация продукта поставщиками решения для промышленной автоматизации

Решения Касперский Лаб для сетей

Риски и угрозы	Технологии Лаборатории Касперского
Неавторизованные сетевые устройства в промышленной сети	Контроль целостности сети обнаруживает новые и неизвестные устройства
Неавторизованные коммуникации в промышленной сети	Контроль целостности сети отслеживает коммуникации между новыми/неизвестными устройствами
Вредоносные команды ПЛК, инициированные: • Оператором или сторонним специалистом (подрядчиком) • Инсайдером • Злоумышленником / вредоносным ПО	Промышленный DPI анализирует коммуникации, происходящие на уровне промышленных протоколов, и детектирует появление аномалий в командах ПЛК и значениях параметров технологического процесса.
Сетевые атаки	Передовая система обнаружения вторжений (IDS) эффективна против всех известных шаблонов сетевых атак, в том числе против эсплуатации уязвимостей в индустриальном ПО и оборудовании.
Отсутствие данных для экспертного расследования и анализа	Инструменты цифровой криминалистики: мониторинг и безопасная запись подозрительных событий в промышленной сети и данных об обнаруженных атаках

Технические решения активно развиваются и широко освещаются в профессиональном сообществе – на эту тему публикуется большое количество материалов, затрагивающих все стороны этого сложного и многогранного процесса.

Отдельно необходимо проанализировать большую группу рисков и угроз, которые связывают с использованием программного обеспечения, либо оборудования, либо и того и другого, производителем которого являются мировые мейджоры из США, Японии, других стран.

Импортозамещения в области IT и риски локализации

В условиях санкций преимущество отдаётся всему отечественному. Но в области информационных технологий и промышленной автоматизации на сегодняшний день уровень использования отечественных продуктов ещё категорически невысокий. В критических системах, обеспечивающих обороноспособность страны, мы используем исключительно продукты, произведённые нашими разработчиками и изготовителями. В остальном же, уровень импортозамещения в области IT едва достигает 20-25 процентов.

До сих пор превалирующими операционными системами на российском пространстве являются системы американских компаний. Для построения ERP систем используются платформы западных мейджоров. Да и для более низких уровней IT-ландшафта часто применяется ПО иностранного производства. Хотя здесь уже гораздо больше присутствие отечественных разработчиков и производителей. Безусловно, с точки информационной безопасности (ИБ) гораздо правильнее не использовать продукты нероссийских производителей. В то же время, весьма интересно рассмотреть реальность рисков, связанных с использованием нероссийских продуктов.

Один из независимых экспертов по ИБ, Алексей Плешков приводит перечень из семи основных, но все ещё гипотетических, последствий начала активного применения западными технологическими компаниями-гигантами точечных санкций против наших соотечественников, которые смогут повлиять на процесс обеспечения защиты информации в организации:

1. Непродление/отзыв лицензий на право использования программного или

аппаратного обеспечения (или на получение сервиса) в новом периоде, в т.ч. остановка поставок обновлений, блокировка доступа к тематическим информационным порталам и витринам данных, прекращение уведомлений по всем ранее доступным каналам, снятие с технической поддержки продуктов и пр.

2. Принудительный отказ (с предусмотренной возможностью выплаты штрафов) вендора/интегратора от выполнения обязательств по ранее заключённым договорам в части проведения работ или оказания услуг, в т. ч. находящихся (поставка оборудования, создание продукта, интеграционные настройки, строительные работы и пр.).

3. Выполнение исполнителем условий договоров с низким (относительно ранее обговорённого) уровнем качества и/или фактический саботаж (в т. ч. несвоевременное информирование о наступлении рисковых событий, искусственное увеличение количества ошибок первого и второго рода и пр.) при оказании услуг.

4. Преднамеренная активация в программном и аппаратном обеспечении закладок различной природы и выполнение несанкционированных действий в целевой инфраструктуре в интересах третьих лиц и/или спецслужб.

5. Преднамеренная компрометация западными компаниями (ранее работавшими по контрактам с российскими юридическими и физическими лицами из санкционного списка) по запросам третьих лиц собранных в ходе совместных проектов массивов данных об инфраструктуре, процессах, персонале, компетенциях, профессиональных или бизнес-интересах и перспективных планах или иной интересующей информации о целевом объекте.

6. Активное влияние на принятие решения и лоббирование дополнительных, заранее невыгодных условий при заключении иностранными (не только США) компаниями-партнёрами новых контрактов с российскими организациями из санкционного списка или аффилированными с ними лицами.

7. Отзыв статусов и применение дополнительного воздействия финансового характера на партнёров и контрагентов, имеющих действующие контракты с компаниями из санкционного списка, вплоть до выдвижения требований по расторжению.

Кроме этого можно добавить ещё несколько гипотетических рисков, которые возникают в результате воздействия через закладки в программном и аппаратном обеспечении с целью выполнения несанкционированных действий в целевой инфраструктуре Заказчика с целью:

- остановки работы системы;
- затормаживание работы;
- стирание накопленных библиотек и баз данных;
- утечки конфиденциальной корпоративной информации через систему;
- разрушения самой системы Заказчика.

