



КОД БЕЗОПАСНОСТИ – ЗАЩИЩАТЬ РЕАЛЬНОСТЬ

Российская компания «Код Безопасности» (ГК «Информзащита») разрабатывает соответствующие требованиям международных и отраслевых стандартов программные и аппаратные средства для обеспечения безопасности информационных систем. Продукты компании используются при защите конфиденциальной информации, персональных данных, среды виртуализации, коммерческой и государственной тайны. Генеральный директор компании Александр Ширманов рассказывает, как «Код Безопасности» обеспечивает своим клиентам качественные решения для задач информационной безопасности.



Александр Ширманов: «Наши продукты характерны еще и тем, что они обеспечивают возможность использования современных сетевых технологий в ИТ-инфраструктурах государственных организаций, поскольку их защитный функционал подтверждается сертификацией ФСТЭК России»

– Как изменились угрозы информационной безопасности в последние годы и какие из них наиболее сильно повлияли на развитие средств защиты?

Инновации в области информационных технологий породили новые угрозы безопасности, которые раньше трудно было представить. Например, распределенные инфраструктуры на платформе виртуальной среды, в которых совершенно по-другому требуется контролировать обеспечение сохранности и доступ к данным. Тенденции последних лет, такие как проникновение технологий мобильности во многие сферы деятельности, удаленный доступ сотрудников к корпоративным ресурсам, интернет-сервисы или услуги, предлагаемые по модели SaaS (приложение как сервис), а также облачные вычисления делают понятие сетевого периметра компании или организации размытым. Периметр фактически перестает существовать. Угроза несанкционированного доступа к распределенным ресурсам, похищения или уничтожения конфиденциальной информации, непубличных персональных данных многократно возрастает. Соответственно, эти изменения и приоритеты в области корпоративной безопасности повлияли на выбор нашей компанией направлений разработки

средств защиты информации применительно к российской действительности.

– Какие факторы определяют сегодня спрос на российском рынке решений обеспечения информационной безопасности?

Особенно надо выделить сегмент рынка информационной безопасности, формируемый действующими в стране нормативными и законодательными требованиями. В каждой стране есть свое национальное законодательство в области информационной безопасности, поэтому в России в этом сегменте доминируют отечественные производители, тогда как на рынке информационной безопасности в целом работает немало зарубежных производителей.

Сегодня основной спрос в данном сегменте, на котором и специализируется наша компания, определяется законодательством о гостайне, конфиденциальной и коммерческой информации, а также законом «О персональных данных». Информатизация в госорганах, необходимая для развития муниципального управления, организации электронных торгов и государственных услуг гражданам, порождает за-

В 2012 году, по мнению аналитиков Gartner, 60% виртуальных серверов будут защищены хуже, чем физические серверы, которые они заменили. Этот показатель уменьшится до 30% только к 2015 году.

Аналитики Forrester Research предложили своим респондентам ответить на вопрос, какие инициативы в области безопасности будут для них наиболее приоритетны в 2010 году



Источник: Forrester Research, 2010

дачи обеспечения информационной безопасности и потребности в обновлении средств ИБ.

– Существуют ли уже готовые решения, способные удовлетворить спрос в сегменте соответствия требованиям регуляторов?

Для соответствия нормативным актам, принятым в конце прошлого века, средства защиты, конечно, существуют. Однако, закон «О персональных данных» повысил уровень требований, и сегодня в нашем продуктовом портфеле представлены средства защиты информации, в том числе сертифицированные, удовлетворяющие всем его требованиям. Кроме них, мы разработали ряд новых программных продуктов, таких как: специализированное средство защиты информации (СЗИ) vGate для виртуальной среды на платформе VMware, HoneyPot Manager – система обнаружения вторжений с помощью «ловушек» – имитаторов баз данных и файловых серверов, распределенный межсетевой экран TrustAccess с централизованным управлением для разграничения доступа к критичным ресурсам сети. Все эти продукты характерны еще и тем, что они обеспечивают возможность использования современных сетевых технологий в ИТ-инфраструктурах государственных организаций, поскольку их защитный функционал подтверждается сертификацией ФСТЭК России.

– Сейчас много говорят о требованиях к техническим средствам защиты ИСПДн и их сертификации. Как изменились требования к безопасности персональных данных после внесения изменений в документы, регламентирующие выполнение закона «О персональных данных»?

