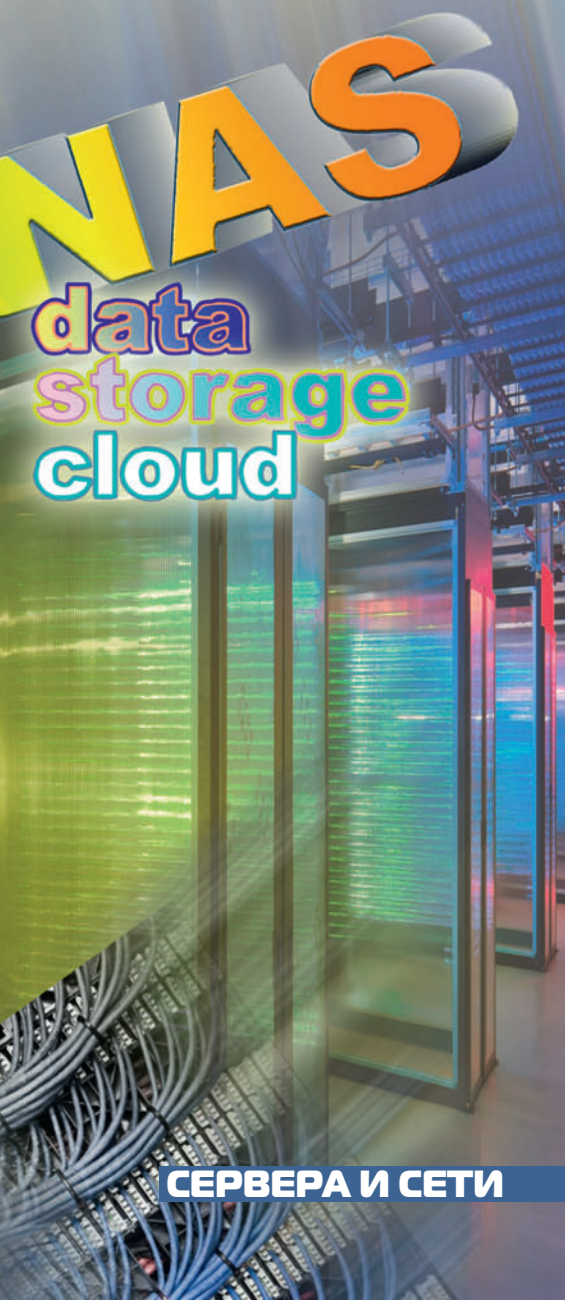
ФИНАНСОВО-ЭКОНОМИЧЕСКИЕ И ПРОМЫШЛЕННО-ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Раткин Леонид Сергеевич
главный специалист Центра фундаментальных исследований Физико-технического отделения НИЦ «Курчатовский институт», к.т.н.