Несмотря на то, что многие эксперты указывают на возможность влияния разработчика системы на неё в процессе работы, на наш взгляд риски такого воздействия не так велики. В первую очередь это объясняется очень высокими репутационными рисками для разработчика и производителя. В нормальных условиях невозможно себе представить, чтобы уважающая себя крупная фирма мирового уровня позволила случиться какому-то инциденту у её заказчиков, приводящему к потере клиента или рынка, или даже только к угрозе такой потери. К тому же проблемы, возникшие на одном из рынков, незамедлительно повлияют и на другие. Невозможно себе даже представить, что разработчик или производитель уровня мировых мейджоров позволил бы себе такое

поведение на своём рынке. Более вероятно в таком случае падение сервиса или преднамеренные действия какой-то небольшой фирмы, для которой репутационные риски не стоят так высоко и могут быть компенсированы какими-то сиюминутными интересами. Либо же вероятность развала небольшой фирмы и потери заказчиком сервиса можно оценивать гораздо выше, чем вероятность каких-то преднамеренных действий со стороны мейджора.

Исходя из этого, в конечно счёте, мы должны оценивать в большей степени санкционные риски. То есть ситуацию, когда гипотетически разработчика или производителя можно заставить выполнять какие-либо действия, которые он ни в коем случае не станет делать в обычной ситуации на рынке. Но, во-первых, санкции могут заставить национальные компании страны, присоединяющейся к санкциям не поставлять какую-либо продукцию или не покупать какую-либо продукцию. Что уже может наносить достаточно ощутимый урон тем, кто санкции объявляет и поддерживает. Как правило, это наносит урон всей экономике стран, участвующих в санкционном процессе. Заставить же свои компании нарушать условия действующих контрактов с клиентами по рабочим системам, значит взять на себя риски глобальной потери клиентов – читай денег, огромных денег не только на санкционном рынке. Какая должна быть компенсация и откуда, из какого источника, чтобы она могла покрыть такие потери?

Поскольку политика является концентрированным выражением экономики, трудно себе представить, чтобы политика могла приводить к глобальным потерям в экономике в результате своей реализации.

В итоге, безусловно, мейджоры никогда не допустят ситуаций, при которых могут пострадать их деньги. И с учётом их масштабов для национальных экономик – и деньги национальных экономик в целом. Это абсолютно невероятно.

По сравнению с этим гораздо более вероятно прекращение функционирования и обслуживания систем, созданных небольшими производителями, в том числе и отечественными. Это может произойти, как уже упоминалось, в силу обычных причин течения жизненного цикла предприятия – кризиса кадров, конкуренции на внутреннем рынке, банкротства, аварий и пр.

Очень маловероятно, что серьёзные игроки на рынке промышленной автоматизации допустят какие-то серьёзные сбои в работе созданных ими систем. Слишком велика цена таких рисков для самих разработчиков и производителей.

Безусловно, технически, есть определённо риски воздействия разработчика или производителя на инфраструктуру Заказчика с учётом знания строения системы и, например, наличия постоянного сервисного канала связи. Теоретически, возможность влияния есть.

Есть отдельные известные эпизоды утечки приватной информации в системах, разработанных гигантами ИТ. Но это касалось социальных сетей, таких как ФБ, ВКонтакте, Одноклассники, мессенджеров – Viber, WhatsApp. Но в этих случаях никто и не гарантировал, что выложенная в социальную сеть, в личный эккаунт, информация будет гарантировано сохраняться, как тайна. Такую задачу эти системы, в принципе, не ставят перед собой. Надо понимать, что уровень конфиденциальности информации, выкладываемой в социальные сети, далеко не достигает 100 %. Здесь мы имеем дело с ошибочными ожиданиями и требованиями. Не более того.

По крупным промышленным системам управления случаев фактической реализации на практике упомянутых рисков до сегодняшнего дня не зафиксировано.

Тот же независимый эксперт по ИБ Алексей Плешков подтверждает, что выявленных внутри, полностью доказанных и подтверждённых с противоположной стороны фактов

реализации данной угрозы (в классическом понимании этого термина в контексте обеспечения информационной безопасности) по состоянию на март 2018 г. не зафиксировано. Все участники описанных выше рисков и сценариев демонстративно показывают друг другу свои партнёрские намерения и с удовольствием обсуждают условия, при которых заказчик сможет предпочесть импортозамещённому товару иностранный аналог.

Помимо этого, защита от рисков использования не отечественного «стороннего» оборудования и программного обеспечения может осуществляться, как техническими средствами, с помощью тех решений, которыми занимаются профессионалы ИБ и КБ, так и с помощью различных организационных мер. Большое значение имеет вопрос интеллектуальной собственности для защиты от данного вида рисков. Скажем, передача кода заказчику и в соответствующие структуры является частичной или полной передачей интеллектуальной собственности и способом защиты от подобных рисков для Заказчика. Поскольку это даёт право и возможность Заказчику контролировать, развивать и обслуживать свою систему дальше в любом случае, независимо от рисков, связанных с разработчиком или производителем.

