Государственные информационные системы: безопасность данных на особом контроле

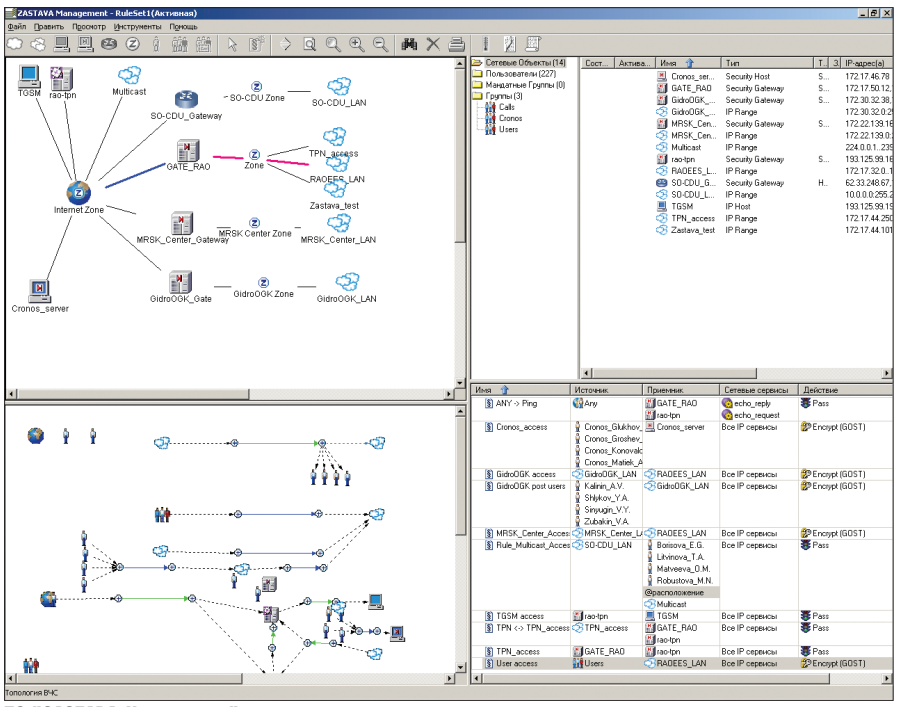
ИГОРЬ ШИТОВ

Для российской ИТ-отрасли 2013 год стал без преувеличения знаковым. Была опубликована "Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 — 2020 годы и на перспективу до 2025 года". Совет Федерации разработал стратегию кибербезопасности России, а в январе 2014-го началось её общественное обсуждение. Эти два программных документа чётко указывают на то, что государство выбрало свой вектор развития в области ИТ. Госорганы активно поддерживают данное направление, становясь не только разработчиками руководящих документов, но и потребителями самых масштабных и интересных решений.

Однако 2013-й стал и годом атак на информационные ресурсы. Компания Cisco в своём отчете "Cisco 2014 Annual Security Report" отмечает, что количество зарегистрированных атак в прошлом году значительно превысило этот показатель за предыдущие годы. Теперь их объектами становятся не только корпорации и частные лица, но и государственные информационные системы (ГИС). Спектр мотивов таких атак — от хактивизма до наступательных действий в кибервойнах.

Государственные органы непосредственно не занимаются коммерческой деятельностью, но размер их информационных систем и ценность информации, обрабатываемой в них, зачастую даже превосходят эти показатели для крупных коммерческих структур. В проведённом исследовании B2B International отмечено, что средний размер ущерба от одного инцидента в сфере ИБ для крупной компании можно оценить в 25 млн. рублей. А общий ущерб для государства даже сложно представить!

В России основными руководящими документами по информационной безопасности государственных информационных систем в 2014 году будут "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (приказ ФСТЭК России от 11 февраля 2013 г. № 17) и "Требования и методы по обезличиванию персональных данных государственными и муниципальными органами" (приказ Роскомнадзора от 5 сентября 2013 г. № 996). В феврале 2014-го приказом ФСТЭК России планируется введение в действие методического документа "Меры защиты информации в государственных информационных системах", который будет разъяснять порядок выполнения требований, установленных приказом № 17. Кроме того, ФСТЭК ведёт разработку единого методического документа, устанавливающего порядок моделирования угроз для безопасности информации независимо от вида обрабатываемой в ГИС информации ограниченного доступа (за исключением государственной тайны). Пока такая методика разработана только для персональных данных.



ПО "ЗАСТАВА-Управление" — мониторинг в реальном времени

Давайте попробуем разобраться, какие же меры защиты регулятор считает приоритетными для государственных информационных систем. Для этого нужно обратиться к 17-му приказу. Состав мер защиты (что нужно делать) получается очень обширным: идентификация и аутентификация субъектов и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защита машинных носителей информации; регистрация событий безопасности; защита от вредоносного кода; обнаружение (предотвращение) вторжений; контроль (анализ) защищённости информации; защита среды виртуализации; защита технических средств; защита систем связи и каналов передачи данных, обеспечение целостности и доступности информационной системы и информации.

Среди перечисленных одной из самых важных задач является именно обеспечение сетевой безопасности для ГИС. Это обусловлено прежде всего огромной территориальной распределённостью таких систем и масштабом происходящих изменений. Ярким примером тут может служить проект полного перевода органов госвласти на электронный документооборот к 2017 году. Региональные госструктуры тоже не отстают и строят территориально распределённые ИС, причём их проработка и зрелость зачастую даже выше, чем у федеральных систем. И все эти системы предъявляют самые строгие требования к защите каналов связи.

