Круглый стол:

«Информационная безопасность сегодня и завтра»

Часть вторая – решение

Участники:
Валерий Андреев — *директор по науке и развитию компании* ИВК
Алексей Бугров — *главный специалист по информационной безопасности* LETA IT-company
Александр Колыбельников — *эксперт отдела внедрения систем информационной безопасности* «Квазар-Микро»
Сергей Мишенков — *технический директор компании* АСВТ
Дмитрий Огородников — *руководитель департамента информационной безопасности* «Энвижн Груп»
Дмитрий Попович — *глава Российского представительства компании* Eset

Как организации решить, что именно и в какой степени надо защищать?

ИВК. Ущерб от недостаточной защиты очевиден, но и избыточная защита вредна. Ведь это – неоправданные немалые расходы и дополнительные неудобства для пользователя. В поисках оптимума организация должна исходить из ценности защищаемой информации и из оценки объема ресурсов, на которые может опираться атакующая сторона. Какая информация более ценна? Это – данные о финансах, это результаты ключевых технологических разработок, в которые вложены значительные ресурсы, различные ноу-хау компании, в том числе по работе с клиентами, конфиденциальная информация о клиентах и партнерах. Ясно, что несанкционированный доступ к этим сведениям серьезно угрожает самой организации. И как бы она ни выстраивала свою деятельности, как бы ни выбирала соотношение между компьютерной и некомпьютерной обработкой этих данных, важно, чтобы вся организационно-техническая система ИБ гарантировала надежную защиту этих сведений.

LETA. Наряду с защитой собственно информации важно защитить и бизнес-процессы как упорядоченную совокупность действий, связанных определенными правилами и ограничениями. Важность документа может быть обусловлена не только ценностью содержащихся в нем сведений, но и тем, что он является связкой между шагами одного или разных бизнес-процессов. Иными словами, уничтожение или искажение подобного документа способно внести хаос в упорядоченную систему действий или направить эту последовательность в нужное русло. Именно соединяя представления о ценности информации в документе со взглядом на документ как на связь между рядами действий, можно «измерить» его истинную ценность и, соответственно, выбрать необходимый уровень защиты.

NVG. Современные организации все чаще рассматривают информационную безопасность как один из инструментов, помогающих обеспечить непрерывность бизнеса. При таком подходе организация анализирует и документирует важнейшие угрозы, причем это могут быть не только информационные риски, но и угрозы, связанные с таким слабым звеном, как человеческий фактор. Затем организация разрабатывает план сохранения непрерывности бизнеса, в котором прописаны организационно-технические мероприятия, как профилактические, так и предусмотренные на случай возникновения какого-либо заранее определенного сценария развития событий. Такой документ более содержателен, чем просто реестр угроз, поскольку здесь прописана и алгоритмическая составляющая подготовки к угрозе, и варианты реагирования на ее возникновение.

АСВТ. Бизнес оператора связи опирается на постоянную обработку информации, бесперебойность и эффективность которой служат важнейшим условием успеха компании. Частично эта обработка происходит в реальном времени (например, в биллинговых системах), частично – в режиме оффлайн (например, аналитическая обработка для точной сегментации клиентской базы). И защитить исходные данные и результаты их обработки оператор должен очень серьезно. Кроме того, для оператора связи проблема выбора объектов и уровней защиты имеет дополнительные аспекты, которые становятся все более важными и сложными по мере увеличения популярности конвергентных инфокоммуникационных услуг связи, в которых участвуют услуги передачи и компьютерной обработки информации, и их взаимопроникновение рождает новое потребительское качество. В соглашении о качестве обслуживания оператор берет на себя обязательства

по определенной защите данных клиента, передаваемых по линиям связи и хранящихся на хостинг-площадках. Причем уровень защиты задается потребителем и может зависеть от множества факторов: конкретного абонента, территориальной площадки, той функции компьютерной программы, с которой работает потребитель и мн. др. Чтобы точно выполнить эти требования для каждого клиента, оператор должен располагать соответствующей технической базой, пакетом лицензий и квалификацией, иначе его система ИБ может оказаться колоссом на глиняных ногах.