СЕРВЕРА И СЕТИ

Аспекты информационной безопасности сложно анализировать, не учитывая специфику объекта. При универсальности многих подходов, рассматривать их лучше на наглядном примере. В данной статье задачи и их решения исследуются в применении к диверсификации систем защиты данных нефтяных скважин. Опишем примерную корпоративную информационную систему (КИС) вертикально интегрированной нефтяной компании (ВИНК) для учета и сбора данных с нефтяных скважин (сведения о приводимой структуре являются условными и могут варьироваться в зависимости от различных факторов – страны, сезона, климата, часового пояса, штатной численности, уровня капитализации ВИНК и т. д.). Инфраструктура современных КИС ВИНК предполагает порционное агрегирование данных и их оперативную аналитическую обработку (On-Line Analytical Processing, OLAP) с построением многомерных OLAP-кубов на разных уровнях. Самый нижний уровень – куст скважин, разработка которого ведется, как правило, единым подрядчиком с возможностью привлечения в качестве субподрядчиков ряда компаний. В этом случае данные, в т. ч. об их материально-техническом оснащении, уровне профессиональных компетенций, объемах капитализации и, разумеется, системах информационной безопасности, присутствуют в КИС ВИНК. Статистика проведенных работ каждым из субподрядчиков в рамках ВИНК и (согласно данным открытых информационных источников) по проектам ВИНК должна быть положительной (как минимум, неотрицательной), причем статистика по временной шкале должна быть эволюционирующей, т. е. значения ключевых показателей должны улучшаться по истечении определенных интервалов! Приветствуется линейный рост, но чаще наблюдается традиционная «пила»: субподрядчик «нестабилен» и от проекта к проекту демонстрирует чередование падений и взлетов. В этом случае субподрядчик может быть включен в т. н. «серый список» потенциально ненадежных исполнителей, что даже с точки зрения информационной безопасности может иметь далеко идущие последствия. Например, субподрядчик поставляет датчики для учета ежедневной прокачки добываемой нефти на куст скважин. На другом кусте скважин эти датчики не используются, поэтому проверить их на точность учета и, тем более, на «закладки» не всегда возможно. В минувшие годы (например, в конце 1990-х и начале 2000-х) это нередко приводило к тому, что датчики далеко не всегда поддерживали защищенный протокол передачи данных, и с помощью аппаратуры дистанционного наблюдения или перехвата сигнала представители конкурирующих ВИНК или промышленной разведки взламывали систему информационной безопасности, получали доступ к сведениям, составляющим коммерческую (или иную) тайну, которые нередко использовали для получения прибыли, формирования «стабильно-долгоиграющего» канала утечки или для других целей [1].

Следующий уровень КИС ВИНК – нефтяной промысел, объединяющий систему кустов, учитывающий пространственно-территориальное распределение датчиков и обсуживающих их подсистем, каналов связи и обработки информации. Здесь к проектированию OLAP-кубов подключается оперативная обработка транзакций (On-Line Transaction Processing, OLTP). Каждая транзакция – это сведение о проведенной операции, причем не только о добыче, но и ремонте, замене оборудования, вынужденном простое участка, засорении скважины, остановке бурового инструмента, промывке раствором и т. д. Синтез OLAP и OLTP на втором уровне КИС ВИНК оправдан большим числом операций – на 2-3 порядка выше, чем на первом. Возрастает нагрузка на каналы передачи и приема информации, соответственно, предъявляются повышенные требования, например, к аппаратуре защиты протоколов. К информационной безопасности добавляется промышленная: эксплуатируемая на участке КИС ВИНК система должна учитывать возможности возникновения нештатных ситуаций, неправильное реагирование на которые способно привести к аварии или техногенной катастрофе: например, «неотработка» или неправильная отработка ситуации способна перевести

аварию на кусте в техногенную катастрофу локального характера с перспективой расширения зоны охвата. Множество типов значений параметров и рабочих показателей значительно увеличивает информационный трафик, причем не только входящий или исходящий (как от системы «в целом»), но и между частями системы (т. н. «внутренний»). Это может привести к нарушению функций между частями системы, поэтому для минимизации рисков от угроз информационной безопасности необходимо «разрастание» системы не только «вглубь», но и «вширь» [2, 3]. Автору, бывшему системному администратору КИС, до сих пор памятны регулярные беседы с финансовым директором, часто не до конца понимавшим, что затраты на закупку новых систем или модернизацию существующих систем информационной безопасности «второго уровня» многократно окупятся, но они несравнимо малы по сравнению с теми моральными и физическим потерями, а также множественными убытками, которые предприятие может понести, сэкономив на информационной безопасности. Ведь мощная система защиты данных – это повышенная скорость обработки информации на более дорогих серверах, дополнительные нагрузки на энергосеть и системы двойного резервирования, вспомогательные накладные расходы на командирование специалистов для их обучения… Начиная со второго уровня ВИНК финансово-экономические и промышленно-технологические аспекты информационной безопасности становятся более осязаемы, как и необходимые затраты, которые потребуются для формирования инфраструктуры – не всей, а только ее наиболее важных элементов.