У нашей компании есть значительный опыт работы с государственными заказчиками. На протяжении последних лет мы решили многие задачи по проектированию систем защиты информации для ГИС, запуску и модернизации технических подсистем ИБ и их технической поддержке. Нашими заказчиками стали Банк России, ФСТЭК, ФНС, Росфинмониторинг, Росреестр, Комитет информатизации и связи г. Санкт-Петербурга, Правительство республики Татарстан. Реализуя эти проекты, мы смогли выделить несколько задач, решение которых должно быть приоритетным при обеспечении сетевой безопасности.

Однако при реализации крупных федеральных и региональных проектов мы столкнулись с важной задачей централизации управления защищённой сетью. Этого требует не только территориальная удалённость подразделений, но и не всегда достаточная компетенция персонала, обслуживающего системы на местах. Вторая важная задача — организация защищённого доступа удалённых (мобильных) пользователей к информационным ресурсам органов госвласти. Это особенно актуально для сотрудников, часто выезжающих в командировки, проводящих выездные проверки и инспекции.

Практика и количество внедрений показывают, что для решения задач сетевой безопасности как нельзя лучше подходят VPN/FW-продукты, в том числе и из линейки "ЗАСТАВА", разработчиком которых является компания "ЭЛВИС-ПЛЮС".

Одно из ключевых преимуществ семейства продуктов "ЗАСТАВА" — гибкость масштабирования системы. Сейчас в промышленной эксплуатации находится корпоративная сеть с общим числом узлов более 10 000 (филиалы, удалённые подразделения и региональные представительства, удалённые пользователи), а технологических ограничений на количество узлов просто нет. Администраторы, работающие с системой каждый день, также отмечают удобство и продуманность централизованного управления из одной географической точки в режиме реального времени с помощью продукта "ЗАСТАВА-Управление". Они могут гибко настраивать правила VPN/FW, вести мониторинг работы всей системы, проводить диагностику и анализ логов, удалённо обновлять VPN/FW-агенты. При этом есть одна интересная особенность: вместо одного глобального центра можно создать целую иерархию центров управления. На каждом уровне иерархии администраторы будут обладать только ограниченным, заранее определённым набором прав в рамках своего территориального сегмента.

Решения семейства "ЗАСТАВА" совместимы с различными операционными системами и аппаратными конфигурациями, в том числе отказоустойчивыми, что обеспечивает высочайшую надёжность системы. Кроме этого наша компания предлагает широкий выбор программно-аппаратных комплексов, которые прошли предварительное тестирование и на которых обеспечена максимальная производительность VPN/FW "ЗАСТАВА".

В каждый проект для ГИС наша компания привносит не только те или иные технические решения, но и экспертизу. Мы сознаём, что разобраться в большом количестве появляющихся нормативных документов бывает очень непросто, поэтому периодически организуем специализированные семинары и вебинары для сотрудников служб ИТ-органов госвласти. Мы всегда открыты к диалогу и готовы делиться своими знаниями с отраслью. Задать вопросы, а также найти анонсы ближайших мероприятий вы всегда можете на сайте компании "ЭЛВИС-ПЛЮС".

Автор статьи — руководитель направления компании "ЭЛВИС-ПЛЮС".

СПЕЦПРОЕКТ КОМПАНИИ "ЭЛВИС-ПЛЮС"

Российский рынок ИБ...

◂ ПРОДОЛЖЕНИЕ СО С. 19

требований со стороны федеральных регуляторов.

Если до недавней поры, как отмечет Андрей Голов, разработка нормативных документов в большинстве случаев велась во ФСТЭК исключительно собственными силами внутри ведомства, то теперь к этому процессу все больше и больше привлекают экспертное сообщество, что является важным шагом в поиске золотой середины между требованиями регуляторов и возможностями тех, на кого эти требования распространяются.

Представители ведущих ИБ-компаний и независимые эксперты стали принимать активное участие в деятельности сформированных при ведомствах рабочих комитетов, таких как технические комитеты по стандартизации "Криптографическая защита информации" (ТК 26), "Защита информации" (ТК 362) и другие. Это дает им возможность на ранних стадиях формирования регулятивных требований высказывать и отстаивать свои позиции перед регуляторами. Изменения регуляторами подхода к разработке своих документов, по оценкам экспертов, заметно повысило их качество и сократило сроки подготовки.

В прошлом году были разработаны проекты актуальных для страны стандартов. В частности, в ТК 362 подготовлено три проекта по стандартам, два из них — по обеспечению информационной безопасности в облаках.

В конце прошлого года Совет Федерации РФ высказал намерения подготовить новую редакцию закона "О персональных данных". Суть изменений, по словам одного из инициаторов проекта сенатора Руслана Гаттарова, заключается в достижении баланса между техническими требованиями и ответственностью за защиту персональных данных (ПДн). Эксперты ожидают, что новая редакция закона снимет многие практические вопросы, связанные с организацией такой защиты.

По мнению Сергея Вихорева, одной из наиболее острых национальных проблем настоящего времени в области ИБ остается отсутствие отраслевых моделей угроз по отношению к ПДн. Разработка таких моделей предписана законом "О персональных данных". Именно на эти модели ориентирована новая система выбора операторами ПДн мер и способов защиты. К большому сожалению, без них ни постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", ни упомянутый выше приказ ФСТЭК России № 21 не могут работать в полную силу.

Благая идея сократить расходы операторов персональных данных на создание эффективной защиты ПДн за счет переложения части бремени на отраслевых регуляторов пока не заработала. Сегодня, как отмечает г-н Вихорев, операторы ПДн вынуждены — в нарушение закона! — и с большими затратами приглашать внешних специалистов для оценки угроз ПДн, так как без этой процедуры выбрать оптимальный состав мер и средств защиты невозможно.

В этом же ряду, на взгляд Сергея Вихорева, стоит и проблема защиты интересов субъектов ПДн. Закон предпи-

ПРОДОЛЖЕНИЕ НА С. 23 ▸