Скачать или не скачать: вопрос на миллион

Александр Кулибаба,
партнер компании «1Форма»

Платить или не платить за программное обеспечение – выбор каждого. Ответственность невелика. Поэтому сегодня мы расскажем, как определиться окончательно со своими интересами и в случае чего избежать неприятностей.

Как известно, Россия признана самой быстро читающей нацией. Российская скорость чтения равна 100 000 слов в минуту, подсчет был сделан на базе статистики прочтений лицензионных соглашений и нажатия кнопки «Согласен» под ним.

Шутки шутками, но в мировом сообществе известны случаи, когда этой скоростью пользуются сами производители ПО и вставляют в текст фразы, например, такого характера: «...и вы должны будете в случае согласия заплатить нам 100 000 евро». Неплохо, да?

Удивительная штука – в России каждые 7 из 10 опрошенных людей выступают за защиту интеллектуальной собственности. Но все же по неизвестной причине 47% пользователей приобретают программное обеспечение незаконным путем.

Можно долго рассуждать о том, надо ли платить за ПО или нет – это, на мой взгляд, вопрос морали и социального сознания. Моя цель рассказать вам, как правильно делать и первое и второе!

Как не платить

Как заметила моя коллега, можно использовать аналоги. Безусловно, можно, но вы их видели? Я понимаю, что Open Office – это бесплатно и практически так же функционально, как MS Office, вот только радости при работе с ним я не испытываю, да и странно там как-то все. Вроде все так же, но непривычно, а значит неудобно.

Или, например, вместо Windows всем поставить Linux – тоже вариант, но начинаются проблемы с нашими любимыми программами, такими как 1 С, различными играми и даже корпоративный портал, написанный нашим про-

граммистом, перестал работать из-за смены браузера. Ну, собственно, сколько платите, такой и программист.

Исходя из вышеперечисленного, делаем вывод – работать с аналогами неудобно!

Более того, использование аналогов не защитит нас от выемки информации при проверке офиса и компьютеров. В руки правоохранительных структур попадут наши базы, переписка, документация вне зависимости от того, лицензионное это ПО или нет.

И это, на мой взгляд, гораздо более важный вопрос. Надо спрятать информацию и программы от посторонних глаз. Сделать это можно несколькими способами.

Зашифровать серверы и компьютеры

Существует большой перечень программных средств для шифрования данных. Я остановлюсь на двух: бесплатный TrueCrypt и платный Z-Server (ну за одну программку, думаю, можно заплатить).

И первая и вторая программы полностью шифруют жесткие диски ваших компьютеров и серверов. Более того, у Z-Server есть замечательная опция «Кнопка «Паника» – у вас на рабочем столе будет ярлычок, и у охраны будет ярлычок, при нажатии на который вся информация в офисе будет моментально зашифрована.

Если такой жесткий диск попадет в руки правоохранительных структур, то они не смогут даже понять, какие там стоят программы, не говоря уже о том, чтобы разобраться в вашей информации. С точки зрения проверяющих органов – это будет информационный мусор, проку от которого ноль.

По закону РФ у вас могут забрать оборудование для проверки на неограниченный срок. С одной стороны, сложно будет понять изъятую информацию, с другой стороны, можно просто не отдавать вам ваше оборудование. Вы же не будете каждый раз покупать для себя новые комплекты компьютеров и серверов? Или будете?

Более того, важным моментом остается организация и хранение резервных копий, которые тоже нужно шифровать (Z-BackUP это умеет).

Здесь тоже не все так просто. Например, один мой знакомый бизнесмен каждую ночь делает полный бэкап всей имеющейся информации. Утром к нему в офис приходит человек, которого знает только он и начальник СБ.

Они отдают этому человеку ленты с резервной копией. Он их везет на противоположный конец Москвы и кладет в депозитную ячейку, оформленную на третье доверенное лицо, не имеющее отношения к бизнесу моего знакомого.

Вы спросите, зачем так сложно? Дело в том, что при наличии судебного решения могут быть вскрыты депозитные ячейки сотрудников компаний или лиц, косвенно относящихся к организации. А у моего знакомого комар носа не подточит.