Третий уровень КИС ВИНК – группа промыслов. На этом уровне КИС доминирующей идеей является формирование и поддержание в постоянно-актуальном состоянии больших массивов данных. Именно на этом уровне чаще всего системные администраторы задумываются об облачных технологиях и механизмах высокоскоростного переноса информационных объемов. Но насколько оправданны эти размышления? Критерием применимости «облака» в каждой конкретной ситуации является ответ на вопрос: насколько ценны «забрасываемые в облако» данные и не принесет ли вред их использование конкурентом по окончании обработки? Если данные рабочие, т. е. промежуточные расчеты, на основании которых данные о первоначальных значениях неизвестны или «почти не восстановимы», – тогда они могут поменять прописку «на облачную». Но если существует ненулевой риск причинения вреда ВИНК или любой части ВИНК от их «обнародования», тогда привыкшим к строгому системному администрированию КИС ВИНК следует удержаться от «облачных мечтаний». Автор посетил не одну сотню конференций и форумов по информационной безопасности (в т. ч. знаменитый «КОМТЕК» 1991 года, на открытие которого в Москву приезжал легендарный Питер Нортон), но среди всех «заоблачных» высказываний наиболее запомнилось остроумное сравнение одного из спикеров очередной «облачной конференции»: «Представьте, что Вы собрали все ценности в Вашем доме, вынесли их и положили в почтовый ящик! Вы хорошо будете ночью спать, зная, что в почтовом ящике лежат все Ваши ценные вещи?» И проблема не только в уровне защиты и не в степени подготовки кадров: проблема глубже – она в информационной культуре. И современная культура потребления результатов интеллектуальной деятельной, в т. ч. в сфере информационной безопасности, формирует предпосылки для постепенного усложнения ситуации. Судите сами: экспоненциальный рост объемов информационных массивов (сродни третьему уровню КИС ВИНК) приводит к опережающему развитию носителей большего объема и скорости передачи данных. Их удешевление возможно при унификации стандартов, массовости применения, насыщения новых рынков сбыта – всему тому, что снизит стоимость производства и, соответственно, простимулирует рынок на новый инновационный виток. Но массовость применения приведет к активизации конкурентов, снижению доходности и падению прибыли: как не вспомнить пример с «закладкой» в датчик скважины, информирующий конкурента о ежедневном нефтяном трафике! На третьем уровне КИС ВИНК в полной мере проявляются симптомы «болезни роста»: неравномерная акселерация разнонаправленных частей КИС ВИНК делает их наиболее уязвимыми! На этом уровне «случайно или намеренно» подброшенный вирус, спровоцированная хакерская атака будут иметь гораздо больше последствий, чем на первых двух уровнях. Авария или локальная техногенная катастрофа на одном из группы промыслов принесут гораздо больше разрушений для системы управления, нежели для объектов и субъектов управления: внезапно нарастающий информационный объем о нештатной ситуации перегрузит систему и заблокирует ее часть, сделав неспособной адекватную реакцию в наиболее важный период времени начала развития. Теория с построением системы «гладких» математических моделей на деле существенно разнится с практикой эксплуатации родившейся, живой, постоянно развивающейся и «глубоко дышащей» системы, неравномерно растущей и поэтому постоянно нуждающейся в чутком контроле «вездесущего сисадмина» [4].

