# Защита

Ведущая темы
Наталия КИЙ

ждет ваших комментариев
в своем блоге на
www.iksmedia.ru

Информационная безопасность – хит современного российского ИТ-рынка. В вузах растет набор на факультеты безопасности. Компании-безопасники рады попасть на любой журналистский крючок, даже без калорийной наживки. «Безопасные» конференции размножаются делением, чему мы станем свидетелями этой осенью. Безопасность становится не только корпоративной заботой операторов связи, как любой компании, но и – медленно и порой неуклюже – услугой на массовом рынке. Информатизирующиеся государственные органы обеспокоились собственной защищенностью и так подняли градус внимания к сфере ИБ, что и у нас теперь требования регуляторов квалифицируются как одна из угроз безопасности.

Даже за прошлый кризисный год так называемый открытый рынок ИБ вырос на 2%, до $561 млн, а с учетом скрытой в ИТ-бюджетах части – более $1 млрд (данные Leta-IT Company). Рост небольшой, но на фоне ухода ИТ в серьезный минус и снижения всего сектора ИКТ на 2% – приметный. Авторы того же исследования прогнозируют, что в ближайшие два года российский рынок инфобезопасности будет расти на 8–12%.

Передовой отряд российского рынка ИБ – безопасность корпоративная – переживает качественные изменения (на фоне количественных кризисных), с ростом зрелости потребителей превращаясь из периферийной и утилитарной ИТ-задачки в составляющую бизнес-процессов и бизнеса в целом. Векторы движения известны: от фрагментарности – к системности, от частных точечных решений – к комплексным концепциям, от изолированных и слабо интегрированных систем – к интегрированным мультивендорским.

Цена вопроса здесь измеряется не только в рублях, а иногда и в статьях Уголовного кодекса. Порой приходится платить репутацией или даже самим бизнесом.



# по-корпоративному

фокус

# На корпоративных рубежах обороны

**В общем виде задачи обеспечения информационной безопасности в корпоративных сетях можно условно разделить на экономические, связанные в первую очередь с затратами на ИБ, организационные (отслеживание изменений в законодательстве и соблюдение регламентов) и технические. Какова сегодня ситуация на этом рынке?**

**Дмитрий ЗАХАРЕНКО,** начальник отдела систем информационной безопасности Корпорации ЮНИ

## Кризис ослабил «подпитку» безопасности

В 2008–2009 гг. российский рынок средств информационной безопасности, как и большая часть мировой экономики, переживал кризис. Значительно уменьшились расходы на ИБ, часть проектов была заморожена либо отменена вовсе, основной задачей компаний было перераспределение ограниченных бюджетов на поддержание работоспособности целевых информационных систем. В результате существующие системы обеспечения ИБ хотя и продолжают функционировать, но либо не получают должного сервисного обслуживания, либо остались совсем без поддержки. Сокращение финансирования во многих организациях привело и к сокращению обслуживающих бизнес структур, в том числе и ИТ. Было уменьшено количество плановых мероприятий по развитию и модернизации систем ИБ, скорректирован численный и функциональный штатный состав. Оборудование физически и морально устаревает, «проходят мимо» новые версии программного обеспечения, появляются новые уязвимости.

Актуализировать уровень работающих систем зачастую непростая задача, так как при возобновлении сервисного обслуживания многие производители начисляют штрафные санкции за тот период, пока система не обслуживалась. Аппаратные средства защиты, обновление которых было запланировано, но своевременно не проведено, теперь уже сняты с производства или компоненты для них стали недоступны.

## Создаем проблемы – ищем решения

Необходимость привести информационные системы персональных данных в соответствие с требованиями Федерального закона № 152 «О персональных данных» стала в период кризиса дополнительной нагрузкой для предприятий всех вертикальных рынков, вне зависимости от их масштаба (см. подробнее «ИКС» № 7-8'2010, с. 58 и № 9, → см. с. 53. – *Прим. ред.*).

Ориентируясь на регламентирующие документы, одни компании начали самостоятельно пересматривать свою стратегию построения ИБ, другие попытались консолидировать усилия в рамках разработки отраслевой стратегии исполнения требований ФЗ-152. Но ситуация осложняется тем, что регламентирующие документы не дают ответов на все вопросы, а также сами постоянно изменяются. Использование сертифицированных средств ИБ затрудняется небольшим их выбором, а зарубежные аналоги часто не имеют необходимых сертификатов. Если же система ИБ в компании уже построена, но какие-то из ее компонентов не имеют необходимых сертификатов, то переделывать ее целиком – задача практически непосильная. В этом случае основная надежда либо на производителей, которые с выходом закона «О персональных данных» оза-

ботились вопросом сертификации своей продукции, либо на поправки к закону, которые могут дать большую свободу выбора. Возможным выходом также может стать снижение класса персональных данных.

Важным шагом в выявлении проблемных точек в системе информационной безопасности является аудит на соответствие определенным стандартам (ISO 27001, Стандарт Банка России СТО БР, ГОСТ Р, PCI DSS и т.д.). Это может быть внутренний аудит, проводящийся силами штатного персонала, или аудит, выполняемый независимыми специалистами. Основная его задача – объективный анализ всего комплекса мер (организационных, программно-технических, технологических), принятых в компании для обеспечения информационной безопасности, и оценка их адекватности поставленным целям и задачам бизнеса. Основной итог аудита ИБ – оценка и уменьшение операционных рисков. С одной стороны, аудит информационной безопасности дает ответ на вопросы, каково реальное положение дел в организации, что угрожает ее нормальной деятельности, насколько эффективны применяемые меры защиты. С другой – позволяет сделать верное технико-экономическое обоснование для внедрения необходимых мер защиты, спрогнозировать бюджет ИТ- и ИБ-подразделений, который потребуется для поддержания необходимого уровня безопасности.

Аудит информационных систем персональных данных обычно является первым шагом в планировании мероприятий по защите персональных данных. В рамках аудита определяется класс и уточняется перечень подлежащих защите персональных данных, производится анализ текущего состояния ИСПДн, составляется список необходимых организационно-распорядительных документов и т.д. Таким образом, проведение аудита позволяет максимально сократить затраты на последующих этапах создания ИСПДн.

С 1 января 2010 г. российская таможня изменила порядок ввоза шифровальных (криптографических) средств, и теперь для ввоза устройств, содержащих алгоритмы шифрования, требуется получать специальную нотификацию в Центре по лицензированию, сертификации и защите государственной тайны ФСБ России. Необходимость следовать особым таможенным правилам при ввозе оборудования, содержащего алгоритмы шифрования, существовала и раньше, но исполнялись эти требования очень выборочно. Сегодня же для оборудования, содержащего «слабое» шифрование, нотификации постепенно выдаются, а вот с «сильным» (строгим) шифрованием ситуация сложнее. ФСБ ратует за использование на территории России отечественной криптографии (ГОСТ), поэтому получение нотификаций для строгого шифрования сильно затруднено. Причем, если раньше это затрагивало в основном госучреждения, то теперь касается всех компаний. Будем надеяться, что в ближайшее время ситуация изменится, и шифровальное оборудование вновь будет доступно для ввоза в Россию. Иначе придется глобально пересматривать подход к организации VPN-каналов в пользу отечественных решений.

## Что ни день – новые риски

В системе защиты корпоративной сети со временем возникают новые проблемы, хотя и старые не теряют своей актуальности. Например, на клиентских машинах, помимо антивируса, зачастую необходимо развернуть целый эшелон систем защиты – персональный межсетевой экран, модуль VPN, системы шифрования данных, контроля портов, мониторинга запускаемых приложений. Количество возможных угроз и систем, способных им противодействовать, все время растет, и это многообразие серьезно затрудняет внедрение новых систем. Использование продуктов разных производителей влечет за собой усложнение системы управления и процесса интеграции этих продуктов. Выходом из подобной ситуации может стать обращение к производителю, который предоставляет полный спектр решений в области ИБ. Это позволит сократить расходы на переподготовку ИТ-кадров и ускорит накопление опыта эксплуатации.

> Обучение администраторов – не менее важная статья расходов, чем сервисное обслуживание

Часто проблемы с безопасностью в корпоративных сетях вызваны некорректной настройкой систем защиты. Даже если систему проектировали и настраивали квалифицированные инженеры компании-интегратора, то в ходе ее эксплуатации администратором, не имеющим достаточных знаний и опыта, эффективность защиты может значительно снизиться. Подобные проблемы могут возникать и при переходе от одной версии системы к другой, особенно после длительного временного перерыва и существенного изменения системы. Все это говорит о том, что обучение администраторов – не менее важная статья расходов, чем сервисное обслуживание. Все внедряемые в компании ИБ-решения должны обслуживаться квалифицированным инженерным персоналом.

Наряду с вероятностью снижения уровня знаний специалистов в области информационной безопасности нельзя сбрасывать со счетов и риски неквалифицированного использования ресурсов сотрудниками компаний. Как известно, большое количество атак осуществляется изнутри сети. Чтобы спать спокойно, недостаточно установить межсетевой экран на периметре сети и антивирус. Для защиты информации внутри сети применяется целый комплекс инструментов:

- встроенные средства защиты в серверах приложений и базах данных;

- функционал обеспечения безопасности операционных систем;
- инфраструктура специальных сенсоров, выполняющих функцию обнаружения и предотвращения атак (IDS/IPS).

Средства автоматизации сбора, обработки и анализа информации в случае возникновения какой-либо вредоносной активности пресекают ее дальнейшее распространение и оповещают администраторов.

Одна из наиболее значимых внутренних угроз информационной безопасности – утечка данных непосредственно с компьютеров пользователей. Особенно актуальной она стала с повсеместным распространением мобильных накопителей высокой емкости с возможностью подключения через USB-порты (flash-диски, мобильные HDD-диски, телефоны и коммуникаторы). Если не установить контроль за портами рабочих станций, может произойти утечка конфиденциальной информации либо же распространение вирусов и сетевых червей, которые пользователь, может быть, сам того не зная, принес из дома. Для решения проблемы несанкционированного подключения устройств существует специализированное ПО, которое ограничивает и контролирует доступ к внешним портам компьютера. Администратор безопасности может централизованно задавать политику контроля портов рабочих станций, разрешить использование только авторизованных устройств, протоколировать обращения пользователей к устройствам. Некоторые производители подобных систем позволяют шифровать данные на сменных носителях, а доступ к зашифрованной информации ограничивать группой пользователей.

> Распространение широкополосного доступа в Интернет сделало проблему утечки конфиденциальной информации через внешние каналы связи еще острее

Утечка конфиденциальной информации может происходить не только через USB-порты, но и через внешние каналы связи. Распространение широкополосного доступа в Интернет сделало эту проблему еще острее, так как появилась техническая возможность передачи большого объема информации (например, слепка базы данных) за сравнительное небольшое время. Утечка информации может быть результатом и умышленных, и непреднамеренных действий, например отсылки электронной почты по неверному адресу. Контроль над информацией, передаваемой во внешнюю сеть, выполняется системами защиты от утечки информации (DLP-системами). Такие системы производят контекстный анализ передаваемых данных и в случае обнаружения конфиденциальной информации блокируют передачу. DLP-системы уже достаточно давно известны на рынке ИБ, и сейчас почти все ведущие производители имеют в своем портфеле решений продукты с подобным функционалом.

## Как найти иголку в стоге сена?

Комплексная система обеспечения ИБ предоставляет огромное количество информации о различных событиях, что чрезвычайно затрудняет, а то и вовсе делает невозможным своевременное выявление значимых событий безопасности и оперативное на них реагирование. Существует специализированный класс систем сбора и анализа событий (Security Event Management, SEM), собирающих и анализирующих события из журналов аудита, от телекоммуникационного оборудования, сетевых устройств, систем безопасности (межсетевых экранов, систем обнаружения и предотвращения вторжений), а также от пользовательских и серверных приложений. Основная задача SEM-решения – анализ событий ИБ и оперативная отправка уведомлений о нарушениях администратору.