Квазар-Микро. Выбирая степень защиты, современная организация должна мыслить более финансово, нежели технологически. Нарушение системы безопасности является риском, наступление которого приводит к определенным затратам. Например, утрата конфиденциальных данных о клиенте наносит урон репутации компании, и чтобы восстановить его, нужна серьезная работа, конкретное содержание которой зависит от рынка, на котором работает клиент. Продолжая эту линию, нужно учитывать, что современные компании широко используют страховые инструменты защиты от рисков. И когда защищенность информации начнет влиять на уровень ставок страхования, вот тогда руководители организаций будут уделять проблеме ИБ гораздо больше внимания, и произойдет настоящий прорыв на этом рынке.

Eset. Сегодня организации действительно наращивают свои усилия в построении систем ИБ. И эти системы становятся более эффективными. Но одновременно наращивает усилия и атакующая сторона. И если раньше организованная техническая разведка работала против государственных организаций, то теперь это в полной мере касается и коммерческих предприятий. При этом в последнее время начала проявляться новая тенденция – сбор информации о хорошо защищенной организации может быть налажен не только с помощью проникновения в ее ИС, но и с помощью сбора и анализа информации, полученной из информационных систем ее партнеров. Причем использование специальных программ-шпионов позволяет наладить получение информации из сотен источников. Т.о ., каждая организация должна оценивать важность той или иной информации, исходя не только из своих интересов, но и учитывая ущерб, который могут получить партнеры. Рост популярности новой схемы, вероятно, в скором времени приведет к значительному росту числа шпионских программ, написанных под конкретную ИС и конкретную «шпионскую» задачу. Поэтому, создавая свою систему ИБ, уже сегодня стоит продумывать соответствующие механизмы противодействия.

Можно ли надежно защитить современную территориально-распределенную информационную систему, в которой используются различные вычислительные платформы, новые и унаследованные элементы? Причем систему развивающуюся и взаимодействующую с Интернетом и с ИС других организаций? Можно ли гарантировать уровень защиты такой ИС?

NVG. Да, можно, если четко следовать требованиям ISO 27001. Стандарт регламентирует систему процессов управления информационной безопасностью, зависимость которой от размера информационной системы, конкретных платформ и средств защиты незначительна. Основной акцент в ISO 27001делается на полноту, саморегуляцию, непрерывность и периодическую оценку эффективности процессов управления информационной безопасностью. Именно эти свойства гарантируют необходимый уровень защиты любой ИС.

LETA. Можно и нужно защитить такую систему. Но не нужно изобретать велосипед. В мире существуют и активно применяются стандарты и рекомендации, на основе которых целесообразно строить свою безопасность. Это, прежде всего, серии стандартов ISO 17999и ISO 27001. На их основе вполне можно создать такую систему ИБ, в рамках которой основные риски будут минимизированы.

Квазар-Микро. Да, безусловно, можно. Для облегчения проектирования систем ИБ существует ряд рекомендаций, закрепленных в различных стандартах, как зарубежных, так и отечественных, руководствуясь которыми, можно обеспечить заказчику рекомендуемый нами или выбранный им самим уровень защиты ИС. При этом важно помнить, что построение действительно защищенной информационной системы – это постоянный мониторинг, модернизация, аудит всех ее элементов: стратегии управления рисками, вытекающей из нее архитектуры информационной системы, конкретных технологий и продуктов, применяемых в организации. Никогда нельзя останавливаться на достигнутом уровне.

ИВК. Да, такую систему защиты создать можно. Но это требует существенного пересмотра самих принципов построения информационной системы, применения иных системных архитектур и использования дополнительных системообразующих элементов. На наш взгляд, сегодня существует единственная возможность надежной защиты информационных и вычислительных ресурсов в таких ИС – реализация политики ИБ системы в целом на средствах middleware (ПО промежуточного слоя), позволяющих упорядочить информационный обмен между разнородными приложениями, объектами и пользователями ИС на основе унифицированных механизмов доступа и абонентского шифрования, механизмов предотвращения НСД на уровне конкретного информационного объекта, его функции или структурного элемента. ПО промежуточного слоя как центральный элемент ИС, по сути, предлагает прикладному ПО системы заключать своего рода «контракты» на своего рода доставку информации, на проведение логической обработки информации по заданному регламенту, на защиту информации, контроль ее целостности и подлинности, доступ к ней с учетом всех правил и ограничений и др. А реализация этих функций полностью скрыта от прикладного ПО, что обеспечивает такой системе массу преимуществ: ускорение разработки прикладных программ, централизованную взаимную привязку организационной и технической составляющих системы ИБ и др. Такой подход только

начинает применяться в России. Но наша страна уже приступила к масштабному построению крупных информационных систем на всех уровнях, и другого пути просто нет.

