Государственное регулирование только создает дополнительные риски

написано Александр Астахов | 10 июня, 2023

> *«Бизнес — это не более чем работа. Спекуляция готовыми товарами — это не бизнес, это более или менее пристойная разновидность воровства. Но законом ее не запретишь. Законы вообще мало на что годятся. Они не несут в себе ничего конструктивного… Пока мы будем рассчитывать на то, что законодательство избавит нас от бедности или запретит особые права и привилегии, до тех пор нищета будет распространяться, а привилегии расти».*
>
> *Генри Форд, один из самых честных предпринимателей, «Моя жизнь, мои достижения»*

Указ Президента РФ № 351 от 17 марта 2008 года фактически разрешил подключение систем, содержащих государственную и служебную тайны, к сети Интернет. Единственным необходимым условием для такого подключения служит использование сертифицированных средств защиты информации (СЗИ).

Может ли государственная система сертификации СЗИ предоставить необходимые гарантии защищенности от интернет-угроз — вопрос риторический. Сертификацию даже нельзя рассматривать в качестве защитной меры. Это, скорее, официальная процедура подтверждения заявленных производителем свойств продукта и соответствия установленным требованиям.

Не говоря уже о том, что сертификация СЗИ в общем случае достаточно длительная и дорогостоящая процедура, которая далеко не всегда экономически оправдана, особенно когда речь идет о современных динамически изменяющихся информационных системах с непрерывным циклом установки программных коррекций,

обновлений баз данных, внедрения новых приложений и т.п. Цикл разработки новых версий ПО зачастую короче цикла его сертификации. В то же время стоимость сертификации и аттестации может быть сопоставима со стоимостью самой ИС. Оправдано ли такое удорожание?

Сертификация в области ИБ преследует две цели: предоставление гарантий отсутствия в средствах обработки информации недекларированных возможностей и подтверждение качества (эффективности) продуктов.

Первая цель достигается только в том случае, если анализу на недекларированные возможности подвергаются все программные (и аппаратные) компоненты ИС, что достижимо только для особой категории критичных систем.

Для достижения второй цели требуются четко определенные критерии оценки, коими должны служить в данном случае профили защиты, которые сегодня в дефиците, т.к. практическое внедрение международного стандарта ISO 15408 «Общие критерии оценки безопасности информационных технологий» затянулось в России на неопределенно долгий срок.

Если же нет возможности анализа всех компонентов системы, а глубоко проработанные и согласованные критерии сертификации отсутствуют, как это в основном происходит на практике, то желаемого эффекта не достигается и сертификация превращается в формальную разрешительную процедуру. Таковой она и воспринимается всеми участниками рынка. В результате средства, которые необходимо было бы потратить на реализацию практических мер по защите информации, расходуются на бюрократические бумажные процедуры.

Вопрос даже не в том, правильно или неправильно подключать критичные государственные информационные системы к Интернет. Вспомним, что отмененный Указ Президента № 611 от 2004 г. явным образом *запрещал* «осуществлять включение ИС, сетей связи и автономных ПК, в которых обрабатывается информация,

содержащая сведения, составляющие государственную тайну, и служебная информация ограниченного распространения в Интернет». Дебаты вокруг этого Указа не утихали. Предлагались различные трактовки понятия «включения в состав сети», обыгрывались словосочетания «логическое и физическое, прямое и опосредованное включение», появлялись даже сертифицированные СЗИ, предназначенные для подключения государственных организаций к Интернет с соблюдением требований Указа № 611 (явным образом запрещавшего такое подключение). Жизнь все равно, как говорится, шла вперед.

Похожая ситуация существует и вокруг Указа Президента № 334 от 1995 года, который запретил использование государственными организациями шифровальных средств, не имеющих сертификата ФАПСИ, а также ввоз на территорию РФ шифровальных средств иностранного производства без разрешения ФАПСИ. Криптографические средства в настоящее время входят в состав операционных систем, телекоммуникационного оборудования, повсеместно используемых приложений, СЗИ, как отечественных, так и импортных, поэтому выполнение запрета на их использование представляется фактически невыполнимым условием. Примерно в то же время (середина девяностых) до России «дошел» Интернет. И вопрос ввоза чего-либо программного через таможенные границы фактически отпал, т.к. у пользователя сети с тех пор всегда есть под рукой практически любые криптосредства, которые ниоткуда привозить не требуется. Поэтому вопрос ввоза импортных шифровальных средств перешел в риторическую плоскость и под запрет, явным образом попадают лишь специализированные аппаратные криптографические модули.

