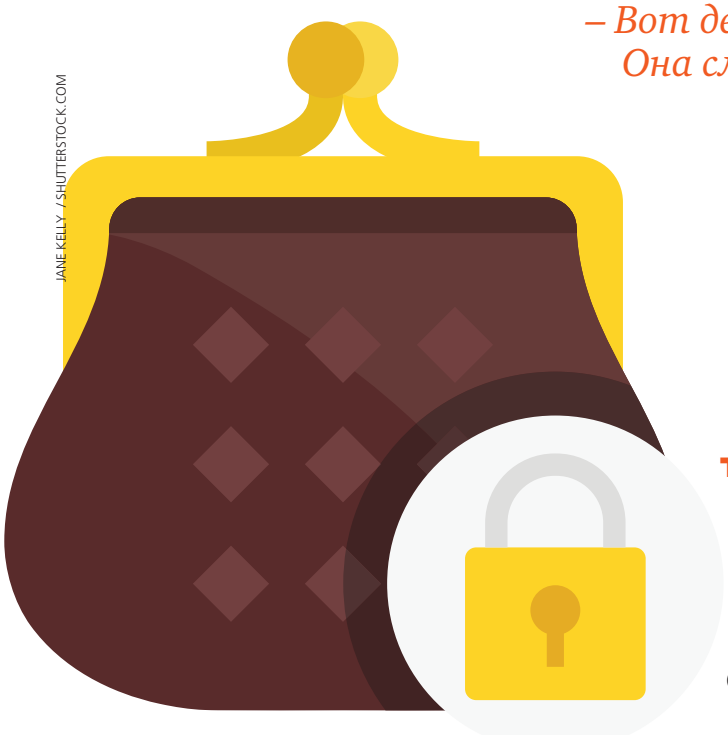
ИГОРЬ СОБЕЦКИЙ,
заведующий кафедрой экономической безопасности Учебного центра «Информзащита»

Бюджетирование безопасности или бюджетная безопасность?



JANE KELLY / SHUTTERSTOCK.COM

– Вот держи, можешь облизать эту бумажку. Она сладкая, год назад в нее была завернута карамелька с ромом.

Экономия оперативных расходов в изложении Дж. Родари

Автор статьи не ставит своей целью написать тысяча первое руководство по вытягиванию из топ-менеджеров компании денег на нужды службы безопасности. Этот вопрос неоднократно и детально рассматривался, в том числе, и на страницах этого журнала. Сейчас же хотелось бы обсудить смежную тему – до какой степени можно сэкономить на безопасности.

В принципе с такой проблемой сталкивается каждый начинающий[1] специалист по безопасности. Топ-менеджер, санкционировавший создание подразделения информационной безопасности, уже несколько раз успел пожалеть об этом необдуманном решении. В наше кризисное время выделить еще целую ставку – или две ставки, или даже три (доктора сюда!) ставки – не для очередного менеджера по продажам, а для дармоеда из службы безопасности – слишком рискованный ход. И, как оказалось, проигрышный. Вновь принятый горе-специалист[2], вместо того, чтобы в первый же день уже что-нибудь заработать для компании, а завтра уже полностью отбить свою зарплату, начинает требовать еще денег. Да как он только посмел? Сейчас американские санкции, кризис, рост доллара, разруха в головах – нету денег! Совсем нету. Пусть лучше налаживает безопасность организационно-административными методами. Регламент какой-нибудь,

например, напишет. Также, говорят, очень хорошие результаты дает подготовка корпоративной программы обеспечения безопасности до 2025 г. Так что пусть специалист пока поработает без капиталовложений, деньги целее будут.

Через несколько месяцев выясняется, что безопаснее в компании не стало. Без технических средств защиты от несанкционированного доступа и мониторинга сетевой активности не представляется возможным контролировать соблюдение принятых регламентов. Грозная программа на 2025 год в году 2014 никого не испугала. В IT-отделе на недопущенного к бюджету специалиста смотрят, как на бедного родственника. Словом, бесплатно хорошо не бывает.