Некоторые SEM-системы ориентированы в первую очередь на сбор и анализ событий от продуктов какого-либо конкретного производителя (например, Cisco MARS, Check Point Eventia), но могут использоваться и для сбора информации из разнородных источников. Таким образом, при выборе подобной системы надо ориентироваться на то, оборудование какого производителя по обеспечению ИБ установлено в компании, или же обратить внимание на универсальные системы.

Внедрение системы сбора и анализа событий безопасности дает компании целый ряд преимуществ:

- централизованное управление событиями безопасности путем объединения существующих межсетевых экранов, IDS/IPS-сенсоров и других источников данных в единую систему управления;
- высокую скорость обнаружения, расследования и реагирования на инциденты безопасности;
- возможность управлять инцидентами ИБ;
- повышение эффективности управления рисками ИБ;
- повышение уровня соответствия политикам и нормативным требованиям.

■ ■ ■

Если руководство компании не будет уделять вопросам безопасности серьезное внимание, от проблем в этой области не избавиться. Пора перестать экономить на безопасности, ведь потеря конфиденциальных данных может отразиться на репутации компании и привести к финансовым убыткам.

Госорганизациям и организациям, являющимся операторами персональных данных высокого класса, в первую очередь необходимо сосредоточиться на приведении систем ИБ в соответствие с требованиями законодательства. Сегодня и в ближайшей перспективе соответствие законодательству – ключевая тема для систем обеспечения информационной безопасности. ИКС

# Виртуализация – страшный сон отдела безопасности

**Несостоятельность классического подхода к информационной безопасности виртуальных сред очевидна. Виртуализация и облачные вычисления ставят с ног на голову традиционные представления о том, что и как нужно защищать.**

**Михаил КОНДРАШИН,**
эксперт по продуктам и сервисам Trend Micro, гендиректор ЗАО «АПЛ»

Последние годы в корпоративном секторе ИТ прошли под знаком виртуализации. Этот процесс постоянно набирает обороты, ведь, по сути, виртуализованные системы работают так же, как и традиционные, только позволяют экономить на аппаратном обеспечении, счетах за электричество и людских ресурсах.

По мнению экспертов[1], следующим этапом эволюции корпоративных ЦОДов будет переход к корпоративным «облакам» (private clouds). Виртуализованный корпоративный ЦОД предлагает вычислительные мощности как внутрикорпоративную услугу. Ключевое преимущество корпоративных облаков – это повышение эффективности работы ИТ-подразделений, которые получают в свое распоряжение вычислительные мощности, необходимые им в данный момент. Нужно только написать заявку: выделение виртуальной машины необходимой конфигурации – дело нескольких минут. При этом сохраняется возможность обеспечить соответствие корпоративным регламентам, стандартам и т.д.

Истинной революцией станет дальнейшее развитие идей виртуализации, а именно переход к облачным вычислениям в рамках концепции IaaS (Infrastructure as a Service), когда корпоративные заказчики не будут строить собственные ЦОДы, а необходимую вычислительную мощность будут брать в аренду у поставщика IaaS-услуг, т.е. произойдет перенос ЦОДов в публичные «облака».

Сегодня все перечисленные модели эволюции корпоративных ЦОДов сосуществуют с перевесом в сторону традиционных ЦОДов, хотя при нынешнем бурном росте популярности технологий виртуализации такое соотношение сил продержится недолго. Облачные сервисы пока не являются сколько-нибудь значимой платформой для построения ИТ-инфраструктуры, но и они активно развиваются и многие эксперты сходятся во мнении, что за ними будущее[2].

На каждом из этапов эта эволюция сталкивается со всевозможными препятствиями, не позволяющими предприятиям в полной мере насладиться инновационными технологиями и испытать на себе все преимущества, которые обещают облачные вычисления. При пристальном изучении трудностей, встающих на пути инновационных технологий построения ИТ-инфраструктуры, обнаруживается основной негативный аспект – информационная безопасность[3].

## Виртуальная машина ≠ физический компьютер

На раннем этапе развития технологий виртуализации основным тезисом было утверждение об эквивалентности физической и виртуальной машины (ВМ). Скорее всего, именно поэтому долгое время в ИТ-среде бытовало устойчивое мнение, что вопросы ИБ в виртуализованных средах решаются так же, как и в

[1] См. Томас Битман (Thomas Bittman), Gartner, http://blogs.gartner.com.
[2] См. Джеймс Уркухарт (James Urquhart), The three routes to cloud computing's future, CNET, март 2009.
[3] IDC Enterprise Panel, август 2008, http://blogs.idc.com.

физических. То есть традиционными средствами: антивирусами, криптографией, межсетевыми экранами, системами обнаружения и предотвращение вторжений. Однако с ростом популярности технологий виртуализации несостоятельность традиционного подхода к ИБ в применении к виртуальным средам стала очевидной. С одной стороны, использование виртуальных систем существенно сужает возможности применения традиционных средств защиты, а с другой, эксперты по безопасности выявили новый пласт угроз, специфических для современных платформ виртуализации.

Одно из основных отличий виртуальных машин от физических – наличие гипервизора, т.е. программной прослойки, которая обеспечивает эмуляцию аппаратной части компьютера, позволяя на одном физическом сервере запускать множество виртуальных. Присутствие такого компонента в архитектуре неизбежно порождает сложности при обеспечении безопасности. Во-первых, становится сомнительной возможность применения в виртуальных системах аппаратных средств защиты, например, криптографических плат расширения (ведь они проектировались без учета того, что будут использоваться одновременно несколькими ОС). Во-вторых, сам гипервизор является новой мишенью для всевозможных атак, против которых все традиционные решения бессильны.

## Гипервизор – новая цель для атаки

Только на первый взгляд гипервизор полностью спрятан от виртуальной машины. На самом деле для эффективной работы системы виртуализации необходимо обеспечить взаимодействие между ВМ и гипервизором или ВМ друг с другом. Например, такая необходимость возникает при передаче данных через буфер обмена между ВМ и внешней ОС в реализациях систем виртуализации для рабочих станций.

Обмен данных между ВМ и гипервизором не может быть реализован в рамках стандартных операций компьютера, так как гипервизор по определению все стандартные операции обрабатывает как настоящий физический компьютер. Для взаимодействия с гипервизором ВМ подготавливает данные для передачи и использует нестандартный порт ввода-вывода или несуществующую инструкцию процессора. Такая нештатная ситуация вызывает прерывание, в результате чего управление передается в гипервизор, который и обрабатывает подготовленные данные. Очевидно, что подобный механизм может содержать в себе уязвимости, а значит, им могут воспользоваться вредоносные программы. Атака позволит им получить контроль над гипервизором, но для него традиционный антивирус неприменим, а специализированные продукты защиты только начинают появляться на рынке. В качестве примера можно привести vSecurity компании Catbird.

## Превратности виртуализации

Кроме атак на гипервизор, виртуализация обладает еще рядом свойств, которые способны превратить работу отдела безопасности в страшный сон.

# Пять тактик защиты от угроз в виртуальной среде

**МИХАИЛ РОМАНОВ**, директор по развитию бизнеса Stonesoft в России и СНГ

**Сегодня многие компании активно внедряют технологии виртуализации, но специалистов по информационной безопасности, как правило, не привлекают вовсе или привлекают в последний момент. В результате в существующую систему сетевой безопасности не вносится никаких изменений, не меняются и технологии защиты. Это резко ослабляет общую защищенность корпоративной сети, поскольку не учитываются те новые угрозы, которые появились вследствие самого перевода сетевой инфраструктуры в виртуальную среду.**

По результатам последних исследований Gartner[1], более 60% виртуальных серверов, которые заменят традиционные серверные системы до 2012 г., будут менее защищены, чем заменяемые ими физические собратья.

Для снижения рисков облачных вычислений корпорация Stonesoft предлагает пять тактик, которые помогут ИТ-специалистам эффективно защититься от угроз в виртуальной среде:

1 **Используйте технологии однократной аутентификации.** Для облачной вычислительной среды характерна хаотичность доступа пользователей к различным приложениям и сервисам, вследствие чего компании могут потерять контроль над обеспечением строгой аутентификации пользователей в виртуальной среде. Чтобы уменьшить этот риск, необходимо организовать «единый вход» (Single Sign On), который позволит пользователям получать доступ к многочисленным приложениям и сервисам, единожды пройдя аутентификацию под своей учетной записью.

2 **Подумайте над обеспечением непрерывности бизнеса.** Когда большинство критически важных бизнес-данных хранятся в «облаке», простои сети или временная недоступность сервисов могут представлять серьезную проблему. Доступ к сервису «облака» должен быть всегда, даже во время технического обслуживания, что потребует применения в рамках всей сетевой инфраструктуры высокотехнологичных решений, таких, как кластеризация в режиме Active / Active, динамическая балансировка нагрузки на серверы, балансировка нагрузки между провайдерами связи и др. При этом лучше использовать технологии, штатно встроенные в сетевые решения, а не приобретать их в качестве автономных продуктов, поскольку каждое дополнительное устройство само по себе может стать точкой отказа.

[1]Исследование Addressing the Most Common Security Risks in Data Center Virtualization Projects, Gartner, январь 2010.

В первую очередь при переходе к виртуализованному ЦОДу значительно увеличивается число серверов, что неудивительно: для ввода в эксплуатацию новой машины достаточно сделать копию файла с образом подходящего сервера и «включить» его. Получается, что число охраняемых объектов постоянно меняется. Но хуже другое. Серьезную угрозу представляют образы как таковые, ведь они могут быть созданы за несколько месяцев до начала эксплуатации. Соответственно, на них и последние заплаты не установлены, и старые уязвимости не залатаны. Именно такие, «проверенные временем», уязвимости наиболее популярны у хакеров и вирусописателей.

Другая проблема – сложности при настройке межсетевых экранов. Защищаемые ими серверы не привинчены к стойке, а способны перемещаться между физическими платформами, чем охотно пользуются ИТ-специалисты, поскольку это позволяет на недостижимом ранее уровне оптимизировать производительность. В результате становится весьма непросто формировать строгую политику на межсетевом экране и отслеживать все изменения. На самом деле сложностей при обеспечении сетевой защиты еще больше. В системе виртуализации основная часть сетевого трафика проходит внутри платформы виртуализации, т.е. минуя аппаратный межсетевой экран и систему обнаружения и предотвращения вторжений. Таким образом, у скомпрометированных ВМ появляется возможность бесконтрольно атаковать соседние машины.

И это еще не всё. Такой, казалось бы, простой продукт, как традиционный корпоративный антивирус, также создает проблемы при применении его в виртуализованной среде. Типичный пример: полное сканирование всей системы. Если в корпоративной сети полное сканирование устраивают в какое-то определенное время, скажем, в обеденный перерыв или ночью, то при проверке ВМ это может привести к неприятным последствиям: если все ВМ одновременно существенно повысят потребление вычислительных ресурсов, то производительность всех сервисов всех ВМ катастрофически снизится.

## Средства защиты систем виртуализации

Очевидно, что для защиты виртуализованных сред необходимы специализированные продукты. В настоящий момент доступны такие сетевые программные решения, как Cisco Nexus 1000V Series Switches, которые позволяют подменить стандартную сетевую подсистему платформы виртуализации и обеспечить сквозное управление сетью вне зависимости от числа используемых аппаратных платформ. В этом случае появляется возможность формулировать строгие политики безопасности для каждой ВМ и не перенастраивать их при миграции ВМ между аппаратными платформами.

Другой подход к решению вопросов безопасности – использование так называемых виртуальных устройств (virtual appliance), готовых виртуальных образов систем защиты, с помощью которых можно построить за-

**3** **Обеспечьте многоуровневую защиту в виртуальной среде.** Расширение «облачной» вычислительной среды и постоянно возникающие новые угрозы требуют построения многоуровневой системы защиты как периметра, так и внутренних сетевых потоков в виртуальной среде. Для решения этой задачи рекомендуется внедрить в виртуальную инфраструктуру виртуальный межсетевой экран, обладающий интегрированными возможностями межсетевого экрана и IPS, что позволит осуществлять глубокий анализ всех уровней трафика – начиная с базового просмотра веб-страниц до анализа зашифрованного SSL-трафика. Дополнительно может быть внедрено отдельное IPS-решение для защиты от внутренних атак, направленных на получение несанкционированного доступа к «облаку», выявления фактов использования нерегламентированного или вредоносного программного обеспечения.