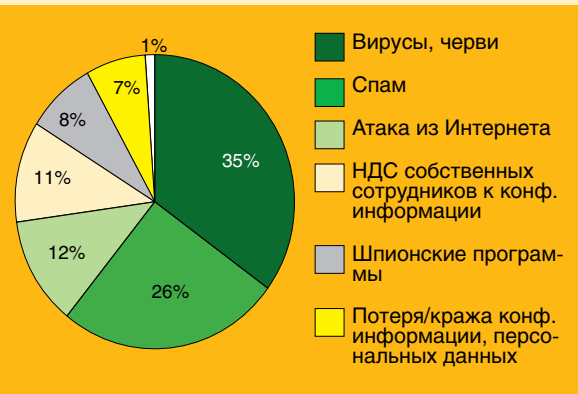
Во-первых, требования к безопасности персональных данных не изменились. Они были и остаются в соответствии с ФЗ-152 «О персональных данных» и постановлением Правительства РФ № 781. В приказе ФСТЭК № 58 изложены уточнения о методах и средствах для выполнения обязательных требований закона. В частности, методы и способы в зависимости от типа, класса информационных систем обработки персональных данных, особенностей их

построения и эксплуатации, других характеристик могут не использоваться, но тогда это должно быть обосновано моделью угроз безопасности ИСПДн (информационных систем персональных данных). Оператор персональных данных может воспользоваться услугами специализированного интегратора для аудита информационной безопасности, определения модели угроз и внедрения системы защиты ИСПДн, которой он может доверять, поскольку обязательной аттестации защиты ИСПДн не требуется. Во-вторых, касаясь технических средств защиты, мы считаем, что применение сертифицированных ФСТЭК/ФСБ России СЗИ для защиты персональных данных – это юридически оправданный и наименее рискованный путь выполнения требований законодательства в области обеспечения защищенности персональных данных. Уровень сертификации определяется классом ИСПДн. Например, в п. 7 приказа ФСТЭК № 58 указано на необходимость применения СЗИ, имеющего сертификат НДВ 4, для защиты ИСПДн 1 класса. Уровень сертификата соответствия СЗИ в ИСПДн 2 и 3 класса может определяться оператором персональных данных. Кстати, теперь оператор имеет право сам сертифицировать используемые им СЗИ, но, на мой взгляд, ему в ряде случаев удобнее воспользоваться уже сертифицированными средствами известного производителя.

– На кого возложены задачи аудита информационной безопасности, разработки модели угроз и проекта защиты, технологии внедрения?

Прежде всего, на наших партнеров – интеграторов. Компания «Код Безопасности» разрабатывает программные и аппаратные средства технической защиты информационных систем и не занимается прямыми продажами услуг или проектов безопасности. К заказчику мы всегда идем вместе с нашим партнером и готовы помочь ему в подготовке крупных корпоративных проектов. Специалисты нашего отдела продаж и менеджеры по продуктам нацелены на предпродажную поддержку проектов. Если заказчик обращается к нашим менеджерам, которые полностью готовы для него спецификацию проекта защиты, то в конечном итоге она передается одному из наших партнеров для поставки и внедрения. Мы видим нашу задачу в обучении партнера и выращивании его бизнеса по разрывыванию и сопровождению наших продуктов. Для этого мы усиливаем нашу партнерскую программу новыми курсами обучения, техническими семинарами и совместными маркетинговыми мероприятиями для заказчиков.

Серьезные инциденты, связанные с информационной безопасностью, отмеченные участниками мероприятий, проводимых компанией «Код Безопасности» в 2009-2010 годах



Программные и аппаратные средства для защиты персональных данных

Security Studio Suite – программный комплекс, не имеющий аналогов на российском рынке, предназначенный для защиты персональных данных на рабочих местах. Позволяет выполнить требования Федерального закона «О персональных данных» в части защиты информации в информационных системах с применением средств защиты от несанкционированного доступа, межсетевых экранов, антивирусов и средств защиты от программно-математических воздействий. Продукт Security Studio Suite создан на базе известного средства защиты Secret Net и нового продукта Security Studio Endpoint Protection.

TrustAccess – система распределенных межсетевых экранов (МЭ) высокого класса защиты (МЭ 2) с централизованным управлением, предназначенная для защиты сетевых ресурсов информационной системы от несанкционированного доступа. TrustAccess обеспечивает соответствие всем требованиям по защите персональных данных в части межсетевого экранирования и может применяться для сегментирования информационной сети.

vGate – средство обеспечения безопасности виртуальной инфраструктуры на базе систем VMware Infrastructure 3 и VMware vSphere 4. Применение vGate даст возможность легитимного использования в виртуальных средах информационных систем, обрабатывающих информацию ограниченного доступа, в том числе и персональные данные.