Специалиста просят прикинуть потребности в технических средствах защиты информации. Конечно же, он не просит золотые горы, а ограничивается лишь минимально необходимым. Из минимально необходимого в компании хорошо бы иметь:

- надежный аппаратный межсетевой экран, если он еще не установлен специалистами IT-отдела[3];
- надежное корпоративное антивирусное средство[4];
- средство защиты от несанкционированного доступа, хотя бы на часть рабочих станций;
- система резервного копирования;
- DLP-система, хотя бы host-based;
- криптографическое средство для организации виртуальных частных сетей (VPN), если компания имеет филиальную структуру;
- система видеонаблюдения в офисе;
- система контроля и управления доступом в служебные помещения (СКУД).

Как говорил один английский классик, эти средства «не то, с чем мы как-нибудь обойдемся, а то, без чего никак нельзя обойтись». Поэтому в том или ином виде соответствующие аппаратные и программные средства вставляются в политику безопасности компании, а затем и в планы закупок.

И вот тут начинается Великий Торг между топ-менеджером, его доверенным финансистом и специалистом по безопасности. Беда в том, что рынок всех перечисленных продуктов отличается крайне высоким уровнем конкуренции, и не существует ни одной компании, предоставляющей все эти решения в комплексе[5]. В результате цены на продукты одного и того же назначения у разных производителей могут отличаться на порядок. Например, та же DLP-система может стоить от 900 руб. за одно контролируемое рабочее место (Staff Cop) до 18 000 руб. (Search Inform) за то же самое. Откровенное мошенничество на рынке средств безопасности не водилось даже в лихие 90-е, все продаваемые продукты работают и выполняют поставленные задачи[6].

Беда специалиста по безопасности в том, что у него, как правило, не готовы аргументы в пользу продуктов группы luxury. Если убедить топ-менеджера в пользе, например, антивирусного средства, принципиально возможно, то доказать преимущества платного антивируса Касперского (83 000 руб. за защиту 50 PC в течение 1 года) перед дешевым Avast (38 000 руб. за то же самое) или условно бесплатной Avira может оказаться весьма непросто.

Большинство руководителей российских компаний, в особенности среднего бизнеса, недостаточно ориентируются на рынке технических средств безопасности. В результате срабатывает один из главных принципов нашего бизнеса: денежки счет любят. Если одна и та же задача может быть решена разными способами, то имеет смысл выбрать самый дешевый. И по аналогии с самой дешевой мебелью для персонала (пусть комендант сам покрутится со сломанными стульями), компьютерами noname и в десятый раз заправленными картриджами для принтера (системный администратор тоже не барин, справится) компания обзаводится самыми дешевыми средствами безопасности. При этом руководитель чувствует себя настоящим благодетелем для специалиста по безопасности: ну как же, тот еще ничего для компании не сделал, а ему уже столько денег отвалили!

Результат не заставляет себя ждать. Быстро выясняется, что дешевые при покупке средства в эксплуатации почему-то не совсем удобны. Межсетевой экран за бесценок, оказывается, требует сложнейшей настройки. Специалист целыми днями просиживает перед экраном, но закончить эту работу постоянно мешают какие-то проблемы – то менеджеры не могут пробиться к своему же сайту, то безвестный украинский хакер начисто блокирует доступ в Интернет всей компании, то на всех компьютерах почему-то появились навязчивые рекламные баннеры. Бесплатный антивирус вроде бы работает неплохо, но то один, то другой компьютер внезапно сходят с ума и начинают требовать серьезного лечения.

Средство защиты от НСД странным образом установилось не на всех компьютерах – на самых новых оно почему-то не функционирует, а на самых старых иногда намертво блокирует загрузку. Как правило, беда случается как раз в момент отправки срочных платежей, после чего пользователи из бухгалтерии скандалят и жалуются руководству.

Прочие средства защиты функционируют в том же ключе. DLP-система конфликтует с бизнес-

БОЛЬШИНСТВО РУКОВОДИТЕЛЕЙ НЕДОСТАТОЧНО ОРИЕНТИРУЮТСЯ НА РЫНКЕ СРЕДСТВ БЕЗОПАСНОСТИ

приложениями и время от времени «подвешивает» компьютеры пользователей. Пользователи, от которых DLP-система засекречена, требуют помощи от системного администратора. Администратор стал мрачен и угрожает кулачной расправой.