**4** **Обеспечьте централизованное управление.** Человеческий фактор остается одной из самых серьезных угроз безопасности, в том числе и в виртуальной среде. Для защиты виртуальных сетей компании внедряют все новые и новые сетевые устройства. При этом, с одной стороны, экспоненциально повышаются риски, обусловленные неправильным управлением и настройкой этих устройств, что в итоге снижает уровень безопасности информационной системы в целом. С другой стороны, увеличиваются эксплуатационные затраты на систему информационной безопасности, поскольку процессы управления, мониторинга и конфигурации всего конгломерата средств становятся более трудоемкими, менее организованными и хуже контролируемыми. Поэтому целесообразно использовать единую консоль управления и мониторинга для всех устройств безопасности – как физических, так виртуальных, а также связанных устройств ИТ-инфраструктуры.

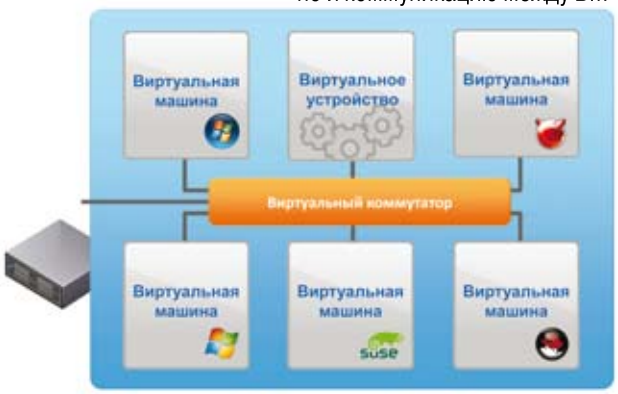
**5** **Защитите виртуальные рабочие станции.** Виртуальные рабочие места даже более уязвимы, нежели их физические аналоги. Для организации надлежащей защиты виртуальных рабочих станций рекомендуется выделить их в отдельный сетевой сегмент и постоянно инспектировать сетевой трафик в этом сегменте с целью эффективного предотвращения внутренних и внешних угроз. Для этого хорошо подходят современные IPS, предназначенные для работы в виртуальной среде и обеспечивающие многоуровневую защиту: предотвращение несанкционированного доступа изнутри, защиту удаленного доступа через IPsec, SSL и др., а также защиту клиентов от воздействия вредоносного ПО. Для защиты от несанкционированного доступа извне в виртуальной среде могут применяться многофункциональные решения SSL VPN, позволяющие задать детальные политики доступа и верификации клиента.

Грамотный подход и подключение специалиста по информационной безопасности на начальном этапе проекта по виртуализации даст возможность избежать многих ошибок и построить эффективную систему защиты в виртуальной и физической среде.

щиту на сетевом уровне непосредственно внутри среды виртуализации. Фактически подобные продукты являются полными аналогами аппаратных решений, доступных на рынке уже не один год. Виртуальное устройство представляет собой программный код, который при традиционном подходе поставляется вместе с аппаратной платформой в виде ее «прошивки». Примерами таких устройств могут служить межсетевые экраны McAfee Firewall Enterprise (Sidewinder), Kerio WinRoute Firewall, семейство продуктов StoneSoft StoneGate Firewall/VPN, Altor VF Virtual Firewall, системы предотвращения вторжений Check Point Connectra NGX Virtual Appliance, StoneGate Virtual IPS Appliance, StillSecure Strata Guard. Кроме продуктов широкого профиля, встречаются более специализированные решения, нацеленные на защиту, например, непосредственно веб-приложений, такие как Profense Web Application Firewall.

Более радикальное решение предлагала компания Third Brigade, поглощенная в прошлом году японским производителем антивирусов компанией Trend Micro. Решение Third Brigade (носящее теперь название Trend Micro Deep Security) основано на программных агентах, которые внедряются непосредственно в каждую ВМ. При таком подходе миграция ВМ не является препятствием. Все возможности Deep Security (межсетевой экран, система предотвращения вторжений, защита веб-приложений, анализ подозрительной активности в системе и пр.) обеспечиваются вне зависимости от того, где и как запущена ВМ.

Виртуальные устройства, разворачиваемые внутри системы виртуализации, позволяют защитить не только внешние по отношению к этой системе ресурсы, но и коммуникацию между ВМ




## На горизонте – облачные вычисления

Несомненно, эволюция ЦОДов на виртуализации не закончится. Следующий этап – переход к облачным вычислениям в рамках концепции IaaS. Облачные вычисления в их IaaS-ипостаси представляют собой публичные виртуальные ЦОДы, сдающие виртуальные серверы архитектуры x86 в аренду. Первопроходцами были хостинг-провайдеры, предлагавшие виртуальные Linux-серверы на основе решений Parallels Virtuozzo и им подобных. Сейчас же все чаще заходит речь о переносе в «облако» всей инфраструктуры. Разумеется, этот процесс не может идти очень активно, так как поднятые выше вопросы безопасности становятся еще острее. Более того, многие специалисты по ИБ полностью отвергают возможность перехода на облачные платформы.

При переходе к использованию услуг IaaS стирается периметр корпоративной сети и теряется контроль над всей защитой уровня гипервизора и ниже. С другой стороны, появляется неоспоримое преимущество – возможность получить «здесь и сейчас» именно ту вычислительную мощность, которая нужна, а главное, отказаться от нее в будущем, если необходимость отпадет.

Частично решить означенные проблемы способны продукты класса Deep Security, функциональность которых не зависит от того, частный ли это ЦОД или облачная инфраструктура.

Есть и другая фундаментальная проблема облачных вычислений. Это доверие, а вернее, недоверие потенциального заказчика к поставщику услуги IaaS.

Один из подходов, позволяющих безбоязненно разворачивать свои сервера в «облаке» вне зависимости от уровня доверия к поставщику, – сквозная криптографическая защита всего сервера и его транзакций. Подобную инициативу в рамках инициативы Secure Cloud уже предложила компания Trend Micro, но сейчас сложно сказать, насколько благосклонно отнесутся к этой затее заказчики.

■ ■ ■

Виртуализация не есть нечто принципиально новое для ИТ. Еще в 60-е годы XX века она была основой широко распространенной архитектуры мэйнфреймов IBM/360. Новый виток популярности этой технологии начался уже в XXI веке, когда компания VMware не пошла по пути разработки собственной виртуальной среды, подобной Java от Sun Microsystems, а создала систему эмуляции аппаратной части архитектуры x86. Именно это дало толчок развитию технологий виртуализации во всех областях ИТ. Ведь многозадачность современных ОС оставалась не востребована в полной мере. Чаще всего на предприятиях каждый сервер выполнял только одну функцию. И это несмотря на то что современные ОС способны одновременно предоставлять различные сервисы и изолировать друг от друга процессы и приложения. Именно виртуализация позволила решить всевозможные проблемы, связанные с неэффективностью сложившегося подхода.

Теперь на одном физическом сервере можно развернуть несколько ОС, но каждая будет обслуживать только одно приложение. Но вместе с очевидными преимуществами подобной архитектуры обозначилось множество проблем с обеспечением информационной безопасности. Сегодня стало очевидно, что о дальнейшем распространении данной технологии нечего и говорить без специализированных средств защиты виртуальных сред. Только последовательное внедрение таких средств даст возможность предприятиям безболезненно виртуализировать свои ЦОДы и даже частично перенести серверы в облачные среды, получив несомненные конкурентные преимущества. ИКС

# Центр безопасности оператора связи в ожидании стандартизации

**Создание системы управления сетями связи – одна из обязанностей оператора сети общего пользования. Частью такой системы является центр управления информационной безопасностью. Каким должен быть ЦУИБ?**

**Дмитрий КОСТРОВ**, директор по проектам ОАО «Мобильные ТелеСистемы»

Этот вопрос активно дискутируется и в мире, и в России. Так, Минкомсвязи в целях обсуждения разместило на своем сайте проект Требований к управлению сетями электросвязи, которые, в частности, возлагают на системы управления сетями мониторинг функционирования сети в целях прогнозирования возникновения аварийных ситуаций, в том числе связанных с разрушающими информационными воздействиями, а также координацию деятельности персонала по выявлению угроз ИБ, включая деятельность по обнаружению и ликвидации последствий компьютерных атак.

Организация непрерывного и качественного предоставления услуг связи, непрерывность бизнеса – основные задачи оператора связи. Вместе с тем число и технический уровень инцидентов безопасности постоянно растет: здесь и компьютерные инциденты в Интернете, и инфраструктурные атаки, атаки в сетях сигнализации и взломы протоколов обмена, спам, мошеннические действия и т.п. В таких условиях создание единого центра управления безопасностью становится неотложным делом.

Очевидно, что стандартизация рекомендаций и требований к созданию и функционированию ЦУИБ позволит обеспечить приемлемый уровень безопасности мировой взаимоувязанной сети связи.

При создании центра можно использовать некоторые рекомендации Национального института стандартов и технологий США (NIST), однако они не направлены собственно на операторов связи.

Напомним, что на Всемирном саммите по вопросам развития информационного общества (WSIS) и Полномочной конференции (Plenipotentiary Conference) 2006 г. определена фундаментальная роль МСЭ – построение конфиденциальных и безопасных ИКТ. Учитывая, что МСЭ-Т разрабатывает стандарты для операторов связи (например, X.1051, X.1056), можно предположить, что в рамках МСЭ и будет создан нужный документ.

МСЭ-Т уже выпустил рекомендации по некоторым проблемам информационной безопасности: E.409 “Incident organization and security incident handling: Guidelines for telecommunication organizations” и X.1056 “Security incident management guidelines for telecommunications organizations”. Однако предложения по созданию CERT/CSIRT[1], а также рекомендация X.1056, посвященная ISIRT[2], описывают только часть проблем с безопасностью ИКТ. Для целого ряда вопросов рекомендации пока не разработаны.

## ЦУИБ: определяем круг задач

Обеспечение безопасности оператора связи не ограничивается проблемами, вызванными компьютерными инцидентами. Необходимо предпринимать ком-

[1]CERT (Computer Emergency Response Team)/CSIRT (Computer Security Incident Response Team) – центр реагирования на компьютерные инциденты. Основная задача центра – снижение уровня угроз информационной безопасности для интернет-пользователей. С этой целью он оказывает содействие юридическим и физическим лицам при выявлении, предупреждении и пресечении противоправной деятельности. Осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак.

[2]ISIRT (Information Security Incident Response Team) – это команда подготовленных и доверенных специалистов, которая может управлять инцидентами безопасности. К разбору компьютерных инцидентов данная команда может привлекать других специалистов.

плексные действия по созданию систем в защищенной архитектуре; работе взаимосвязанных сетей при чрезвычайных ситуациях и стихийных бедствиях; гарантированию непрерывности бизнеса (business continuity and disaster recovery plan) и т.п. Одной из новых проблем ИБ, с которой столкнулись операторы связи при отказе от «закрытой» модели сети сигнализации, являются DDoS-атаки. Также регистрируются многочисленные новые инциденты, например, техническое мошенничество (фрод) в сетях фиксированной и мобильной связи.

Создание защищенной системы передачи информации, киберсекьюрити, защита от фрода, безопасное взаимодействие, сбор и обмен лучшими практиками – вот неполный перечень задач, которые должен решать ЦУИБ.

Основной задачей ЦУИБ оператора связи является мониторинг состояния (обеспечения) ИБ, своевременное обнаружение и эффективное разрешение инцидентов ИБ, анализ событий ИБ и эффективности используемых средств защиты с целью предотвращения новых инцидентов. ЦУИБ реализуется с помощью тесно взаимосвязанных и логично дополняющих друг друга систем: системы управления событиями ИБ; системы аудита действий пользователей; системы управления инцидентами ИБ; системы управления уязвимостями и контроля соответствий. Оператор может создать у себя отдельный ЦУИБ либо делегировать данные функции центру управления сетью или службе безопасности.