Четвертый уровень КИС ВИНК – это КИС дочерней компании ВИНК. К нагрузкам трех предыдущих уровней добавляются текущие задачи выполнения планов, отработки ключевых показателей (пресловутый KPI), взаимодействия с центром (штаб-квартирой, главный офис, Правление) и выездом «на места». Традиционно принято называть «центром управления» работы высший уровень (что логично и справедливо), но по сути «центрами» являются КИС дочерних компаний ВИНК. Назовем их «центрами тяжести»: из физики известно, что центр тяжести всей системы определяется через центр тяжести его связанных частей. И для центра тяжести системы, и для центра тяжести любой из его частей справедлив другой физический постулат: система устойчива, если «центр тяжести не выходит за площадь опоры». Полагая часть системы также в качестве системы, состоящей, в свою очередь, из подсистем, приходим к выводу: применительно к КИС ВИНК и КИС дочерних компаний ВИНК площадью опоры являются, в т. ч., контуры финансового, экономического, промышленного, технологического (и ряда других) управления. Неоднократно поднимая «упавший сервер», автору приходилось задумываться о первопричинах «падения» и разработки методики профилактики «серверных падений». «Упал бы сервер», если бы финансовое управление позволило выделить время на обучение «нового поколения» подрастающих специалистов и профилактические работы? Состоялось бы «серверное пике», если бы экономическое управление прислушалось к настоятельным просьбам системного администратора заложить поквартальные средства на техническое оснащение? Даже не рассматриваем экстремальный случай «серверопада» в период сдачи бухгалтерской отчетности: что может компенсировать нервы, время, силы и затраты работников финансово-экономической сферы? И для промышленников, и для технологов «падение сервера» – тоже катастрофа с далеко идущими последствиями! Но с финансово-экономической и промышленно-технологической точки зрения своевременное участие в процессе регулярного придания устойчивости «серверной крепости» – не обременительная дань, а разумная необходимость! Следствием падения является временная частичная или полная утрата вычислительных ресурсов и производственных мощностей с нарастанием угроз для информационной безопасности подразделению, предприятию, корпорации!

Пятый уровень КИС ВИНК – КИС группы дочерних компаний (дивизиона). Дивизионная КИС ВИНК в чем-то по функциям схожа с АСУ управления вооруженных сил дивизии: ставятся задачи, в т. ч. управления крупным войсковым соединением, развития и прокладки коммуникаций, разверты-

вания наступления, захвата и удержания плацдармов и, конечно же, обеспечения информационной безопасности от отдельного взвода, роты, полка, батальона до инфраструктурного подразделения – дивизии! В КИС ВИНК приоритеты сугубо гражданские: защищенные от взлома информационно-коммуникационные системы, связь с дочерними предприятиями, группой скважин, кустом скважин, каждой скважиной – до конкретного исполнителя! Развертывание наступления для дивизионной КИС ВИНК – это агрессивная маркетинговая политика с завоеванием и отстаиванием новых рынков сбыта. Задача пятого уровня – подготовка «к стыковке» с верхними эшелонами управления ВИНК, устранение противоречий в протоколах и административно-управленческих функциях, сшивка разнородных управленческих систем и интеграция данных.

Шестой уровень КИС ВИНК – КИС департаментов ВИНК. На этом этапе четко прослеживается нарастающая плотность потоков данных «с историей», от скважины, куста скважин, группы кустов, группы промыслов до дочерних компаний ВИНК. Значительно расширяется структура информационных потоков, они диверсифицируются: для поддержания наполнения потоками системы в дополнение к технологиям OLAP и OLTP для мониторинга состояния изделия (в нашем случае – выкачанной из скважины нефти) подключаются технологии непрерывной поддержки жизненного цикла (Continuous Acquisition and Life-cycle Support, CALS). Три типа систем в КИС ВИНК отражают три подхода обработки информации и обеспечения ее безопасности: оперативной аналитической, оперативно-транзакционной и поддержки «продукционного цикла». В нашем случае продукцией является нефть, выкачанная из скважины, куста скважин, группы кустов, группы промыслов, дочерней компании. На пятом уровне построение OLAP-кубов осуществляется медленнее, чем на нижних уровнях, но объединяется информация из разных источников, передаваемых с разной скоростью из различных регионов в зависимости от степени доступности.

Верх семиуровневой КИС ВИНК – КИС Правления ВИНК. Здесь самый высокий статус у проработанности информационных массивов, поэтому выше и ответственность за распределенное хранение. Помимо диверсифицированных систем защиты, применяемых на различных участках КИС ВИНК, поддержку бесперебойному функционированию оказывают репозиторные комплексы. Энергетическое обеспечение оказывают системы тройного резервирования на каждом участке КИС Правления ВИНК с возможностью перекрестной поддержки и целевой переброски мощностей. Высокая скорость вычислений ориентирована на применение суперкомпьютеров и квантовых компьютеров [5], наряду с обычными вычислительными системами. С течением времени, по мере модернизации КИС Правления ВИНК, проводится регулярное обновление программного обеспечения, разработанного с применением технологий компьютерного проектирования программных систем (Computer-Aided Software Engineering, CASE). В КИС Правления ВИНК CALS, CASE, OLAP и OLTP наряду с другими технологиями обеспечивают не только финансово-экономическую, промышленно-технологическую и информационную безопасность [6], но и взаимоувязанное и согласованное развитие как всей КИС, так и ВИНК.