Дешевая СКУД обошлась одним замком на парадной двери и одним на служебном входе. Опоздания прекратились – в каждом отделе работники избрали дежурного, по утрам проводящего по замку пачкой proximity-карт. Вывести хитрецов на чистую воду по видеозаписи невозможно – дешевые камеры наблюдения не дают уликовых записей, на видео можно понять, что с замками проказничают гуманоиды, у хитрецов по две руки, две ноги и одна голова, более существенные подробности скрывает низкое разрешение камер.

А поскольку администрирование всего этого «зверинца» отнимает слишком много времени, даже самый трудолюбивый специалист попросту не справляется с работой. Приходится приглашать ему в помощь второго, третьего, четвертого… В общем, остается только вспомнить народную мудрость: скупой платит дважды.

Автору уже неоднократно в различных российских компаниях приходилось видеть[7] результаты работы потомков Плюшкина. В чем же причина казуса? Проблема в том, что специалисты «второго эшелона» при проектировании системы информационной безопасности компании учитывали только стоимость приобретения, но не стоимость владения соответствующих аппаратно-программных средств.

Проект системы технической защиты информации должен отталкиваться от сформулированных в политике информационной безопасности требований. По сути, в таком случае политика информационной безопасности компании может рассматриваться как неформальное техническое задание на проектирование.

При этом в начале пути от политики безопасности к проекту и далее к выбору конкретных средств защиты информации следует выделить основные задачи, которые должны быть решены готовой системой, например контроль доступа в информационную систему, защита от вирусов, контроль за действиями персонала и т. д.

Затем необходимо определить, какие типы аппаратно-программных средств необходимы для реализации этих задач. Возможно, что одно средство защиты может обеспечить выполнение нескольких требований. Например, некоторые антивирусные пакеты также могут быть использованы для ограничения доступа к ресурсам сети Интернет, а многие межсетевые экраны способны

Остается вспомнить народную мудрость: скупой платит дважды

JANE KELLY / SHUTTERSTOCK.COM

поддерживать функционирование VPN. На этом этапе формируется эскизный проект технической защиты. Перед выбором конкретных средств защиты также потребуется провести подробное обследование действующей информационной системы компании, в ходе которого стоит прояснить как минимум следующие вопросы:

- сколько и какого компьютерного оборудования имеется в компании;
- модели пользовательских рабочих станций, их основные технические характеристики, в том числе, объем оперативной памяти, общее и свободное дисковое пространство, наличие и типы свободных слотов на материнской плате, наличие и типы свободных внешних портов (USB 2.0, 3.0, FireWire и т. п.), наличие и скорость работы сетевых плат;
- модели используемых серверов, их размещение, наличие и типы свободных внешних портов, наличие свободных мест в серверных стойках;
- сетевое оборудование, наличие и места расположения коммутаторов, управляемость сети, наличие и места физического расположения SPAN-портов коммутаторов;
- планы модернизации компьютерного парка, планируется ли списание или закупка рабочих станций и серверов, принято ли решение по закупке конкретных моделей и спецификация этих моделей;
- средства защиты, установленные в данное время, в том числе, модель межсетевого экрана, вид антивирусного средства, иные аппаратно-программные средства защиты информации, наличие и тип лицензий на соответствующие программные модули (подписка на программное обеспечение, годовая лицензия, бессрочная лицензия), а также стоимость последующего продления лицензий;
- оценить перспективы совместимости действующих средств защиты информации с планируемым к закупке оборудованием;
- используемое программное обеспечение, наличие и типы лицензий на него, планы замены и модернизации программного обеспечения;
- наличие и тип используемой системы видеонаблюдения – архивное или оперативное видеонаблюдение, тип камер (цифровые или аналоговые), раз-

ВЫВЕСТИ ХИТРЕЦОВ НА ЧИСТУЮ ВОДУ ПО ВИДЕОЗАПИСИ НЕВОЗМОЖНО

решающая способность камер, средства хранения видеозаписей (серверы или специальные видеорегистраторы), наличие средств интеллектуального анализа видеозаписей, практическая отдача от видеонаблюдения в настоящее время, интеграция системы видеонаблюдения с другими системами;

- наличие и тип используемой системы контроля доступа в помещения (СКУД) – модель системы, на каких проходах стоят замки и сколько такие замки стоят, типы ключевых носителей (iButton, proximity карты, штрих-код и др.) и возможность использования этих ключевых носителей для решения смежных задач (например, в средствах защиты от несанкционированного доступа), а также возможности модернизации СКУД и интеграции ее с другими системами.