Каждый оператор связи должен нести ответственность за поддержку общего уровня информационно-телекоммуникационной безопасности как внутри страны, так и при межнациональном обмене.

Такой подход ориентирован на интеграцию основных направлений обеспечения безопасности (архитектура, управление, взаимодействие и т.д.) и основных тенденций IP-перестройки (трансформация сети связи общего пользования в сервисную инфраструктуру общего пользования, в которой Интернет является частью приложений).

Общеизвестно, что уровень готовности к реагированию на угрозы информационно-телекоммуникационной безопасности по-прежнему низок. Ранее при построении сетей связи действовал принцип обособленности, т.е. считалось, что национальная сеть (например, сеть сигнализации SS7) отделена от других. Сейчас уже не говорят о национальных сетях связи и их замкнутости – сети объединились. Однако при высоком уровне взаимосвязанности сетей резко повышается опасность нарушения качества предоставления услуг из-за роста количества и уровня сложности атак, исходящих из сетей, наименее подготовленных к обеспечению защиты.

Поэтому очень важна агрегация проблем, связанных с обеспечением информационно-телекоммуникационной безопасности сетей связи общего пользования, а также их решений (лучших практик снижения рисков безопасности) на национальном уровне. Она не может выполняться на уровне одного оператора и/или объединения/ассоциации. Это задача национального и международного масштаба.

Обычно центрам рекомендуется вести собственную электронную «базу знаний» об угрозах и методах защиты (с учетом национальных нормативных актов в части защиты конфиденциальной информации). Предлагаемая архитектура данной базы – клиент-серверная, с применением «тонких» клиентов со встроенной криптографической защитой. А вот облачное хранение данных (data-Storage-as-a-Service, dSaaS, хранилище как сервис) использовать не рекомендуется.

## А как у них?

В США и Японии основной «боевой» единицей обеспечения информационной безопасности операторов связи являются CSIRT. Такие центры формируются специалистами для предотвращения инцидентов, управления ими и выработки лучших практик в области компьютерной безопасности.

Первый центр реагирования на компьютерные инциденты – CERT – был создан в 1988 г. в ответ на появление первого вируса (интернет-червя). С тех пор количество зарегистрированных в системе DNS интернет-хостов увеличилось на порядки, превысив 200 млн, и стало ясно, что одним центром не обойтись. Но поскольку название CERT является торговым знаком, сегодня такие организации используют наименование CIRT (Computer Incident Response Team).

Правительство США поддерживает создание CIRT с помощью целого ряда как собственных, так и международных документов. В их числе:

- **Закон Сарбейнса-Оксли** (Sarbanes-Oxley Act of 2002). Устанавливает строгую ответственность за нарушение (уничтожение) электронных записей – штраф до $25 млн и до 20 лет тюремного заключения.
- **Стандарт ISO 17799.** Описывает процедуры внутренних расследований и управления инцидентами ИБ, а также процесс обеспечения управления и сохранения компьютерных записей (доказательств).
- Некоторые штаты имеют тщательно прописанные законы (подзаконные акты) об управлении инцидентами. Пример: Калифорния, **акт SB 1386/ Civil Code 1798.82.**

CIRT обеспечивают анализ инцидентов, защиту от них, восстановление после обнаруженного инцидента, координацию действий и т.п. Направления деятельности CIRT можно разделить на три большие группы: реактивный сервис, проактивный сервис и сервис управления безопасностью. В дополнение к расследованию компьютерных инцидентов CIRT могут осуществлять управление уязвимостями, применять системы обнаружения вторжений (IDS) и т.д.

Работа CIRT строится по одной из двух широко известных моделей: CERT/CC либо NIST/SANS.

**Модель CERT/CC.** Требует от компаний разработки стратегии и процессов управления инцидентами компьютерной безопасности и их предотвращения. Эти

процессы делятся на четыре категории: защита, детектирование (IDS\IPS\MOM), сортировка, ответные действия. Процессы управления должны опираться на безопасную и устойчивую инфраструктуру ИБ, которая поддерживается в рабочем состоянии и постоянно усовершенствуется.

**Модель NIST/SANS.** Применяется в различных департаментах правительства США и описывает шесть важных процессов (шагов): подготовку, идентификацию, локализацию и сдерживание, уничтожение, восстановление и отслеживание.

| Что же делает CIRT? | Выгоды создания CIRT: |
|---|---|
| ✓ Становится «мозгом» по координации и управлению любыми инцидентами безопасности.<br>✓ Выявляет уязвимости и управляет процессом их исправления.<br>✓ Сотрудничает с другими центрами (CIRT, CERT/CC или FIRST) для расследования инцидентов и снижения рисков ИБ.<br>✓ Составляет и поддерживает базу данных инцидентов.<br>✓ Готовит материалы для повышения осведомленности по вопросам ИБ. | ✓ Систематическое расследование инцидентов.<br>✓ Помощь организациям в быстром восстановлении компьютерных сетей после обнаружения инцидентов компьютерной безопасности с минимальными потерями информации и сервисов.<br>✓ Использование опыта расследования инцидентов для усиления существующих CIRT и взаимодействие с другими центрами.<br>✓ Работа в правовом поле страны. |

## Модели создания CIRT

CIRT создается исходя из ответов на вопросы: «что мы делаем?», «кто в нас нуждается?», «какие первые шаги мы должны делать?», «как взаимодействовать?» и т.п. В организациях CIRT обычно является частью департамента безопасности. В небольших компаниях это могут быть просто несколько специалистов в области ИБ.

Группа по расследованию инцидентов должна иметь возможность полного контакта со всеми, кто занят проблемами ИБ. Существует три модели создания CIRT.

1. Централизованная (Central Response Team). Это команда специалистов или иной компании, действующая в пределах малой географической зоны.
2. Распределенная (Distributed Incident Response Team). Несколько команд специалистов, каждая из которых занимается расследованиями в разных логических или физических доменах предприятия.
3. Координирующая (Coordinating Team). Такая группа обеспечивает высокоуровневое руководство расследованием, она подобна национальному центру для центров безопасности операторов связи.

Эти группы могут быть заняты расследованиями все рабочее время либо частично, или же для расследований может привлекаться организация-аутсорсер. ИКС

# Базовый уровень – основа стандартизации операторов

**Базовый уровень безопасности операторов связи представляет собой минимальный набор рекомендаций. Их выполнение будет гарантировать достаточный уровень информационной безопасности коммуникационных услуг, обеспечивая при этом баланс интересов операторов, пользователей и регулятора.**

**Сергей КОТЬКАЛО,**
гендиректор ООО «Безопасные телекоммуникации»

Мировой опыт показывает высокую эффективность института добровольной сертификации при условии существования самоорганизующихся профессиональных объединений. Активная и консолидированная позиция операторов связи позволяет формировать среду их существования. Очевидно, что в перспективе требования добровольной системы сертификации станут элементами системы обязательной сертификации, целью которой будет законодательно поддержать операторское сообщество на уровне, определенном самими же операторами.

В области ИБ сетей связи стандартизация и сертификация особенно важны, поскольку внедрение новых технологий, интеграция инфраструктур сетей и растущий уровень взаимодействия операторов открывает дорогу все новым угрозам. В рамках направления «Управление информационной безопасностью сетей и систем операторов связи» в Системе добровольной сертификации «Связь-Качество» разработан нормативный документ – Требования «Базовый уровень информационной безопасности операторов связи» (далее – Базовый уровень безопасности).

Опираясь на этот документ, учитывая, какие стандарты безопасности актуальны, когда и как они должны применяться, каждый оператор может оценить состояние своей системы информационной безопасности.

Базовый уровень безопасности можно рассматривать как основу стандартизации и сертификации в области информационной безопасности сетей связи. Для операторов этот документ значительно полезнее других систем сертификации по информационной безопасности (ISO 27001, ГОСТ 15408, аттестация на соответствие требованиям безопасности информации), поскольку он ориентирован именно на деятельность операторов и обеспечение безопасности их взаимодействия и содержит ограниченный набор требований.

## Базовый уровень и реформа «Связьинвеста»

Сегодня, когда готовится реформа «Связьинвеста», Базовый уровень безопасности особенно важен. Как известно, реформа госхолдинга будет происходить в несколько этапов: консолидация МРК на базе «Ростелекома», присоединение региональных операторских компаний и объединение сотовых активов новой компании.

На каждом из этапов предполагается интеграция организационно-технических инфраструктур управления сетями связи объединяющихся операторов. Очевидно, что уровень информационной безопасности присоединяемых операторов связи сильно различается, а исходя из принципа непрерывности защиты, общий уровень ИБ новой структуры будет зависеть от уровня ИБ каждого оператора. Это требует создания механизма оценки информационной безопасности присоединяемых операторов, который обеспечил бы их взаимное доверие. Именно в качестве такого механизма целесообразно рассматривать систему сертификации операторов на соответствие требованиям Базового уровня безопасности.

Однако, чтобы этот механизм начал действовать и стал по-настоящему эффективным, нужно провести большую работу:

- уточнить и детализировать требования Базового уровня безопасности на основе лучших мировых практик (ISO 27001 и 27002, рекомендаций МСЭ и т.д.);
- выработать более строгую систему оценок и поддающихся измерению критериев;
- для обеспечения высокого качества и независимости аудита разделить функции подготовки к сертификации и ее проведения.

Опыт, который будет получен при объединении МРК на базе «Ростелекома», даст уникальную возможность для доработки и развития Базового уровня безопасности и системы сертификации. В частности, на наш взгляд, в Базовом уровне должны найти отражение повышенные требования к ИБ, обусловленные планируемым размещением акций объединенной компании на Лондонской фондовой бирже.

## Базовый уровень и централизованное управление сетью

В ближайшем будущем Базовый уровень безопасности может иметь и другие конкретные применения. Например, соответствующий ему механизм контроля может быть использован при оказании услуг связи государственным спецпользователям, в част-

ности в рамках создания системы централизованного управления (далее – СЦУ) сетью связи общего пользования (ССОП) Единой сети электросвязи РФ в чрезвычайных ситуациях и в условиях чрезвычайного положения.

Цель создания СЦУ – управление взаимодействием спецпользователей и операторов для обеспечения эффективного и надежного предоставления услуг связи для государственных нужд с необходимым уровнем информационной безопасности. СЦУ взаимодействует с центрами управления сетей операторов, входящих в ССОП и участвующих в оказании услуг спецпользователям, а также с центрами управления сетей связи специального назначения. СЦУ является распределенной иерархической системой и состоит из ряда центров управления: НЦУСС (национальный центр управления сетями связи) и ТЦУСС (территориальный центр управления сетями связи) в каждом федеральном округе.

С точки зрения предоставления услуг связи спецпользователям сети, присоединенные к СЦУ, являются ее частью, и поэтому к ним и к их системам управления, участвующим в предоставлении услуг связи спецпользователям, должны предъявляться соответствующие требования по уровню управления сетями электросвязи вообще и по обеспечению ИБ и уровню управления системами ИБ в частности. В чрезвычайных ситуациях и в условиях чрезвычайного положения сеть электросвязи должна обеспечить:

- организацию и контроль исполнения решений о приоритетном использовании ресурсов сети связи и средств связи, сохранившихся в зоне чрезвычайных ситуаций;
- мониторинг хода восстановления работоспособности сети связи и средств связи в случаях их повреждения;
- подготовку и доведение до эксплуатационного персонала оперативных решений по обеспечению дополнительно возникающих потребностей в связи для нужд государственного управления, обороны страны, безопасности государства, обеспечения правопорядка;
- взаимодействие с органами всех уровней единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций.

В рамках вклада комитета ИК-17 МСЭ-Т в развитие Резолюции 58 «Поощрение создания национальных групп реагирования на компьютерные инциденты, в частности для развивающихся стран» российская делегация на Всемирной ассамблее по стандартизации электросвязи 2008 г. предложила разработать рекомендации по созданию национальных центров безопасности сетей связи (NNSC), которые должны обеспечивать координацию усилий национального операторского сообщества в вопросах обеспечения безопасности ССОП. Защищенная передача информации, киберсекьюрити, защита от фрода, безопасное взаимодействие,

## Чего требует Базовый уровень

В разработке «Базового уровня информационной безопасности операторов связи» под эгидой АДЭ участвовала группа представителей предприятий отрасли. Авторы документа опирались на Правила системы добровольной сертификации услуг связи, средств связи и систем менеджмента качества организаций связи «Связь-Качество», утвержденные Протоколом № 1 от 23.12.2004 заседания организаторов Системы добровольной сертификации «Связь-Качество».