Honeypot Manager – средство защиты информации, предназначенное для обнаружения вторжений и несанкционированного доступа с помощью имитации персональных данных и конфиденциальной информации. Программа анализирует поведение нарушителей, атакующих прикладные программы и сетевые сервисы и позволяет существенно снизить риски раскрытия информации ограниченного доступа, обрабатываемой в базах данных современных бизнес-приложений (CRM, ERP, бухгалтерия и кадры). Honeypot Manager своевременно обнаружит попытки доступа к базам данных, реализованные посредством внешних хакерских атак или действий внутренних нарушителей (инсайдеров).

«Континент» – аппаратно-программный комплекс шифрования, сочетающий в себе межсетевой экран, средство построения VPN-сетей и маршрутизатор. Применяется для объединения через Интернет локальных сетей предприятия в единую корпоративную сеть и подключения удаленных и мобильных пользователей по защищенному каналу. Современная ключевая схема, реализующая шифрование каждого пакета на уникальном ключе, обеспечивает гарантированную защиту от возможности дешифровки перехваченных данных. Для защиты от проникновения со стороны сетей общего пользования комплекс «Континент» обеспечивает фильтрацию принимаемых и передаваемых пакетов по

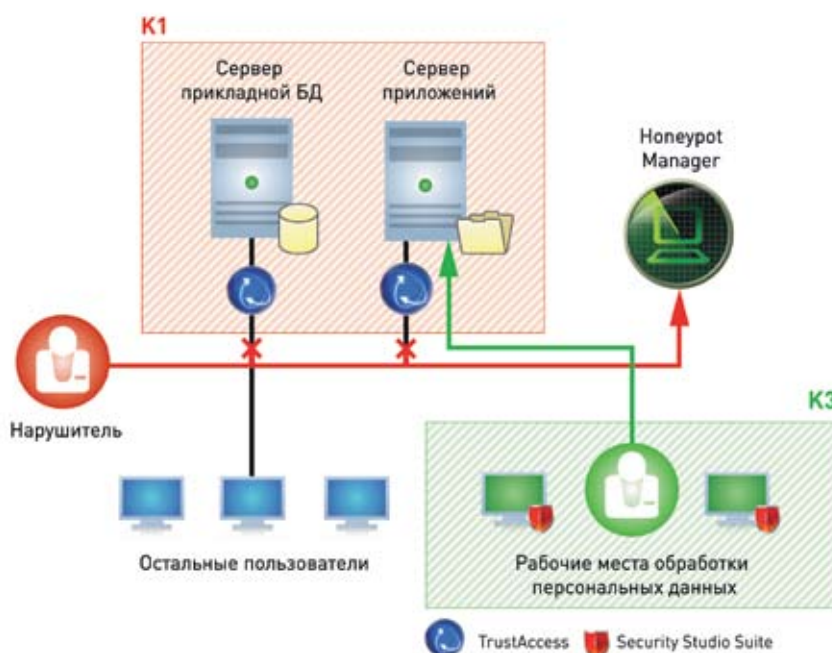
различным критериям (адресам отправителя и получателя, протоколам, номерам портов, дополнительным полям пакетов и т.д.). Осуществляет поддержку VoIP, видеоконференций, ADSL, Dial-Up, спутниковых каналов связи, технологии NAT/PAT для сокрытия структуры сети.

Электронный замок «Соболь» – программно-аппаратное средство, предназначенное для обеспечения доверенной загрузки и предотвращения несанкционированного доступа. Может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети. Поддержка платы PCI Express позволяет применять электронный замок для защиты любых современных компьютеров.

Схема демонстрирует реальный сценарий организации защиты ИСПДн с помощью продуктов компании «Код Безопасности» с применением метода сегментирования, который заключается в разделении информационной системы на несколько сегментов для оптимизации набора средств защиты информации, применяемых в каждом сегменте.

Применение TrustAccess и персонального межсетевого экрана (ПМЭ) 4 класса Security Studio Endpoint Protection, входящего в состав Security Studio Suite, позволяет реализовать в проекте безопасности сегментирование ИСПДн до K1 включительно. Образованные TrustAccess сегменты могут представлять собой отдельные ИСПДн более низкого уровня защищенности или класса, что существенно снижает затраты на построение защиты информационной системы.