И только теперь можно переходить к выбору конкретных аппаратно-программных средств для закупки. При выборе того или иного средства желательно ответить на следующие вопросы:

- требуются ли какие-то специальные лицензии (ФСТЭК или ФСБ) на приобретение и эксплуатацию данного средства;
- совместимо ли данное средство с имеющимися в компании рабочими станциями и серверами, а также с техникой, планируемой к закупке;
- совместимо ли данное средство с программным обеспечением, используемым бизнес-пользователями, с учетом перспектив модернизации и замены программного обеспечения;
- условия приобретения – разовый платеж, ежегодные платежи, аренда;
- развертывание и внедрение средства в компании – своими силами с учетом квалификации имеющегося персонала, с помощью сторонних консультантов или специалистов компании-поставщика;
- продолжительность внедрения средства и проблемы для бизнес-пользователей, могущие возникнуть на этапе внедрения;
- возможность получения бесплатных тестовых версий и проверки на совместимость на реальной информационной системе компании и ее филиалов;
- необходимость приобретения дополнительных инфраструктурных компонентов для эксплуатации данного средства (сервера, стойки, кабели, отдельные рабочие станции для администрирования, нестандартные считыватели для ключевых носителей и т. д.) и их стоимость;
- условия эксплуатации средства – требуется ли наличие специального персонала, сколько часов в день занимает администрирование средства, включая анализ лог-файлов, возможна ли эксплуатация средства своими силами с учетом квалификации имеющегося специалиста по безопасности, требуется ли дополнительное обучение (и сколько такое обучение будет стоить) или найм дополнительного персонала;
- надежность средства, угрозы для корпоративной информационной системы при выходе средства из строя, стоимость восстановительных работ;
- возможность интеграции средства с уже имеющимися в компании средствами технической защиты, стоимость такой интеграции, при невозможности интеграции – перспективы использования ранее установленного оборудования (параллельное использование нового и старого оборудования, передача в региональный филиал компании, продажа третьим лицам, списание) и связанные с этим издержки;
- перспективы использования данного средства в филиалах компании – масштабируемость, возможность централизованного управления из главного офиса, возможность развертывания, обслуживания и ремонта местным персоналом с учетом его квалификации, потребность в дополнительном персонале или регулярных выездах специалиста из головного офиса;
- стоимость приобретения средства.

Проект, подготовленный с учетом всех перечисленных данных, уже не будет страдать «детскими болезнями». Можно рассчитывать, что средства защиты будут приобретаться с учетом минимизации совокупной стоимости приобретения, эксплуатации и ремонта. Потребность в обслуживающем персонале будет увязана с действительной численностью подразделения информационной безопасности – то есть либо приобретаются более дорогостоящие средства, требующие меньших затрат времени на администрирование, либо планируется найм дополнительного персонала с учетом фактической потребности времени на администрирование более дешевых систем. В таком варианте специалист по безопасности будет гарантирован от неприятных сюрпризов по ходу реализации своих планов, а непроизводительные затраты сил и средств существенно сокращаются. ●

1 Начинающий работать в компании среднего бизнеса.
2 Зарплата специалиста – тоже предмет экономии, поэтому в экономную компанию приходят, как правило, специалисты «второго эшелона».
3 Увы, дешевые IT-специалисты тоже иногда предпочитают бесплатные программные решения типа пакетных фильтров, ClearOS или IPCop.
4 Security Essentials и Avira не предлагать!
5 Автор остается при своем мнении, несмотря на то, что ему известно о существовании компании Cisco Systems.
6 По крайней мере выполняет все задачи, перечисленные в руководстве по эксплуатации.
7 А также по мере возможности исправлять допущенные при проектировании системы безопасности ошибки.