Соответствие рекомендациям Базового уровня означает готовность и способность оператора связи взаимодействовать с другими операторами, пользователями и правоохранительными органами с целью совместного противодействия угрозам информационной безопасности.

Выполнение всех рекомендаций может быть проверено. Проверка может осуществляться как самостоятельно оператором с последующим декларированием, так и аудиторским органом через систему подтверждения соответствия. Рекомендации могут использоваться для установления многосторонних критериев, с помощью которых оператор может оценить состояние своей сетевой и информационной безопасности.

Документ содержит требования к политикам оператора, к функциональности (техническим средствам) и к взаимодействию.

Операторам рекомендуется иметь утвержденную в соответствии с внутренними процедурами политику безопасности, основанную на лучших практиках оценки и управления рисками, отвечающую требованиям деловой деятельности и национальному законодательству. Политика безопасности должна публиковаться и доводиться до сведения персонала оператора и внешних участников (клиентов, взаимодействующих операторов, других заинтересованных лиц).

Требования к функциональности рекомендуют использовать только сертифицированные технические средства в строгом соответствии с условиями лицензионного соглашения, определяемого их изготовителем. Для доступа к управляющим функциям коммуникационного оборудования применяются персональные учетные записи. На коммуникационном оборудовании запрещается неавторизованный доступ или доступ с паролем по умолчанию к управляющим и консольным портам, управляющим или административным учетным записям любого коммуникационного оборудования и/или ПО.

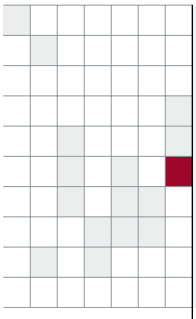
В отношении взаимодействия оператору рекомендуется иметь возможность идентифицировать клиентов и других операторов, с которыми он непосредственно взаимодействует на физическом и канальном уровнях. Также оператор должен иметь круглосуточную службу реагирования на инциденты безопасности – собственную или аутсорсинговую.

**Д. КОСТРОВ,** директор по проектам ОАО «МТС»

сбор и обмен решениями (лучшими практиками) – вот неполный перечень проблем, которые должен решать NNSC. Российский NNSC может быть построен на базе СЦУ как наиболее подходящего для этих целей института. В этом случае круг операторов связи, которые будут подключаться к СЦУ, значительно расширится и актуальность выполнения присоединенными операторами требований обеспечения безопасности повысится. Система сертификации на соответствие Базовому уровню безопасности может стать тем фундаментом, на котором будут формироваться и развиваться требования, предъявляемые к СЦУ в части информационной безопасности.

В заключение отметим, что создать эффективную систему контроля уровня информационной безопасности на основе системы сертификации на соответствие Базовому уровню безопасности можно только при деятельной поддержке как операторского сообщества, так и государства. ИКС





# Compliance как угроза

**Соответствие требованиям регуляторов – одна из основных прикладных задач обеспечения безопасности компаний и организаций различных отраслей и масштабов. Несмотря на тенденцию усиления регуляторных рисков, процесс compliance management может быть разумно встроен в систему управления ИТ и ИБ, реализованную на основе общепризнанных методик и рекомендаций.**

**Сергей ГОРДЕЙЧИК,**
технический директор
компании
Positive Technologies

Долгое время в России было принято считать отечественный рынок информационной безопасности очень жестко регулируемым и при каждом удобном случае кивать на Запад, где свободнее и проще. Глобализация привнесла в нашу жизнь элементы зарубежного регулирования, и выяснилось, что многие требования, казавшиеся сложными и затратными для исполнения, меркнут по сравнению с новыми.

В области управления соответствием требованиям регуляторов (compliance management) можно выделить **три устойчивых тренда: увеличение количества требований и регуляторов, расширение круга компаний и организаций, подпадающих под действие требований, и переход требований из разряда рекомендательных в обязательные.**

За последние несколько лет к привычным требованиям, закрепленным в российском законодательстве и контролируемым ФСТЭК и ФСБ, добавились несколько международных, государственных и отраслевых стандартов, исполнение которых во многом определяет развитие отрасли. Рассмотрим по одному наиболее яркому представителю из каждой группы.

## Стандарт PCI DSS

Стандарт безопасности информации индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard) с 2004 г. обязателен для исполнения в мире и с 2006 г. активно внедряется в России. Несмотря на то что начало применения штрафных санкций и других мер наказания за неисполнение стандартов для резидентов Российской Федерации неоднократно откладывалось, есть основания полагать, что очередной установленный Советом по безопасности PCI Security Standards Council срок (сентябрь 2010 г.[1]) больше переноситься не будет. Многие думают, что требования стандарта касаются только банков – эмитентов пластиковых карт. Это заблуждение. В той или степени положения стандарта должны соблюдать все компании, связанные с электронными платежами, начиная с финансовых организаций и заканчивая магазинами и операторами связи (мерчантами). Один из наборов требований,

[1] М. Эмм. «Защита персональных данных и требования PCI DSS», www.infosec.ru.

выделенных в стандарт PA DSS (Payment Applications Data Security Standard), относится непосредственно к разработчикам информационных систем, обслуживающих и осуществляющих транзакции с использованием платежных карт. Таким образом, стандарт PCI DSS является международным отраслевым стандартом, обязательным для исполнения большим количеством компаний. Следует отметить, что на сегодняшний день PCI DSS – один из наиболее ориентированных на практику, корректно сформулированных и процедурно выстроенных международных стандартов в области ИБ.

**Чтобы положения, заложенные в стандарты, соблюдались, они должны быть выполнимыми и не противоречить здравому смыслу и сложившейся в отрасли легитимной практике**

## Стандарт СТО БР ИББС

Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» развивается достаточно давно, но до сих пор не является обязательным для исполнения и носит рекомендательный характер. Однако тенденции последних двух лет показывают, что с высокой степенью вероятности организации кредитно-финансовой сферы примут положения стандарта в качестве основы для выполнения требований Федерального закона «О персональных данных». Это сделает его де-факто обязательным и, естественно, серьезно повысит его популярность. Учитывая, что при разработке стандарта широко использовался передовой мировой опыт в области управления ИБ, с концепцией СТО БР ИББС гармонично сочетаются процессы управления соответствием как высокоуровневым таксономиям (например, CobiT или ITIL/ITSM), так и более практическим рекомендациям уровня PCI DSS.

## Закон «О персональных данных»

Принятие Федерального закона «О персональных данных» (ФЗ-152) вызвало бурную реакцию на рынке. Особенность закона в том, что он затрагивает не какую-либо одну отрасль или индустрию, а всех субъектов, которые участвуют в обработке информации, относящейся к персональным данным. Таким образом, под действие стандартов подпало огромное количество компаний и организаций – от детских садов до транснациональных корпораций и госорганизаций. Учитывая глобальность охвата, а также наличие в законе и нормативной базе целого ряда недочетов, перенос на год срока приведения информационных систем в соответствие с требованиями законода-



# Как помочь оператору превратить защиту информации в качественную и полноценную услугу

**Екатерина ЯБЛОКОВА,** заместитель директора по развитию бизнеса Stonesoft в России, СНГ и странах Балтии

С развитием аутсорсинга на уровень ответственности оператора стали переводить и такие традиционно корпоративные задачи, как межсетевое экранирование, «очистка» трафика с помощью систем предотвращения вторжений, динамическая веб- и контентная фильтрация, аутентификация пользователей, защищенный удаленный доступ и др.

Но для того чтобы предложить потребителям эти услуги с высоким качеством и по привлекательной цене, операторам необходимо многофункциональное, гибкое и легко управляемое решение. Традиционные средства безопасности операторского уровня тяжеловесны, их эксплуатация и настройка под условия конкретного заказчика занимает много времени и ресурсов, а значит, повышается стоимость услуги и, следовательно, снижается ее привлекательность.

Попытки же унификации настроек безопасности, т.е. разбиение клиентов на предопределенные категории и использование фиксированного набора настроек приемлемым вариантом не назовешь: во-первых, это все равно требует значительных усилий, а во-вторых, не устраивает большинство заказчиков, которым необходим «персонифицированный» подход.

Компания Stonesoft давно работает на этом рынке, поэтому прекрасно понимает эти и другие проблемы операторов управляемых услуг безопасности. Предлагаемое компанией решение представляет собой унифицированную систему централизованного управления и мониторинга информационной безопасности, которая позволяет для каждого клиента организовать отдельные «домены безопасности». Каждый «домен» имеет собственных администраторов, создающих списки пользователей, открывающих доступ, организующих VPN, управляющих политиками безопасности и т.д. Глобальный администратор системы имеет полный контроль над оборудованием, сохраняя за собой право создания «доменов безопасности», их администраторов, управления интерфейсами. При этом достигается требуемая изоляция и разделение административного доступа в соответствии с иерархией ответственности. Кроме того, в такой конфигурации в качестве одного из сервисов можно предлагать заказчикам управление политикой безопасности их средств безопасности без угрозы влияния на элементы других заказчиков, что актуально для абонентов, предпочитающих держать все под контролем.

В результате внедрения такого решения оператор получает возможность быстро и эффективно реализовать на своей мультисервисной сети набор управляемых услуг в области безопасности.

реклама

тельства представляется необходимым. Однако отметим, что, несмотря на перенос, проверки соответствия проводятся регуляторами достаточно давно и зачастую заканчиваются констатацией нарушений.

Конечно, тремя обозначенными стандартами требования по защите информации не ограничиваются. Существуют привычные регулирующие документы ФСБ и ФСТЭК, такие как требования к ключевым системам информационной инфраструктуры (КСИИ), менее популярные отраслевые («Базовый уровень безопасности» РСС), корпоративные (например, серия стандартов СТО Газпром 4.2) и международные (закон Сарбейнса–Оксли, SOX) требования. Но их количество и разнообразие лишь подтверждает наметившуюся тенденцию усиления регуляторных рисков.

## Compliance как риск

Если рассматривать соответствие требованиям регуляторов с точки зрения анализа рисков, то можно провести следующее сопоставление с терминами информационной безопасности:

- угроза и ущерб – возможные последствия нарушения, обозначенные регулятором;
- уязвимость – несоблюдение требований;
- атака – проверка регулятора;
- контрмера (защитный механизм, средство защиты) – соблюдение требований.

При таком подходе возникает практически беспрецедентная ситуация: появляются все необходимые исходные данные для количественного анализа рисков на основе классической методики[2], согласно которой итоговый потенциальный ущерб равняется ARO × SLE, где ARO (Annualized Rate of Occurrence) – усредненная вероятность реализации угрозы, SLE (Single Loss Expectancy) – потенциальный ущерб от единичной реализации угрозы.

В рамках нашей аналогии:

- ARO – вероятность проверки регулятором;
- SLE – прописанные регулятором последствия нарушения.

При таких допущениях можно рассмотреть «худший сценарий» рисков, связанных с ФЗ-152. В качестве угрозы могут выступать последствия, указанные в законе и подзаконных актах:

- административная ответственность, штрафы;
- приостановление «до устранения» или прекращение обработки персональных данных в организации и вызванный этим простой или деградация бизнес-процессов;
- привлечение компании и (или) ее руководителя к уголовной (гражданско-правовой, административной или другой) ответственности – катастрофический риск;
- приостановление действия или аннулирование лицензий на основной вид деятельности компании – риск, близкий к катастрофическому.

В качестве атаки выступает проверка регуляторов. Детальные расчеты обоих показателей по отраслям деятельности и регионам можно провести на основе открытых источников, таких как план и результаты проверок[3]. Учитывая, что редкая проверка заканчивается без вынесения предписания об устранении нарушений, можно констатировать увеличение риска наступления катастрофических последствий в дальнейшем.

Законы против стандартов?