При использовании TrustAccess совместно с продуктом Honeypot Manager авторизованный пользователь получает доступ к персональным данным, а при попытке соединения с ИСПДн пользователь, не обладающий на это правами, автоматически перенаправляется в ловушку. При этом происходит оповещение по электронной почте администратора информационной безопасности и производится запись в журнал событий, который хранится в локальной базе данных системы.



Реальный сценарий защиты ИСПДн

Оптимизация защиты: сегментирование

Если в некоторой локальной сети из 100 компьютеров только два обрабатывают данные ограниченного доступа (коммерческая тайна, служебная тайна или персональные данные), то нужно ли защищать все 100 компьютеров или только два? Ответ зависит от того, изолированы ли эти два компьютера от всех остальных. Изолировать их можно путем физического отделения от сети или путем установки межсетевого экрана на границе.

Представим более сложную ситуацию. В сети есть компьютеры, обрабатывающие данные разной степени конфиденциальности. Нужно ли всю сеть защищать по максимальному классу, например К1. Ответ зависит от тех же факторов, что и в первом примере, имеется ли сегментирование автоматизированных систем (АС), обрабатывающих конфиденциальные данные.

Сегментирование – процесс разделения информационных систем персональных данных или автоматизированных систем на взаимодействующие участки сети, который применяется для оптимизации набора средств защиты информации, используемых в каждом сегменте. Сегментирование позволяет, с одной стороны, уменьшить стоимость защиты, а с другой – снизить избыточность СЗИ в тех случаях, когда защищаемые данные расположены неравномерно по сети.

Какие основания для сегментирования имеются исходя из требований регуляторов в области защиты информации? Как следует из нормативного документа ФСТЭК «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» (пункт 5.1.7): «Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из объединяющихся АС может сохранять свой класс защищенности». А пункт 5.8.4 гласит: «Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Таким образом, если в локальной сети есть несколько АС разных классов, то основанием для сегментирования является применение сертифицированных ФСТЭК межсетевых экранов соответствующих классов.

А что можно сказать про требования к защите персональных данных? Приказ ФСТЭК России № 58 от 5 февраля 2010 г. «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», п. 2.11: «Подключение информационной системы к информационной системе другого класса или к информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) осуществляется с использованием межсетевых экранов». Из п. 2.4 приложения к данному приказу: «При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом».

Как этот механизм применяется на практике? Рассмотрим два основных сценария сегментирования – выделение сервера в отдельный сегмент сети и сегментирование до уровня отдельных рабочих мест пользователей. В первом случае можно исходить из того, что на сервере обрабатывается данных больше, чем на рабочих местах (если это действительно так в конкретной ИСПДн). В этом случае сервер следует классифицировать как ИСПДн более высокого класса, чем ИСПДн, располагающаяся на рабочих местах пользователей. Разумеется, сервер при этом следует защитить, например с помощью TrustAccess – распределенного МЭ высокого класса защиты. Применение TrustAccess не требует физической реконфигурации сети и достаточно лишь установить на защищаемый сервер агент TrustAccess.

Сегментирование до уровня отдельных рабочих мест пользователей в некоторых случаях позволяет понизить класс ИСПДн. Использование персонального межсетевого экрана дает возможность отделить рабочее место пользователя от остальной части сети. Применение продуктов компании «Код Безопасности» – сертифицированных ПМЭ 4 класса Security Studio Suite или «Континент-АП» – позволяет выделить отдельное рабочее место в отдельную ИСПДн класса К3 и К2. В таблице 1 указаны классы межсетевых экранов, которые следует использовать для сегментирования, а в таблице 2 – классы МЭ, применяемые для сегментирования ИСПДн.

Таблица 1. Классы межсетевых экранов для сегментирования АС

АС	МЭ
1Д, 3Б, 2А	МЭ 5
1Г	МЭ 4
1В, с грифом «секретно» 3А, 2А	МЭ 3
1Б, с грифом «совершенно секретно» 3А, 2А	МЭ 2
1А, с грифом «особой важности» 3А, 2А	МЭ 1

Таблица 2. Классы межсетевых экранов для сегментирования ИСПДн

Класс ИСПДн	Подключение ИСПДн к сетям общего доступа	
	Нет	Есть
К3	МЭ 5	МЭ 4
К2	МЭ 5	МЭ 4
К1	МЭ 4	МЭ 3

Таким образом:

1. Применение системы серверных межсетевых экранов класса 2 с централизованным управлением TrustAccess позволяет реализовать в проекте безопасности такое сегментирование АС до 1Б включительно или ИСПДн до К1 включительно, что образцовые TrustAccess сегменты могут представлять собой отдельные АС или ИСПДн индивидуального уровня защищенности или класса.
2. Применение сертифицированного персонального межсетевого экрана класса 4 Security Studio Suite или «Континент-АП» позволяет выделить АРМ в отдельную ИСПДн класса К3 и К2.
3. Смысл экранирования заключается в понижении класса ИСПДн на данном сегменте, т.е. целью является классификация именно по К3 или К2, а не по К1 (так как в этом случае нет никакого выигрыша в цене средств защиты).



Безопасность виртуальной инфраструктуры

В области виртуализации есть такой термин – «коэффициент консолидации». Это количество виртуальных машин, одновременно работающих на одной физической машине. Обычно подсчитывают среднее значение для всей виртуальной инфраструктуры предприятия. Для серверов, которые подверглись виртуализации, коэффициент консолидации обычно находится в пределах от 5 до 15 (для виртуальных десктопов – выше). ИТ-менеджеру этот коэффициент дает понять, насколько плотнее размещены информационные системы и сколько можно будет сэкономить на площади ЦОД, оборудовании и электроснабжении.

Но что этот коэффициент подсказывает лицу, ответственному за информационную безопасность в компании? А он дает понять, что с увеличением плотности размещения информационных систем растут и ставки потерь, поскольку если злоумышленник получит доступ к серверу виртуализации, то как минимум все виртуальные машины на этом сервере можно считать скомпрометированными.

Очевидно, что виртуальные машины должны быть защищены так же надежно, как и их физические аналоги. Но каков их реальный уровень защищенности? Исследовательская компания Gartner задась этим вопросом и в начале 2010 года провела исследование, которое дало ошеломляющие результаты – около 60% виртуальных серверов защищены существенно хуже, чем физические. По мнению Gartner, многие проекты виртуализации проводятся без учета проблем безопасности виртуализации и проведения необходимого аудита. Большинство компаний, которые перенесли свои информационные системы в виртуальную среду, полагают, что защищенность информационных систем не изменилась при их виртуализации. При этом они не учитывают наличие гипервизора – дополнительного слоя, на котором основана виртуализация. Среди ключевых рисков аналитики называют отсутствие контроля за административным доступом к гипервизору и средствам управления виртуальной инфраструктурой. Также в Gartner признают, что гипервизор – это новая платформа, которая может содержать еще не обнаруженные уязвимости.

Как пользователю защитить информационную систему? Очевидно, нужно снизить поверхность возможной атаки путем изоляции и/или контроля доступа к данной системе. В данном случае дополнительно нужно защищать гипервизор и сред-

ства управления виртуальной инфраструктурой от несанкционированного доступа (локального и сетевого).

Также, когда ставки реально высоки, нужно защищать от нерегламентированных действий администраторов виртуальной инфраструктуры. Например, возможность доступа к конфиденциальным данным, обрабатываемым в виртуальных машинах, может выходить за рамки функциональных обязанностей администратора виртуальной инфраструктуры. Тем более администратор не должен иметь возможность делать копии конфиденциальных виртуальных машин на внешние носители. Такие попытки должны контролироваться и пресекаться.

Средство защиты для виртуализации vGate специально предназначено для защиты информации в виртуализированных средах от несанкционированного доступа. Продукт vGate предназначен для обеспечения безопасности виртуальной инфраструктуры на базе VMware Infrastructure 3 и VMware vSphere 4 – самых распространенных на рынке платформ виртуализации.

vGate аутентифицирует администраторов и разграничивает доступ к элементам виртуальной инфраструктуры, позволяя при этом разделить права над виртуальной инфраструктурой на две роли – администратор безопасности и администратор виртуальной инфраструктуры. Администратор безопасности не имеет возможности производить какие-либо действия непосредственно с виртуальной инфраструктурой, но задает настройки безопасности и контролирует действия администраторов виртуальной инфраструктуры.

Первая версия vGate позволяет не только повысить защищенность виртуальной инфраструктуры от несанкционированного доступа, но и обеспечивает защиту, сертифицированную по нормам российского законодательства, что обеспечивает легитимность информационным системам, обрабатывающим в виртуальной среде данные ограниченного доступа (служебную тайну, коммерческую тайну, персональные данные и т.п.).