АСВТ. Теоретически – можно. Независимо от того, территориально-распределенная ИС или нет. При этом очень важно отказаться от стереотипного противопоставления ИТ и телекоммуникационной составляющей. Современная телекоммуникационная инфраструктура корпоративного и операторского уровней – это сложнейшие компьютеризированные комплексы, которые могут при правильном проектировании повышать защищенность, а при неправильном – создавать в системе ИБ широкие «бреши». Например, из оборудования ведущих поставщиков можно уже сегодня создавать интеллектуальную телекоммуникационную инфраструктуру, которая анализирует различные виды трафика, выявляет в нем вредоносные элементы, например компьютерные вирусы, и задействует в этом процессе уже функциональные блоки уровня ИТ. Разумеется, подключение системы к Интернету значительно расширяет спектр угроз, поэтому в действительно надежно защищенной ИС лучше вообще избежать подключения к Интернету.

Eset. Система ИБ конкретной организации может состоять из различных элементов, по разному связанных друг с другом. Все зависит от вида деятельности, угроз, отношения к ИБ и др. Но очевидно, что в таких системах должны быть брандмауэры (корпоративные, офисные, персональные и т.д.) — своего рода «фасад», и система антивирусной защиты, которая служит последним эшелоном противодействия вредоносному ПО. В крупной организации целесообразно одновременно использовать несколько видов антивирусного ПО. Это связано с тем, что если на всех узлах сети используется одна технология защиты, то, преодолев ее в одном месте, вредоносная программа беспрепятственно распространяется по всем компьютерам организации. Кстати, такой принцип построения антивирусных систем рекомендован ЦБ РФ. При выборе конкретных антивирусных программ имеет смысл внимательно оценивать совершенство проактивных методов защиты, которые, собственно, и противостоят еще невыявленному вредоносному ПО, в том числе написанному под конкретную организацию. Организации не менее важно обезопасить себя от всех видов вредоносного ПО, поскольку его разнообразие быстро растет. Важно также постараться одинаково эффективно защитить все используемые вычислительные платформы.

Какое влияние оказывает технический прогресс в сферах ИТ и телеком на системы ИБ?

NVG. Технический прогресс как процесс, в ходе которого появляются новые технологии, новые услуги и новые сервисы, конечно же, оказывает влияние и на системы защиты информации, использующиеся в сетях операторов связи и корпоративных сетях. Следом за появлением новых услуг и сервисов не медлят с появлением и новые угрозы, что, в свою очередь, стимулирует разработчиков выпускать новые решения по защите от этих угроз. Так, например, массовое использование сегодня wi-fi является неоспоримым удобством для сотрудников и гостей офисов, бизнес-центров и отелей, поскольку обеспечивает мобильность и возможность «быть на связи» в любой точке мире. Вместе с тем, подобные нововведения несут в себе угрозы безопасности, которые не рассматривались ранее производителями средств защиты. Но в целом могу отметить, что рынок средств ИБ достаточно динамично реагирует на изменения угроз и оперативно выпускает соответствующие защитные решения.

АСВТ. С одной стороны, системы защиты становятся все сложнее и надежнее, с другой – информация становится более доступной (совершенствуются методы ее перехвата как в радио, так и в «проводных» технологиях). Информация может быть закодирована и защищена разными способами и считаться защищенной, но необходимо помнить, что ее всегда можно «снять». Разумеется, нельзя защищать только компьютерные системы. Не менее важна защита телефонных сетей, переговорных комнат, а также проведение всего комплекса организационно-технических мероприятий по созданию зон безопасности различного уровня внутри офисных зданий, по организации защищенных коммуникационных каналов. Поскольку информация от источника до потребителя проходит, как правило, через сети нескольких операторов связи, необходимо знать технические возможности оператора по защите каналов и наличие у них соответствующих лицензий.

ИВК. Технический прогресс ведет к конвергенции средств ИБ и созданию интегрированных многофункциональных комплексов ИБ. Кроме того, совершенствуются средства защиты, встроенные в операционную систему и различные виды инфраструктурного ПО, например, в СУБД. Естественно, развитие этих продуктов не ограничивается только совершенствованием составляющей, связанной с ИБ. Появляются новые функциональные возможности, привлекательные для пользователей и разработчиков ПО. Именно поэтому постоянно сокращается период обновления версий ПО. Т.о ., постоянные изменения – это норма жизни информационной системы. И система ИБ должна это учитывать Я считаю, что только использование ПО промежуточного слоя позволяет справиться с этой задачей и устранить вечную дилемму – или внедрять инновации за счет снижения безопасности, или «заморозить» систему и игнорировать технический прогресс.