ВЫВОДЫ

1. Современный системный администратор – не только высококвалифицированный «системщик», но и мудрый управленец, дальновидный финансист, прогнозирующий экономист, реалист-промышленник и инноватор-технолог. Пусть и этот перечень не является исчерпывающим и полным, но стабильное функционирование и успешное развитие современного предприятия (не только ВИНК, но и в других отраслях!) зависит от ряда ключевых позиций в компании. Информационная и промышленная безопасность, взаимодействие с филиалами, стратегическое развитие системы, предприятия, компании и всей отрасли и многое другое – в сфере компетенции «сисадмина», регулярно решающего множество текущих и периодически нарастающих проблем и задач [7].
2. В июле 2017 года в Москве состоялся Международный форум по квантовым компьютерам, на котором были представлены результаты создания квантового компьютера, разработанного за рубежом фирмой «D-Wave Systems» (Канада). Компьютер стоимостью порядка 12 млн долларов США уже в течение ряда лет эксплуатируется в NASA и используется для решения ряда специальных задач. Согласно данным открытых информационных источников, скорость квантовых компьютеров на 3 порядка (по экспертным оценкам, в 3600 раз) превосходит скорость работы современных вычислительных систем, что существенно ограничивает применимость традиционных криптографических методов защиты данных. Значительно повысить устойчивость [8, 9] уровень защиты КИС ВИНК и КИС других компаний может система обеспечения информационной безопасности, основанная на инновационных принципах компьютерной стеганографии [10, 11].

ЛИТЕРАТУРА

1. *Конявский В. А., Лопаткин С. В. Компьютерная преступность. В 2-х томах. М.: РФК-Имидж Лаб, 2006.*
2. *Бетелин В. Б. Суперкомпьютерные технологии в России: состояние и проблемы развития // Вестник Российской академии наук. Т. 85, № 11. 2015. С. 971-975.*
3. *Четверушкин Б. Н., Кулешов А. А., Савенков Е. Б. Проблемы применения методов математического моделирования с использованием суперкомпьютеров для решения задач нефтедобычи // Нефтегазопромысловый инжиниринг. Специальный выпуск № 9: Прогноз-2014. С. 26-35.*
4. *Королев А. Сопровождение деятельности специализированных компаний: практический опыт // Энциклопедия российской секьюритизации – 2017. СПб.: Любавич, 2017. С. 147-151.*
5. *Цуканов А. В. Зарядовые кубиты на полупроводниковых квантовых точках в механических резонаторах: управление фотонными процессами // Труды Физико-технологического института. Т. 26: Квантовые компьютеры, микро- и наноэлектроника: физика, технология, диагностика и моделирование. М.: Наука, 2017. С. 30-54.*
6. *Давыдов А. Е., Максимов Р. В., Савицкий О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. М.: Воентелеком, 2017.*
7. *Старостина Е. Дефицит профильных специалистов в сфере кибербезопасности негативно сказывается на работе бизнеса и госструктур // Информационная безопасность. 2018. № 1. С. 12-15.*
8. *Горелик А. Л., Раткин Л. С. Об устойчивости корпоративных информационных сетей // Вопросы оборонной техники. 2003. № 2 (315). С. 43-45.*
9. *Раткин Л. С. Инновационные принципы защиты промышленных информационных систем на основе комбинирования криптографических и стеганографических методов // Промышленная политика в Российской Федерации. 2005. № 9. С. 13-19.*
10. *Раткин Л. С. Применение компьютерной стеганографии при проектировании информационных систем по оборонной продукции корпоративного уровня // Вопросы оборонной техники. 2004. № 4.*
11. *Раткин Л. С. Патент на изобретение № 2322693.*