В большинстве своем требования стандартов не противоречат, а скорее дополняют друг друга. Однако встречаются и исключения из этого правила. Наиболее ярким пример – конфликт Федерального закона «О банках и банковской деятельности» и положений ряда стандартов о периодическом проведении аудита внешними органами. Противоречие обусловлено отсутствием легитимного способа передать третьей стороне сведения, составляющие банковскую тайну. Но в ходе аудита необходимость доступа к таким сведениям время от времени возникает. Также не стоит исключать возможности непреднамеренного ознакомления аудитора с банковской тайной.

Подобные коллизии достаточно редки, тем не менее на них следует обращать пристальное внимание. В некоторых случая ситуация может показаться тупиковой, и выполнение одних требований неминуемо повлечет за собой нарушение других. Но при ближайшем рассмотрении практически все противоречия могут быть разрешены на организационном уровне.

Так, описанная выше коллизия разрешается с помощью распространенного аудиторского приема, в ходе которого операции доступа к данным осуществляет сотрудник банка, а анализ обезличенных результатов производится независимой стороной[4].

## Выполнять невыполнимое?

Для того чтобы положения, заложенные в стандарты, соблюдались, они должны удовлетворять двум важным и очевидным требованиям: быть выполнимыми и не противоречить здравому смыслу и сложившейся в отрасли легитимной практике. Иначе эксперты будут настаивать на их пересмотре или повсеместно их игнорировать. Причем по молчаливому уговору требования могут игнорироваться и исполнителями, и проверяющими, и регуляторами, т.е. всеми сторонами, участвующими в процессе compliance management.

Такие ситуации не редкость (далеко не исчерпывающий их список см. в таблице). Однако в большинстве случаев проблема рано или поздно решается путем отмены или изменения формулировки требования.

Более того, многие стандарты предполагают проведение анализа рисков для определения применимости и эффективности того или иного варианта реализа-

[2] П. Покровский. «Защита информации: анализ рисков», www.ot.ru.
[3] «Персональные данные. Правоприменение», http://community.livejournal.com/personal_data.
[4] Подробнее см. Гордейчик С.В., Гордейчик А.В., Кузнецов Д.Ю. «Юридические аспекты консалтинга в области безопасности», www.ifap.ru.

Требования, игнорируемые в процессе compliance management

| Источник требования | Описание | Ситуация |
|---|---|---|
| Указ Президента РФ от 03.04.95 № 334 | Запрет использования в госорганах криптографических средств, не имеющих сертификата ФАПСИ (фактически – зарубежных криптографических алгоритмов и систем) | Игнорировалось на регулярной основе. Переформулировано в более приемлемой форме в Постановлении Правительства РФ от 29.12.07 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» |
| ФЗ-152, ст. 21, п. 3 | Необходимость уничтожения персональных данных в трехдневный срок после выявления утечки | Наиболее критикуемый в связи с бессмысленностью и практической невыполнимостью аспект закона. С большой вероятностью будет пересмотрен в следующей редакции |
| «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», методический документ ФСТЭК РФ от 15.02.08 | Необходимость применения средств защиты от побочных электромагнитных излучений и наводок для ИСПДН класса К1 | Наличие этого требования привело к широкому распространению практики перевода масштабных ИСПДН (банки, операторы связи) в класс «специальные» с целью уйти от его исполнения. В итоге «Основные мероприятия...» были заменены приказом ФСТЭК от 05.02.10 № 58, где данное требование смягчено |
| Стандарт PCI DSS, п.п. 6.3.7 и 6.6 | В одной из ранних редакций предлагалось использовать анализ исходного кода внешних веб-приложений в качестве основного механизма защиты | В связи с высокими затратами на выполнение требования его формулировка была изменена: ограничена область действия и разрешено использовать более дешевые защитные механизмы (сканеры безопасности и специализированные межсетевые экраны) |

ции требования. Исполнитель может обосновать отказ от применения или изменение типа используемой контрмеры.

## Обеспечение соответствия или обеспечение безопасности?

С момента появления требований регуляторов начал развиваться формальный подход к их выполнению. В настоящее время он приобретает все более и более изощренные формы. Один из интересных вариантов обхода требований безопасности получил название «отказ от соответствия» (Reverse Compliance)[5,6]. Суть этого подхода заключается в сознательном игнорировании ряда требований, которые могут явно продемонстрировать несоответствие. Так, отказ от внедрения системы протоколирования и анализа инцидентов позволяет закрывать глаза на реальные инциденты и атаки, скрывать многие другие несоответствия и даже дает некоторые преимущества в случае реальных инцидентов.

Иногда такой подход оправдан, но в целом требования регуляторов являются огромным подспорьем для повышения реальной защищенности. Поскольку регулятивные риски, как правило, для бизнеса совершенно прозрачны, бюджеты на их минимизацию выделяются достаточно легко. Этим периодически пользуются поставщики различных системных решений, заявляя например, о «новых массивах RAID, необходимых для выполнения требований SOX» или о «построении комплексной системы защиты персональных данных».

Дело в том, что в подавляющем большинстве случаев требования регуляторов строятся на основе передового опыта и сложившихся практик. Поэтому если система или бизнес-процессы создавались с оглядкой именно на них, то «построение» новой системы сводится к анализу и учету новых требований, документированию текущего уровня соответствия и внедрению (реорганизации) процессов и защитных механизмов, а также к адаптации процесса контроля соблюдения новых требований.

Таким образом, система управления ИТ и ИБ может строиться на основе заслуживших доверие рекомендаций, таких как COBIT, ITIL, ISO 27001, а требования регуляторов являются исходными данными для анализа рисков, организации процессов и выбора средств защиты, описанных в методиках.


Такой подход широко распространен в мире, прежде всего из-за того, что позволяет снизить издержки на обеспечение соответствия и использовать этот процесс для повышения качества ИТ-услуг и реального уровня защищенности. Более того, библиотеки взаимного соответствия стандартов (Compliance Mapping) являются одной из стандартных возможностей автоматизированных средств класса «система контроля защищенности и соответствия стандартам». Их использование позволяет достаточно просто формулировать и поддерживать в актуальном состоянии внутренние стандарты, построенные с учетом применимых требований регуляторов, и автоматизировать контроль соответствия. ИКС

[5]D. Ingram. Logs – A double-edged sword?, http://beastorbuddha.com.
[6]A. Chuvakin. Reverse Compliance or Logs as Proof of Incompetence? http://chuvakin.blogspot.com.

ПОДРОБНОСТИ

# Защищаем базы данных

**Артем МЕДВЕДЕВ,** руководитель направления безопасности БД компании «Инфосистемы Джет»

**Критичную бизнес-информацию все компании сегодня хранят в базах данных. Поэтому их защита – последний рубеж обороны корпоративной сети.**

Для обеспечения безопасности баз данных компании, как правило, используют стандартные меры (аутентификацию, авторизацию и контроль доступа), однако растущее число и сложность атак говорят о том, что эти меры более не являются достаточными для защиты критичной информации и персональных данных. Многие атаки на БД проходят незамеченными: ситуации, когда факт кражи данных обнаруживается спустя несколько недель после вторжения, отнюдь не редкость. Доступ к информации из баз данных злоумышленники в основном получают с помощью атак типа SQL-injection с использованием брешей безопасности, которые можно обнаружить на любом сервере СУБД, даже на том, где внедрены современные программные продукты. Другая серьезная угроза – внутренние пользователи, которых бывает сложно контролировать. Тем не менее на обеспечение безопасности СУБД администраторы баз данных (DBA), по некоторым оценкам, тратят менее 5% своего рабочего времени.

## Внедряем процесс обеспечения безопасности БД

Ключевой фактор успешной защиты БД – знание того, какие данные нуждаются в защите (интеллектуальная собственность, финансовая информация, данные о кредитных картах, кадровые или персональные данные) и как наилучшим образом защитить их от всех типов угроз. Для разработки процесса обеспечения безопасности БД необходимо понимать действующие стандарты, такие как PCI DSS, СТО БР ИББС-1.0 – 2006, ФЗ «О персональных данных», закон Сарбейнса-Оксли, Basel II и др. Естественно, политики безопасности БД должны быть интегрированы с общим процессом обеспечения информационной безопасности корпоративной сети.

Процесс обеспечения безопасности баз данных можно разделить на три основные направления (см. рисунок):

1. **Обеспечение базового уровня безопасности** – реализация аутентификации, авторизации и контроля доступа пользователей БД. Сюда же относится сканирование и классификация баз данных с разделением их на категории – высокой критичности, критичные и некритичные. Понимание того, какая база содержит критичную информацию, является основным требованием для построения процесса обеспечения безопасности БД. Необходимо проводить полную и регулярную инвентаризацию всех баз данных,

Основные направления обеспечения безопасности БД

включая те, которые находятся в непродуктивной зоне и используются для разработки, тестирования или обучения. Следует выработать соответствующие политики безопасности для БД каждой категории. Не менее важен процесс управления патчами и обновлениями СУБД. Специалисты по безопасности БД должны своевременно устанавливать патчи и обновления на все критические базы данных для устранения выявленных уязвимостей.

2. **Реализация ряда превентивных мер,** а именно:

- применение сетевого шифрования и шифрования архивных данных для сокрытия информации от любопытных глаз, имеющих доступ к внутренней сети компании;
- маскирование персональных данных в непродуктивных базах, используемых для разработки, тестирования и обучения, с целью предотвращения несанкционированного доступа привилегированных пользователей (разработчиков и тестировщиков ПО);
- внесение в структуру данных таких изменений, которые гарантируют, что в дальнейшем только подтвержденные и разрешенные изменения будут переноситься в продуктивную среду.

В общем случае выполнение этих мер носит рекомендательный характер, но для критичных БД является обязательным требованием.

3. **Аудит, мониторинг и оценка уязвимостей** для эффективного обнаружения вторжений. Необходимо обеспечить быстрое реагирование на незапланированные изменения критичных данных или подозрительную активность, связанную с доступом к данным. Аудит БД дает ответы на такие вопросы, как «кто изменил и какие данные?» и «когда было произведено изменение?». Мониторинг активности в базах данных позволяет оповещать о событиях информационной безопасности БД в режиме реального времени и защищать критичные данные. Отчеты с оценкой уязвимостей СУБД, таких как слабые пароли или превышение привилегий, должны дополнять данные мониторинга, которые предоставляют DBA или группа мониторинга безопасности компании.

## Базовые элементы безопасности БД

Обнаружение, классификация, авторизация, аутентификация, контроль доступа, управление обновлениями и конфигурациями – без этих функций обеспечения базового уровня безопасности БД все остальные меры будут не слишком эффективны. Независимо от типа приложения, базовые элементы безопасности гарантируют, что только авторизованные пользователи получат доступ к критичным данным через программные интерфейсы и автоматизированные процессы. Перечисленные функции поддерживают все СУБД, с их помощью данные можно хранить, использовать и обновлять достаточно безопасно, и организации должны прибегать к их возможностям как можно чаще.

**Обнаружение баз данных и их классификация.** Крупные компании в наши дни могут иметь сотни или даже тысячи баз данных, и многие из них могут содержать критичную информацию. Некоторые компании ограничиваются внедрением продвинутых мер безопасности только для баз данных, которые проверяются аудиторами, не обращая внимания на безопасность всех остальных БД. Крупные организации зачастую считают инвентаризацию БД данных слишком затратной и не знают, сколько всего баз данных есть в компании, какие из них находятся в тестовой среде, а какие в продуктивной, какие из этих баз, таблиц и кортежей содержат критичную информацию. Эта проблема обостряется при эксплуатации корпоративных приложений, плохо документированных в отношении используемых БД. Администраторам БД и сотрудникам департамента безопасности остается только догадываться, какие столбцы или таблицы им нужно защищать.

## Услуги по защите информации пора пакетировать

**Дмитрий БЫРДИН,** начальник управления безопасности Тверского филиала ОАО «ЦентрТелеком»

– Развитие технологий электронного документооборота, каналов удаленного обслуживания (таких как интернет-банкинг), постоянная потребность корпоративного сегмента в защите передаваемых по сетям данных – предпосылки для создания целого пакета услуг по защите информации.