LETA. Сейчас специалистам приходится постоянно мониторить новые технологии, которые потенциально могут стать угрозами. Это, в некотором роде, «соревнование» меча и щита. Владельцы «щита» должны всегда быть в курсе, чем вооружен противник. Именно поэтому важно периодически проводить объективную оценку степени защищенности своей системы, даже если в самой системе ничего не меняется. Такой экспресс-анализ – это вполне доступная услуга, не занимающая много времени. Зато это позволяет своевременно увидеть возникновение «дыр» и правильно распределить усилия по модернизации системы ИБ.

Эффективно ли регулирование в сфере ИБ? На-

Сколько различаются подходы к регулированию и стандартизации, принятые в нашей стране и за рубежом? Как эти различия повлияют на российские предприятия в связи со вступлением России в ВТО?

Квазар-Микро. У нас хорошо развита часть стандартов, регламентирующая защиту информации государства и весьма слабо – регламентирующая защиту информации граждан и коммерческих организаций. Безусловно, вступление в ВТО усилит взаимопроникновение капитала и компаний, но и зарубежным компаниям в России и российским компаниям за рубежом придется соблюдать местное законодательство в данной сфере. Это, в свою очередь, подтолкнет нашу отрасль к ускоренной унификации отечественных стандартов по мировому образцу.

ИВК. Как показывает практика РФ, у нас эффективно регулирование, основанное на своих руководящих документах. Как говорится, уставы пишутся кровью — поэтому их исполнение обязательно и безоговорочно. А вот гармонизированные ГОСТы пока что не идут. Здесь имеется существенная недоработка законотворческих коллективов. Стремление РФ в ВТО даст все необходимое для регулирования ИБ в самом что ни на есть гармонизированном виде, но будет ли это использоваться? Это вопрос не праздный, ибо и здесь есть недоработка в части контроля исполнения. Такое ощущение, что именно контроль исполнения и не гармонизируется! Здесь все как надо – тяжесть российских законов компенсируется необязательностью их исполнения. Но если законы общие, то их исполнением можно вообще пренебречь. Так получается на практике. Надеюсь, что пока.

LETA. Есть разные мнения. С нашей точки зрения, регулирование недостаточно. Прежде всего, отсутствует законодательное определение, что такое информационная безопасность. С другой стороны, есть хорошие наработки ФСТЭК, ФСБ, ЦБ. Поэтому нельзя говорить, что нет регулирования ИБ.

Пока не очень понятно, как вступление в ВТО отразится на рынке безопасности. Скорее всего, изменятся правила лицензирования программных и аппаратных средств. Они могут стать мягче. Также вероятно распространение отраслевых стандартов безопасности.

АСВТ. Возможность предоставления операторами услуг защищенной связи регулируется через институт лицензирования, который работает эффективно. Но кроме лицензирования есть еще и аспект, связанный с технологиями и стандартами. Уровень защищенности информации, вероятно, все чаще будет становиться элементом SLA. Но, как правило, трафик проходит через сети нескольких операторов. Соответственно, сети операторов должны взаимодействовать так, чтобы уровень защищенности не менялся на границе сетей операторов. А это требует использования согласованных технических решений. Такое взаимодействие должно быть основано на стандартах. Российские стандарты в области обеспечения безопасности связи в целом не отличаются от зарубежных. Отмечу также, что к вопросам информационной безопасности вплотную примыкает вопрос сертификации телекоммуникационного оборудования по вопросам защиты.

Eset. Я бы отметил важность не только государственной стандартизации, но и разработки открытых стандартов взаимодействия антивирусных систем с другими элементами информационной системы ИТ и телекоммуникационного уровней. Дело в том, что функция противодействия вредоносного ПО должна неукоснительно включаться при любом способе поступления информации в систему – будь то передача данных по каналам связи, получение электронного письма или «мгновенного сообщения», копирование файлов из сети и др. Рост разнообразия каналов коммуникации современного компьютера, а также растущая популярность шифрования сообщений требуют, чтобы разные программы использовали функции проверки и защиты, «экспортируемые» антивирусом. Сегодня способы такого взаимодействия не унифицированы. Соответственно, для каждой формы такого взаимодействия необходимы специальные интерфейсные программы.