Выход второй версии vGate запланирован на июнь 2010 года. Получение сертификата намечено на конец 2010 года. При этом уровень сертификации позволит применять vGate 2.0 для защиты автоматизированных систем, обрабатывающих информацию, составляющую государственную тайну.

vGate 1.0 – сертифицированная защита виртуальных инфраструктур VMware Infrastructure 3 и VMware vSphere 4

Достоинства:

- vGate позволяет повысить защищенность виртуальной инфраструктуры, защитить от нелегитимных действий привилегированных инсайдеров;
- vGate дает возможность легитимного использования в виртуальных средах информационных систем, обрабатывающих данные ограниченного доступа, и помогает провести аттестацию таких систем.

Сертификаты:

- сертификат ФСТЭК России № 2061 от 26.03.10 на соответствие уровням СВТ 5 и НДВ 4;
- уровень сертификата позволяет применять vGate для защиты автоматизированных систем (АС) до класса 1Г и информационных систем персональных данных (ИСПДн) всех классов.



Коммерческий директор компании «Код Безопасности» Роман Ермолаев

Вместе вдвое сильнее

За последние три года в группе компаний «Информзащита» было образовано несколько новых компаний, две из которых тесно взаимодействуют как производитель и дистрибьютор, это разработчик специализированных программных и аппаратных средств защиты «Код Безопасности» и дистрибьюторская компания SafeLine. Коммерческий директор компании «Код Безопасности» Роман Ермолаев (Р.Е.) и генеральный директор SafeLine Василий Дубинин (В.Д.) рассказывают о преимуществах нового альянса для партнеров и заказчиков группы компаний «Информзащита».

– Как организован бизнес компании «Код Безопасности»?

Р.Е. С момента образования компании в конце 2008 года мы смогли выстроить работу с каналом и теперь выводим на рынок новые продукты. Мы работаем по трем направлениям, соответствующим категориям продуктов: «Сетевая безопасность», «СЗИ от НСД» и «Защита виртуализации». К направлению «Сетевая безопасность» относятся продукты, предназначенные для защиты периметра сети и сетевых приложений, межсетевые экраны. К средствам защиты информации от несанкционированного доступа (направление «СЗИ от НСД») относятся такие известные на рынке средства, как Secret Net или ПАК «Соболь», и новые продукты, разработанные для защиты персональных данных. Новое направление «Защита виртуализации» представлено продуктом Security Code vGate for VMware Infrastructure.

На данный момент можно выделить два сегмента рынка, для которых мы работаем: средства защиты информации, необходимые для приведения автоматизированных систем в соответствие с требованиями регламентирующих органов; программные продукты информационной безопасности для негосударственного коммерческого рынка. Если в первом сегменте наши продукты достаточно широко представлены в продуктовом портфеле нашей партнерской сети, то второй активно развивается.

В начале 2010 года анонсировано несколько новых программных продуктов, которые либо не имеют конкурентов на рынке, либо на достойном уровне конкурируют с лидерами рынка. Среди них СЗИ для виртуальной инфраструктуры vGate, распределенный межсетевой экран TrustAccess, ловушки, имитирующие СУБД, – Honeypot Manager, средство аудита программного и аппаратного обеспечения в корпоративной сети «Код Безопасности: Инвен-

таризация» и комплексное СЗИ, включающее персональный межсетевой экран, средство защиты от программно-математических воздействий и антивирус, – Security Studio Endpoint Protection.

Все эти продукты заказчики получают через двухуровневый канал продаж. Нашим официальным дистрибьютором является компания SafeLine, которая, в свою очередь, взаимодействует с партнерами второго уровня. Главнейшая задача партнеров состоит в обеспечении высокого уровня технической компетенции, ведь они должны не только продать наши продукты, но также внедрить и поддерживать их. Поэтому партнер должен иметь в своем штате сертифицированных специалистов (их количество зависит от партнерского статуса). Обучение можно пройти на льготных условиях в учебном центре компании «Информзащита», а по новым продуктам разрабатываются специальные учебные курсы, которые будут доступны в этом полугодии.

– Почему в группе компаний «Информзащита» была создана компания SafeLine?