На базе Тверского филиала ОАО «ЦентрТелеком» создан Центр компетенции по предоставлению услуг защиты информации, где разрабатываются и реализуются проекты по созданию услуг в области сетевой безопасности. В их числе аудит и консалтинг в области ИБ, поставка программного обеспечения (антивирус, антиспам, резервное копирование, очистка зараженного трафика, межсетевые экраны), создание систем защиты сетевого периметра и организация VPN-сетей, а также услуги по изготовлению и выдаче ключей электронной цифровой подписи (ЭЦП), реализуемые на базе удостоверяющего центра. Область применения ЭЦП обширна: это и предоставление отчетных документов в электронном виде (особенно актуально для госучреждений с развитой филиальной сетью), и проведение электронных торгов, и корпоративный электронный документооборот. В перспективе ЭЦП будет востребована для функционирования системы госуслуг.

## Самая большая брешь в системе безопасности – это персонал

**Павел ПЕТРОВ,** руководитель департамента консалтинга компании «Verysell Проекты»

– Именно по этой причине многие организации пренебрегают технической защитой информации: «Зачем вкладываться в комплексную безопасность, когда наибольший урон может нанести любой сотрудник с флешкой?». Статистика подтверждает – убытки от утечек информации в разы превышают убытки, причиненные вирусами, DoS-атаками и пр. Поэтому политика информационной безопасности организаций должна предусматривать комплекс мер по нейтрализации такого рода угроз.

Сегодня уже многие решения, представленные на рынке, позволяют контролировать трафик онлайн. Эффективным считается подход, основанный на хранении всей информации с последующим анализом. Есть хорошие решения, которые записывают весь трафик, проходящий через шлюзовые устройства, и работают как архив информации: можно поднять переписку любого сотрудника за все время функционирования системы, проверить, какие файлы отправлялись на печать.

Служба безопасности хорошо оценит возможность «подсматривать в замочные скважины». Не секрет, что большинство работников, планирующих смену работы, ищут вакансии на рабочем месте. Зная о «чемоданном» настроении, можно обсудить причины и устранить их либо подготовить замену, обеспечить постепенную передачу дел. Этическую сторону можно урегулировать путем соглашения с сотрудниками.

Наиболее распространенный вид утечки информации – это возможность раскрытия данных с потерянных носителей – ноутбука или флешки. Важно применять такие решения, которые не позволят воспользоваться информацией в отсутствие владельца (секретный диск, device lock).

DLP-системы позволяют контролировать не только передачу информации через сетевые протоколы, но и запись на внешние носители и даже теневые копии. На рынке представлено несколько таких продуктов российских и западных производителей (InfoWatch, Trend Micro, Symantec).

Стоимость этих решений высока, но эффективность очевидна. Даже в тех случаях, когда нет прямой окупаемости, польза от применения систем контроля трафика достаточно наглядна.

Однако надо понимать, что одним, даже «продвинутым», решением невозможно «закрыть» все проблемы информационной безопасности. Требуются усилия многих служб и целый комплекс мероприятий организационного и технического характера.

**Аутентификация и авторизация для контроля доступа к БД.** Имя пользователя в БД может быть связано с LDAP или со службой каталогов Microsoft Active Directory. Таким образом, пользователям, если они уже прошли аутентификацию, не нужно вводить свои идентификационные данные повторно. Администраторы БД должны регулярно проверять все имена пользователей в базах данных и следить, чтобы только авторизованные пользователи осуществляли доступ, деактивируя неиспользуемые учетные записи. В идеале, для того чтобы усилить разделение ролей, создавать учетные записи должна группа, отличная от DBA. Даже если пользователь приложения прошел аутентификацию и авторизацию, администратор БД должен проверить, что только активные учетные записи обращаются к каждой базе данных. Администраторы БД также не должны использовать учетные записи DBA по умолчанию. Организации должны выделять администраторам индивидуальные учетные записи и отслеживать их действия с участием специалистов по безопасности и управлению рисками.

**Контроль доступа для усиления защиты персональных данных.** Администраторы БД должны создать роли для объединения пользователей на основании их привилегий и управлять этими группами, наделяя каждую роль необходимыми привилегиями. Веб-приложения, использующие для доступа к БД единую учетную запись с администраторскими привилегиями, представляют угрозу безопасности и должны находиться под постоянным контролем.

**Контроль действий привилегированных пользователей,** таких как администраторы, разработчики, тестировщики и архитекторы. Их права и обязанности должны быть разделены таким образом, чтобы они не могли иметь полный доступ к персональным данным, а также реализовать основанную на ролях мультифакторную авторизацию.

**Управление уязвимостями и контроль обновлений.** Все версии СУБД уязвимы, и обновления безопасности обычно выпускаются ежеквартально либо по необходимости, для устранения обнаруженной уязвимости. Игнорирование обновлений безопасности серьезно снижает эффективность всех остальных мер и процедур. Установка обновлений должна проводиться регулярно, причем перед установкой любого обновления в продуктивную среду необходимо провести испытания в тестовой зоне для выявления его влияния на работу всех приложений, взаимодействующих с СУБД.

### Дополнительные меры защиты

Для обеспечения безопасности самых критичных баз данных, как продуктивных, так и непродуктивных, необходимо принять дополнительные меры.

**Шифрование баз данных, работающих в продуктивной среде.** Шифрование можно применять на двух уровнях: 1) на уровне БД, т.е. шифровать сами данные, и 2) на сетевом уровне – защищать пакеты данных, которые передаются между СУБД и другими узла-

ми, такими как пользователи или приложения. Сетевое шифрование защитит данные от злоумышленников, использующих сетевые сканеры и сниферы, а также от любопытных пользователей. Так как эти способы шифрования помогают защититься от различных типов угроз, их можно применять одновременно и независимо друг от друга.

**Маскирование данных для защиты тестовых баз данных.** Необходимо помнить, что использование копий данных о клиентах, сотрудниках или конфиденциальной информации компании для разработки или тестирования приложений противоречит закону «О персональных данных» и требованиям регуляторов.

**Внедрение процедур и регламентов контроля изменений для защиты критичных объектов СУБД.** Большинство СУБД допускают изменения структуры данных в процессе работы, причем современные СУБД позволяют совершать многие изменения без перезагрузки сервера, что означает дополнительные риски безопасности. Специалисты по безопасности БД должны контролировать выполнение процедур и регламентов внесения изменений в структуру базы данных администраторами, разрешая изменения только после согласования с руководством и убедившись, что все изменения отслеживаются. Также необходимо побеспокоиться о резервном копировании БД, чтобы иметь возможность восстановления данных в дальнейшем.

**Обнаружение аномалий и проведение регулярных проверок на уязвимости.** Регулярные проверки СУБД на уязвимости и подозрительные аномалии – важный элемент стратегии обеспечения безопасности баз данных. Данные и метаданные в БД могут быть изменены, скопированы или удалены в течение нескольких секунд. Для выполнения требований регуляторов необходимо отслеживать все изменения и доступ к персональным данным в режиме реального времени. Аномалии в поведении пользователей могут обнаруживаться с помощью мониторинга активности, аудита СУБД и оповещения о подозрительной активности. Не все записи в БД нуждаются в непрерывном аудите, но в критичных базах данных необходимо регистрировать транзакции и доступ к персональным данным. Конечно, аудит отрицательно влияет на производительность СУБД и работу приложений, но за последние несколько лет появился ряд производителей, предлагающих решения для мониторинга и аудита сторонних баз данных (Database Activity Monitoring, DAM). В России наиболее известны такие производители и продукты, как IBM Infosphere Guardium, Imperva, Embarcadero DS Auditor. Эти решения поддерживают широкий перечень версий СУБД и позволяют избежать увеличения нагрузки на них. Также существует ряд продуктов от производителей СУБД, поддерживающих свои базы данных, например Oracle Database Vault, которые эффективно решают задачи мониторинга, обнаружения аномалий и оповещений о несанкционированных транзакциях. ИКС

# Архитектура беспроводной сети должна обеспечивать выполнение политики безопасности

**Михаил ЕЛИН,**
ведущий системный архитектор Motorola Solutions

Защита беспроводной сети имеет свои особенности, определяемые тем, что эта сеть, в отличие от кабельной, неизбежно выходит за границы офиса компании – даже при использовании антенн с узкой диаграммой направленности и других ухищрениях. Методы борьбы с угрозами в беспроводных сетях в принципе хорошо развиты: система защиты может прерывать подключения, которые сочтет «вражескими», заполнять канал «неправильными» пакетами данных и т.д. Однако при использовании всех этих методов крайне важна правильная настройка политик противодействия угрозам, иначе в силу отсутствия у беспроводной сети четких границ система защиты может помешать функционированию соседних сетей, работающих на тех же каналах.

Но самая большая проблема организации сетевой защиты состоит в том, что в большинстве российских компаний политика безопасности, частью которой является политика безопасности беспроводной сети, либо отсутствует как таковая, либо не учитывает реальные риски. Поэтому сети либо вовсе не защищают под предлогом того, что «там все равно нет никакой секретной информации», либо, наоборот, стремятся оснастить сертификатами сканеры штрих-кодов на бутылках газировки. Часто в ТЗ можно увидеть требование обеспечить анализ «любого трафика в любой точке сети в реальном времени». Это можно сделать, но стоимость такого решения будет астрономической.

Сначала надо определить реальные бизнес-риски, а потом, исходя из них, сформулировать политику безопасности, которую, в свою очередь, должна обеспечивать архитектура сети. Сеть разумно разбить на области с разными уровнями безопасности: домен, где, например, идет обмен электронной почтой, должен иметь высокий уровень защиты с системой сертификации (и обеспечивать ее работу должен высококвалифицированный персонал), а в домене, обслуживающем склад, такие меры будут излишними. Нужно понимать, какие бизнес-приложения работают в сети и как их изолировать друг от друга для реализации разных уровней безопасности. Технические средства должны соответствовать политике безопасности. К сожалению, такой подход у российских заказчиков пока встречается редко. Реальные меры начинают принимать только после реально понесенных убытков, и Россия в этом смысле не исключение.

## Защита VPN-каналов – главная забота крупных компаний

**Дмитрий БУРЛАКОВ,** отдел информационной безопасности компании «Открытые Технологии»

– Почти каждой крупной компании приходится решать задачу обеспечения непрерывного защищенного информационного обмена между центральным офисом и региональными представительствами. Конечно, можно арендовать защищенные каналы связи, но, как правило, затраты на такую аренду превышают стоимость развертывания собственной VPN.

Основные средства создания VPN можно классифицировать следующим образом:

- По используемым криптоалгоритмам – либо отечественным, на базе ГОСТ 28147-89, либо импортным: DES, 3DES, AES и др.
- По уровню работы на модели OSI: на канальном или сетевом уровнях.

Приступая к построению защищенных каналов, организация должна сделать выбор криптоалгоритма и уровня модели OSI, на котором будет выполняться шифрование.

С точки зрения выбора криптоалгоритма ситуация более или менее простая: если компания государственная (или контрольный пакет ее акций принадлежит государству), то необходимо использовать сертифицированные ФСБ решения, реализующие криптографию на базе алгоритма ГОСТ 28147-89. Такое же решение придется принять, если компания обрабатывает информацию, которая в соответствии с законодательством должна защищаться сертифицированными средствами. В остальных случаях организации могут выбирать отечественные либо импортные алгоритмы шифрования на свое усмотрение.

В том, что касается уровня работы средства шифрования на модели OSI, ситуация несколько иная: у каждого из видов есть свои достоинства и недостатки. Основные преимущества шифрования трафика на канальном уровне – высокая пропускная способность и низкая задержка при передаче пакетов. К примеру, некоторые устройства канального шифрования обеспечивают скорость до 10 Гбит/с, что, скорее всего, позволит полностью удовлетворить потребности достаточно крупной компании. А при шифровании на сетевом уровне (например, IPSec) полезная пропускная способность канала неизбежно снижается (в некоторых случаях до 50% номинальной пропускной способности). К недостаткам канального шифрования можно отнести отсутствие возможности организовать VPN-соединение типа «компьютер пользователя – сеть предприятия», а также необходимость устанавливать одинаковое оборудование на обоих концах канала связи.