Резюмируем: можно защитить информацию и скрыть имеющиеся нелицензионные программы, но возникают сложности иного характера. Переходим к способу «Номер 2».

Вынос серверов на зарубежные площадки

Выглядит это так: у вас в офисе на всех компьютерах Linux, а все серверы с бизнес-информацией – где-то в Германии. Сотрудники приходят на работу, включают компьютеры и подключаются терминально к удаленным рабочим столам, а там их ждут привычный интерфейс Windows и все необходимые программы.

Как это работает? Вы арендуете в странах с нормальной юридической культурой стойки для размещения серверов, ставите туда свои серверы.

По закону и по факту, для того чтобы правоохранительные структуры смогли получить доступ к информации на таких серверах, им придется обращаться к Интерполу, и то не факт, что информацию предоставят. Не буду вдаваться в юридические аспекты, но если все правильно сделать – это так.

Резюмирую: в компьютерах в офисе нет никакой информации и никаких платных программ.

Вся информация лежит на серверах, которые недоступны для проверки. Вопрос с резервными копиями решен автоматически.

Никто не имеет права зайти на ваш сервер, чтобы поискать там нелицензионные программы. Минусы: ваш бизнес зависит от Интернета, а значит, расходы на связь существенно возрастут.

Как правило, это решение подходит крупным или богатым компаниям с несколькими сотнями компьютеров.

Как платить

Для начала проведите аудит программ, которые используют ваши сотрудники. Разошлите всем письма и попросите предоставить список программ, с которыми они работают ежедневно. Обязательно напишите, что все остальные будут заблокированы.

После этого опроса попросите ИТ-директора просеять список, оставив лишь необходимые программы.

Далее проанализируйте, сколько человек у вас постоянно работает в офисе, а сколько разъездных. Исходя из полученной информации, вы сможете понять, какие типы лицензий вам нужны: терминальные или нет.

Посоветуйтесь с ИТ-директором и подберите подходящий вашей организации тип лицензирования программных продуктов от компании Microsoft: есть аренда, а есть выкуп.

А теперь самое печальное. Выделите бюджет и начинайте постепенно закупать необходимое ПО. После того, как вы все купите, вам остается только одно – не попасться!

Все насмарку!

Вы можете все оплатить, все настроить, но потерпеть неудачу и получить штрафы при проверке.

Происходит это по нескольким причинам.

Например, вы приходите домой и ваш ребенок с радостным криком: «Папа (или мама) пришел (пришла), наконец-то я поиграю!» – забирает у вас рабочий ноутбук. Через час на вашем законопослушном ноутбуке 10 новых игр, каждая из которых стоит 200 долларов. В итоге это 2000 долларов или 60 000, а это уже до года лишения свободы.

Или, например, ваши сотрудники качают музыку с популярных музыкальных ресурсов и пересылают ее друг другу, а это нарушение авторских прав. Вы готовы возместить певице Максим ее потери с продаж?

Самое важное

Какой путь вы бы для себя ни избрали, вам нужно четко контролировать этот процесс. Должны быть выработаны соответствующие регламенты и процедуры, по которым будет осуществляться проверка лицензионной чистоты или защищенности информации.

Мне бы очень хотелось, чтобы ваши инвестиции были оправданны.

Все бизнес-процессы, связанные с закупкой или установкой программного обеспечения, а также процессы ревизионного характера должны быть автоматизированы, чтобы исключить человеческий фактор. Помните, такие фразы, как «я забыл», «я не знал», «я не так понял» могут стоить вам очень дорого! И самое главное! Не нужно думать, что раз речь идет о «программках» – это ответственность ИТ-директора, которая к вам, как к управляющему, не имеет никакого отношения.

Это опасное заблуждение. В конце концов – это ваша компания, ваши деньги, ваш сотрудник!

На западе ИТ-директор – это правая рука управляющего, потому что ИТ-решения позволяют вести бизнес эффективнее, безопаснее, безмятежнее. Недаром Microsoft и Google – это богатейшие компании в мире. Посмотрите на своего ИТ-директора... Вы видите в нем партнера? ■