В.Д. SafeLine выросла из департамента по работе с партнерами группы компаний «Информзащита». В какой-то момент времени возникло понимание, что успешно развиваться, одновременно в качестве разработчика собственного продукта и системного интегратора, который его внедряет и продает другим компаниям-интеграторам невозможно. Поэтому было принято решение выделить разработчиков, дистрибьюторский бизнес и интеграцию в самостоятельные направления. Так возникла компания SafeLine, ключевой задачей которой было гарантировать равные условия для всех компаний, желающих покупать и внедрять продукты, разработанные как в рамках группы компаний «Информзащита», так и другими производителями решений в области информационной безопасности. Как мне кажется, с этой задачей мы справились. Для нас принципиально важна fair play (честная игра), и мы не делаем различий между компаниями, входящими в группу, и другими партнерами.

– Что предпринимается для поддержки партнеров?

Р.Е. Все продажи продуктов компании «Код Безопасности» осуществляются только через партнеров. Именно поэтому мы нацелены на тесное взаимодействие с официальным дистрибьютором и его партнерской сетью. Вывод новых продуктов на рынок включает не только рекламную кампанию для заказчиков, но и информационную поддержку партнеров, когда мы совместно с дистрибьютором организуем вебинары, круглые столы и конференции с целью обучения партнеров функционалу новых продуктов. Цель проводимых мероприятий – научить партнеров (несомненно, уже весьма квалифицированных в сфере информационной безопасности) продавать новые продукты и развивать смежное продуктовое направление своего бизнеса – средства защиты информации для коммерческого рынка.

С начала текущего года активно внедряется партнерская программа, нацеленная на комплексное взаимодействие с каждым партнером. В программе

предусмотрено предоставление партнерам демо-оборудования для организации демонстраций его работы перед заказчиками. Внедрена процедура регистрации сделок, направленная на защиту инвестиций, уже сделанных партнером до продажи в подготовку решения для заказчика. Мы помогаем партнеру представить нашу продукцию на мероприятиях для заказчиков. В компании «Код Безопасности» действует программа маркетинговой поддержки партнеров, предоставляющая инструменты развития продаж как для наших постоянных партнеров, так и для начинающих, стремящихся развивать направление информационной безопасности с помощью наших продуктов. Например, партнер может воспользоваться нашим электронным каталогом, чтобы выложить информацию о продуктах на своем сайте, организовать рекламную кампанию в Сети с помощью готовых баннеров, записать на CD-диск рекламные брошюры, сценарии применения и демо-ролики для распространения среди своих заказчиков.

В.Д. «Код Безопасности» остается одним из наших ключевых партнеров. Мы считаем, что продукты этой компании – оптимальное решение в сегменте сертифицированных решений по защите информации. И если раньше все было достаточно просто – SafeLine была лишь окном, через которое партнеры могли общаться с производителем, то теперь мы берем на себя более активную роль: разрабатываем собственные программы по стимулированию партнеров, стремимся продавать не просто продукт, а решения проблем на его основе. Для этого формируется команда из менеджера продукта, отвечающего за коммерческую составляющую продвижения, и инженера, обеспечивающего технический аспект решений. Мы понимаем специфику каждого региона и то, что продажа сложных решений требует плотного взаимодействия с партнерами, поэтому мы ввели институт ответственных аккаунт-менеджеров, курирующих партнеров в регионе и упрощающих взаимодействие с нами.

– В чем специфика дистрибуции продуктов информационной безопасности?

В.Д. На наш взгляд, дистрибьютор, который пытается просто перепродавать продукты информационной



Генеральный директор компании SafeLine Василий Дубинин

безопасности, не будет успешен. Ведь конечному пользователю, а значит, и партнеру, с ним работающему, нужен не продукт, а решение конкретной проблемы. И разнообразие таких задач достаточно велико. Поэтому дистрибьютор в сфере информационной безопасности должен предлагать именно решения под широкий спектр запросов, взяв на себя функции первичного проектирования, исследования продуктов и их более точного позиционирования.

С другой стороны, не может существовать единой технологии продажи: помимо требований разных партнеров, необходимо учитывать требования регуляторов, реальные технологические особенности того или иного продукта и т.п. Мы как дистрибьютор, видим своей задачей максимально освободить партнеров от всего этого и дать им возможность сконцентрироваться на бизнесе с заказчиком.

Классически дистрибуция определяется как: товар–логистика–кредит, и, если с товаром все понятно – им является решение на основе продукта, то два других компонента, логистика и кредит, требуют дополнительного внимания и разъяснения. Прежде всего, мы формируем достаточные складские запасы, чтобы обеспечить передачу партнерам товаров в максимально сжатые сроки. Тем самым мы экономим оборотные средства партнеров и упрощаем их работу по планированию. Отрабатывая свои внутренние процессы и взаимодействие с различными официальными органами, мы обеспечиваем максимально короткие сроки доставки. Кроме этого, мы реализуем кредитные и ребеитные программы, которые позволяют партнерам оптимизировать доходность при работе с нами.