Средства шифрования трафика на сетевом уровне сегодня наиболее популярны, и этому немало способствовала их универсальность. Благодаря широкой распространенности стандарта IPsec компании могут строить свои виртуальные сети, используя оборудование различных производителей и в любой топологии. Платой за такую универсальность является повышенная задержка, а также рост трафика и снижение полезной пропускной способности за счет добавления служебного заголовка.

комментарий юриста

# Сколько стоит нарушение авторских прав

**Есть проблема, с которой может столкнуться абсолютно любая компания малого, среднего, а иногда и крупного бизнеса: что делать, если на предприятие пришла проверка, цель которой – выявить факты нарушения авторских прав?**

Кто, когда и на основании чего может придти в компанию проверить легальность используемого ПО?

Программное обеспечение – один из видов интеллектуальной собственности, причем ст. 1229 ГК РФ устанавливает, что правообладателю принадлежит исключительное право на использование результата интеллектуальной деятельности любым способом. Именно из этой нормы закона и вытекает необходимость лицензирования ПО: лицензия является ни чем иным как согласием (разрешением) правообладателя на использование программ. Использование же ПО без согласия правообладателя незаконно, а экземпляры незаконно используемого ПО являются контрафактными. Контрафактный экземпляр – юридическое понятие, аналогом которого в обыденной речи выступает и контрафактное ПО, и нелегальное ПО, и «левое» или «пиратское» ПО.

Незаконное использование ПО, как и любое нарушение закона, влечет за собой ту или иную ответственность.

В России в 2000 г. было выявлено 875 случаев нарушения авторских прав, а за шесть месяцев 2009 г. таких преступлений насчитывалось уже 4697. И это при том что в 2009 г. количество проверок в сравнении с 2008 г. даже немного снизилось.

### Градации ответственности

Ответственность за нарушение авторских прав можно разделить на три большие группы: административную, уголовную и гражданскую.

**Административная ответственность** за нарушение авторских прав в соответствии со ст. 7.12 Кодекса об административных правонарушениях РФ наступает в случае, если стоимость контрафактных экземпляров программ менее 50 тыс. руб. При этом стоимость конкретных экземпляров будет рассчитываться исходя из стоимости лицензий, реализуемых в рознице: за

основу берется самая высокая цена (как правило, стоимость коробочных версий).

Административная ответственность за нарушение авторских прав наступает, если последнее производится с целью получения прибыли, но это не означает, что наказан может быть только продавец нелегального ПО. Если контрафактное ПО используется коммерческой организацией в повседневной деятельности, факт извлечения прибыли отдельно доказывать не нужно, так как сама деятельность такой организации направлена на извлечение прибыли.

Совершение административного правонарушения, предусмотренного ст. 7.12 КоАП РФ, влечет относительно легкое наказание, как правило, в виде штрафа с обязательным уничтожением как носителя контрафактного ПО, так и использованного оборудования (в случае ПО таким оборудованием будет системный блок или ноутбук).

Еще один вид административного правонарушения предусмотрен ч. 2 ст. 14.33 КоАП РФ, которая устанавливает ответственность за недобросовестную конкуренцию, выражающуюся во введении в оборот товаров, работ и услуг с нарушением прав на интеллектуальную собственность. Классический случай такого правонарушения – продажа на рынке контрафактного экземпляра ПО.

Принципиальное отличие ст. 14.33 КоАП РФ от ст. 7.12 КоАП РФ – возможность наложения оборотного штрафа, т.е. такого штрафа, размер которого определяется исходя из выручки компании.

Если контрафактные экземпляры программ стоят более 50 тыс. руб., наступает **уголовная ответственность**. При этом преступление считается совершенным в крупном размере (ч. 2 ст. 146 УК РФ), если стоимость контрафактных произведений не превышает 250 тыс. руб., в противном случае преступление считается совершенным в особо крупном размере (ч. 3 ст. 146 УК РФ). Ответственность по ч. 3 ст. 146 УК РФ может также наступать, если стоимость контрафактных экземпляров составляет до 250 тыс. руб., но преступление совершено группой лиц по предварительному сговору или лицом с использованием своего служебного положения.

Преступление, предусмотренное ч. 2 ст. 146 УК РФ, относится к категории небольшой тяжести, а ч. 3 – к категории тяжких. Если максимальное наказание по ч. 2 может составить два года лишения свободы, то по ч. 3 – уже шесть лет! Однако несмотря на то что сегодня выносится гораздо больше приговоров с реальным лишением свободы, доля таких приговоров не превышает 1–2% общего числа дел по нарушению авторских прав. Как правило, суд приговаривает пиратов к условному лишению свободы и (или) штрафу в доход государства.

Необходимо отметить, что за нарушение авторских прав в зависимости от стоимости экземпляров произведений наступает или административная, или уголовная ответственность. Одновременное наступление и административной (ст. 7.12 КоАП РФ), и уголовной (ч. 2 или 3 ст. 146 УК РФ) ответственности невозможно.

При этом к административной ответственности может быть привлечен как гражданин, так и должностное лицо (например, руководитель), и сама организация. К уголовной ответственности привлекается только физическое лицо – как правило, или генеральный директор, или системный администратор (ИТ-руководитель).

Кстати, для привлечения к уголовной ответственности (в отличие от административной) совсем не обязательно иметь целью получение прибыли.

Вместе с тем, вне зависимости от наступления уголовной или административной ответственности, правообладатель может привлечь нарушителя к гражданско-правовой ответственности.

**Гражданско-правовая ответственность** выражается, как правило, в виде обязанности по выплате компенсации за нарушение авторских прав или убытков.

По общему правилу при нарушении чьих-либо прав взысканию подлежат убытки (т.е. расходы, которые лицо обязано понести для восстановления нарушенного права). Размер этих убытков доказать трудно. В связи с этим законодатель существенно упростил положение правообладателя и предоставил ему возможность взыскать убытки или компенсацию, причем последняя взыскивается в размере от 10 тыс. до 5 млн руб. по усмотрению суда или в двукратном размере стоимости экземпляров произведений при доказанности только факта нарушения авторских прав. Иными словами, для получения компенсации правообладателю достаточно доказать только факт нарушения своих прав, а размер компенсации обосновывать не нужно.

Взыскание компенсации после привлечения к административной или уголовной ответственности происходит практически «автоматом» и в большинстве случаев – в рамках уголовного процесса. Если уголовный суд по каким-то причинам не рассмотрел гражданский иск или оставил его на рассмотрение гражданского суда, то решение о взыскании компенсации с юридического лица или индивидуального предпринимателя принимает арбитражный суд.

Кроме выплаты компенсации нарушитель может быть привлечен к еще одному виду гражданско-правовой ответственности: в соответствии со ст. 1253 ГК РФ, если юридическое лицо неоднократно или грубо нарушает исключительные права на результаты интеллектуальной деятельности, суд может принять решение о ликвидации такого юридического лица по требованию прокурора. Однако практика применения этой нормы еще не сложилась и по какому пути она пойдет, сейчас предугадать сложно, поскольку закон не устанавливает, что понимается под «грубым нарушением исключительных прав» и, следовательно, практика может быть как чрезвычайно жесткой, так и чрезвычайно мягкой.

Естественно, что опасения быть привлеченным к ответственности побуждают организации приобретать легальные экземпляры ПО, но возможная юридическая ответственность – не единственная причина легализации. Другие причины таковы:

- боязнь парализации деятельности организации в случае проведения проверки правоохранительными органами и изъятия ПК и серверов;
- риски потери клиентов, вызванные неисполнением договорных обязательств из-за изъятия ПК и серверов;

- имиджевые риски – ухудшение имиджа организации и падение доверия к ней в случае привлечения генерального директора или сотрудников к уголовной ответственности;
- технологические риски, связанные с нестабильностью работы контрафактных программ, отсутствием обновлений, технической поддержки и т.п.

## К вам пришли с проверкой...

Вне зависимости от причин, побудивших организацию к легализации, такое решение нельзя не приветствовать. Но, как показывает практика, даже при использовании только легального ПО у организации остается много вопросов относительно возможных проверок, а неизвестность, как правило, порождает страхи... Давайте попытаемся их развеять.

Сама по себе проверка не является чем-то из ряда вон выходящим: при использовании легального ПО и надлежащей подготовке в организации она не займет много времени и не вызовет никаких эксцессов типа изъятия компьютеров.

В подавляющем большинстве случаев проверки проводятся сотрудниками подразделений по борьбе с экономическими преступлениями или подразделениями по борьбе с преступлениями в сфере высоких технологий (отделы или управления «К») на основании закона «Об оперативно-розыскной деятельности».

Указанный закон делит основания для проведения оперативно-розыскного мероприятия на две категории: когда уголовное дело возбуждено и когда оно не возбуждено.

В первом случае основанием для проведения проверки будет служить отдельное поручение следователя, причем оперативный уполномоченный по такому поручению может производить как оперативно-розыскные мероприятия, так и следственные действия.

Во втором случае, когда уголовное дело еще не возбуждено и оперативно-розыскные мероприятия лишь в дальнейшем дадут необходимые основания для возбуждения уголовного дела, оперативный уполномоченный действует на основании постановления о производстве оперативно-розыскного мероприятия. Такое постановление должно содержать наименование оперативно-розыскного мероприятия (или мероприятий), место его проведения и в обязательном порядке должно быть утверждено начальником криминальной милиции или подразделения, которое производит проверку.

Действия проверяющих достаточно стандартны: они предъявляют постановление о производстве оперативно-розыскного мероприятия, просят всех сотрудников отойти от компьютеров, предоставить документы, подтверждающие законность использования ПО, после чего сначала изучают ПО на компьютерах (вручную или с использованием специальных программ-сканеров), а потом – предоставленные документы. Фактическим окончанием проверки является принятие решение об изъятии компьютеров или об отказе от этого.

В проверке обязательно принимают участие понятые. Участие специалиста необязательно и оставлено на усмотрение правоохранителей. Специалистом может выступать любое незаинтересованное лицо, обладающее специальными познаниями в области компьютерной техники и использования ПО.

Даже при наличии в компании только легального программного обеспечения к проверке необходимо быть готовым. От того, насколько компания готова к проверке, зависит ее ход: если компания идет на контакт, предоставляет все необходимые документы, то и правоохранители надолго в ней не задержатся. Главная задача компании при проверке – всеми возможными путями показать законность использования ПО.

## Чтобы спать спокойно

Сведем воедино рекомендации, которые помогут компании спокойно пережить проверку.

1. Использовать только лицензионное ПО, иначе никакие схемы и задумки не помогут.
2. Провести на предприятии аудит установленного ПО, причем поручить его не своим системным администраторам, а сотрудникам сторонних организаций, которые специализируются на этом. Цель аудита – понимание того, какое ПО используется, есть ли среди него нелицензионное, чтобы в случае проведения правоохранительными органами проверки никаких неожиданностей не было.
3. При большом парке компьютеров желательно внедрить на предприятии систему управления лицензиями (software asset management).
4. При приобретении ПО сохранять все документы об этом, а также все его аксессуары (диски, коробки и т.п.).
5. Поставить приобретенное ПО на бухгалтерский учет. Для правоохранительных органов сам по себе факт постановки ПО на бухучет существенного значения не имеет и не проверяется, но такой факт – лишнее доказательство легальности ПО и является дополнительным аргументом в пользу прекращения проверки.
6. В обособленных подразделениях (филиалах, представительствах) или у аффилированных лиц иметь нотариально заверенные документы, подтверждающие законность приобретения и использования ПО.
7. Иметь на предприятии подготовленный комплект документов, подтверждающий законность использования ПО, чтобы в случае проведения проверки немедленно предоставить его проверяющим с целью избежать изъятия компьютеров.
8. Ввести строгий порядок установки программ на компьютер, ознакомить с этим порядком всех работников, разъяснив им ответственность за использование нелицензионного ПО.

**Игорь СЛАБЫХ, руководитель отдела по противодействию интеллектуальному пиратству Adobe Systems в России и СНГ**