Также весьма эффективной мерой является установление и строгое поддержание режима секретности или конфиденциальности, политик и регламентов безопасности при использовании соответствующих систем, обеспечивающего комплекс мер, предотвращающих появление возможных уязвимостей и утечек.

О мифах локализации

Следующий вопрос – как воспринимать продукцию локализованных в России предприятий крупных западных компаний-вендоров. Порой можно услышать некие соображения о рисках, связанных с работой с такими компаниями, которые могут заключаться в том, что уже было перечислено выше, а также нести в себе риск утечки разрабатываемой в России продукции аппаратного плана или интеллектуального плана в западном направлении, в сторону материнской компании. Порой можно услышать мнение, что это некие такие «агенты западных компаний».

Безусловно, необходимо признать, что и такого плана риски являются абсолютно надуманными и ложными. Любая фирма, принадлежащая крупной компании-вендору мирового уровня, будет, находясь в системе координат мирового бренда, подчиняться всем политикам, миссиям и задачам огромной компании и точно так же относиться к важным вопросам своих обязательств, как это было уже описано выше. И для дочерних компаний репутация марки будет стоять очень высоко. При этом локализованная компания будет гораздо устойчивее, надёжней и понятней серьёзному выстроенному Заказчику. Что касается возможных утечек технологий, то необходимо начать с того, что задолго до этих гипотетических утечек такие компании способствуют притоку отсутствующих технологий в России. Причём это технологии, испытанные в мире, отработанные, а не фантастические, только что придуманные. Сначала и постоянно в процессе работы идёт приток передовых технологий, на базе которых уже разрабатываются локальные решения и оборудование. А дальше – если интеллектуальная собственность принадлежит российской компании, работающей в России, каких-то необычайных рисков не видится. Таким образом, есть контрольные параметры (например, интеллектуальные права, условия использования для разных рынков, соблюдения режима конфиденциальности и т.д.) за которыми необходимо следить, и все будет в порядке. Так же, как и в случае со всеми другими компаниями.

К тому же в соответствии с российским законодательством это абсолютно российские компании – тот самый отечественный производитель. Да ещё и с мощной поддержкой мировых вендоров и грандов. Компании зарегистрированы в России, в соответствии с российским законодательством. В таких локализованных компаниях работают российские граждане. Налоги платятся в России, по месту регистрации компании. В чём, собственно, разница с другими российскими компаниями?

Если имеем в виду, что владельцами таких компаний являются зарубежные компании или лица, так у нас значительная часть крупных Заказчиков имеет в числе своих собственников зарубежные компании. Другая часть компаний-заказчиков активно пользуется услугами зарубежных топ-менеджеров и членов Советов директоров. И в этом случае как рассматривать риски, связанные с этими факторами? По итогу анализа эти риски, имеющиеся в самой компании-заказчике, могут оказаться в каких-то ситуациях выше, чем риски, связанные с взаимодействием с локализованной в России компанией, принадлежащей крупнейшим мировым грандам в своей области.

В итоге необходимо признать, что риски локализации совсем не так велики, а скорее ничтожны малы, по сравнению с тем, как это иногда рисуется.

И надо в любом случае проводить комплексную работу по обеспечению кибербезопасности, в большей степени уделяя внимание известным на сегодняшний день угрозам и уязвимостям. И, безусловно, развивать, и увеличивать область знаний в этом направлении и по мере продвижении в этом направлении и комплекс мер по обеспечению кибербезопасности компании, предприятия, организации. Тщательно разрабатывать и расширять политики обеспечения безопасности организации, тщательно и всеобъемлюще исполнять их на практике, уделяя внимание и техническим мерам, и обучению, и аудиту, и тестированию, и работе с сотрудниками, и новым технологиям, и профилактике, и кадрам, и взаимодействию с государственными и проверяющими органами.

Обеспечение корпоративной кибербезопасности – это нечто большее, чем просто покупка технологий и их развёртывание. Оно начинается с того, чтобы разработать универсальную платформу, которая будет отвечать всем потребностям кибербезопасности. Одна из лучших из существующих на сегодняшний день платформ кибербезопасности описана в книге Enterprise Cybersecurity, где подчёркивается, что абсолютная неуязвимость принципиально недостижима. Это связано с тем, что предприимчивый злоумышленник, имея неограниченное количество времени, способен преодолеть даже самую передовую защиту. Поэтому эффективность корпоративной программы кибербезопасности оценивается не в абсолютных категориях, а в относительных: насколько быстро она позволяет обнаруживать кибератаки, уязвимости, находить эффективные решения и насколько долго она позволяет в итоге сдерживать натиск противника. Чем лучше эти показатели, тем больше у штатных специалистов времени на то, чтобы оценить ситуацию и предпринять контрмеры – предпринимать весь необходимый комплекс мер.

Ответственный редактор *Сергей Черных*

info@sngpr.ru.com *www.sngpr.ru.com*