SafeLine

ГК «Информзащита»

Компания SafeLine – дистрибьютор решений и программно-технических средств в области ИТ-безопасности. SafeLine образована и вошла в состав группы компаний «Информзащита» в 2007 году.

Среди вендоров SafeLine – лидеры мирового и российского рынков ИТ-безопасности, дилерами компании являются более 400 компаний в 70 регионах России и странах СНГ.

Тел.: +7 (495) 980-23-45

E-mail: partners@safe-line.ru

<http://safe-line.ru>

История успеха

За 15 лет работы группы компаний «Информзащита» ее клиентами стали более 2,5 тыс. государственных и коммерческих организаций в России и других странах СНГ, а во многих крупных проектах были использованы продукты компании «Код Безопасности» – разработчика программных и программно-аппаратных средств защиты. Среди проектов стоит отметить такие масштабные работы, как участие в разработке и развитии подсистемы обеспечения безопасности информации Государственной автоматизированной системы Российской Федерации «Выборы».

Компания «Информзащита» приняла непосредственное участие в разработке концепции развития информационной безопасности ГАС «Выборы». Созданная подсистема обеспечения безопасности информации и заложенные в ней технические решения обеспечивают безопасность информации во время проведения выборов в различные органы власти.

За последние несколько лет были проведены работы в Федеральной таможенной службе России. Были решены задачи по обеспечению конфиденциальности информации, доступности, целостности и аутентичности. В рамках данного проекта была осуществлена поставка и настройка программных и программно-аппаратных средств защиты информации, в том числе были использованы аппаратно-программные комплексы шифрования «Континент». Решение для ФТС РФ обеспечило:

- криптографическую защиту сетевого трафика между удаленными сегментами сети;
- защиту внутренних сегментов сети от несанкционированного доступа со стороны пользователей сетей общего пользования;
- скрытие внутренней структуры защищаемых сегментов сети;
- усиленную аутентификацию пользователей удаленных таможенных постов и терминалов;
- централизованный сбор и анализ содержимого журналов статистики работы компонентов комплекса;
- централизованное управление настройками всех используемых устройств аппаратно-программного комплекса.

Специалистами компании «Информзащита» был проведен полный цикл работ по приведению информационных систем персональных данных ОАО «Концерн Росэнергоатом» в соответствие с требованиями российского законодательства, включивший в себя инвентаризацию персональных данных, классификацию, проектирование системы защиты, внедрение и аттестацию. На этапе внедрения была осуществлена установка и настройка комплекса сетевой защиты, в том числе с применением продуктов компании «Код Безопасности»: «Соболь» и Secret Net, которые позволили реализовать все требования нормативно-правовых актов ФСТЭК и ФСБ по защите персональных данных, включая требования к подсистемам управления доступом и обеспечения целостности информации.



Код безопасности

ГК «Информзащита»

Компания «Код Безопасности» (ГК «Информзащита») – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, коммерческой и государственной тайны.

Высокое качество продуктов компании подтверждают сертификаты на средства защиты информации, выданные ФСТЭК, Министерством обороны и ФСБ России.

Более 400 авторизованных партнеров поставляют продукты компании «Код Безопасности», обеспечивают их поддержку и сопровождение в 70 российских регионах.

Более 2500 государственных и коммерческих организаций в России и странах СНГ доверяют продуктам компании «Код Безопасности» обеспечение безопасности своих информационных систем.

Наиболее значимые проекты, в которых использовались продукты компании, – это подсистема информационной безопасности ГАС «Выборы», защищенная телекоммуникационная система взаимодействия региональных подразделений Министерства финансов, защита информационных систем региональных управлений Банка России, подсистемы информационной безопасности Федерального казначейства, Федеральной таможенной службы, ОАО «Вымпелком», концерна «Росэнергоатом».

«Код Безопасности» стремится соответствовать высоким стандартам качества и инноваций при разработке новых программных средств защиты и является технологическим партнером ряда ведущих международных компаний – лидеров мирового рынка программного обеспечения и оборудования, таких как Microsoft, VMware, Citrix.

Тел.: +7 (495) 980-23-45

E-mail: Info@securitycode.ru

www.securitycode.ru