В 2007 году в Постановлении Правительства РФ N 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» были сделаны уточнения, позволяющие распространять лицензирование не на все в подряд криптографические средства, тем не менее, вопросы, связанные с применением криптографических средств остаются достаточно сложными с

правовой точки зрения.

Мы уже много раз видели на примере не только России, но и других стран, что государственное регулирование в области защиты информации проблемы зачастую не решает, а, напротив, создает дополнительные трудности для бизнеса.

Требования по защите информации в этом случае определяются не на основе оценки рисков, а «спускаются сверху», что не способствует их осмысленному применению. При этом многие риски безопасности игнорируются. Реальная деятельность по защите информации заменяется «бумажной работой». Соответствующим образом оформленные лицензии, сертификаты и аттестаты соответствия нормативным требованиям означают с точки зрения государства, что у вас все хорошо. У вас же не остается ничего, кроме впустую истраченного бюджета на информационную безопасность и ложного чувства защищенности.

Негативные последствия государственного регулирования в сфере информационной безопасности:

- *Деньги тратятся на «бумажную» безопасность.*
- *Возникает ложное чувство защищенности.*
- *Возникают дополнительные юридические риски для бизнеса.*
- *Запретительные меры препятствуют осуществлению деятельности.*
- *Реальные риски игнорируются.*

Разрешительно-запретительные меры – это фактически единственный доступный государству способ регулирования чего-либо. Запретить подключение к Интернет, запретить использование шифровальных средств, запретить установку несертифицированных средств, запретить деятельность без лицензии и т.п. Польза от таких мер не всегда очевидна, а для

бизнеса это всегда создает дополнительные барьеры и юридические риски.

Все эти рассуждения касаются не только России. В отчете американского Офиса Менеджмента и Бюджета Конгрессу о реализации Федерального Акта по управлению информационной безопасностью 2002 г. с гордостью сообщается о том, что 85% ИТ систем федеральных агентств были сертифицированы и аккредитованы, что на целых 19% больше по сравнению с предыдущим годом. Количество систем с протестированными планами обеспечения непрерывности бизнеса увеличилось с 57% до 61%. Департамент по делам ветеранов сообщил о том, что все 585 принадлежащий ему ИТ систем были сертифицированы и аккредитованы. Однако проверка отчетов о сертификации, проведенная одним из агентств, показала, что все испытания выполнялись поверхностно. Многие компании, проводившие сертификации, признаются, что их отчеты и заключения даже не читались заказчиком, а в этом случае вряд ли можно говорить о каких-либо улучшениях. Количество выданных лицензий и сертификатов стремительно увеличивается, а безопасность остается на прежнем уровне. Миллиарды долларов американских налогоплательщиков были истрачены на бесполезную бумажную работу. Подтверждением тому служит нашумевшее в США «дело ветеранов».

В 2006 году данные о 26,5 млн. ветеранов и членов действующего резерва национальной гвардии и резервных войск США были украдены у служащего агентства, который отнес свой ноутбук домой. Незашифрованные данные, включавшие номера социального страхования и прочую информацию о ветеранах и их супругах, были скомпрометированы.

«Дело ветеранов» – крупнейшая утечка данных в истории США и ярчайший пример, который выдвинул на первый план потребность в

тщательном рассмотрении вопросов информационной безопасности в правительстве США. Хотя, насколько нам известно, положение дел с безопасностью там заметно не улучшилось, а законы и нормативная база после того случая особо не изменились.

Как говорил выдающийся предприниматель Генри Форд, один из тех, кто в свое время вытащил Америку из «великой депрессии», «законы мало на что годятся… в них нет ничего конструктивного». Вопрос не в том, правильно или нет запрещать либо разрешать подключение к Интернет, использование несертифицированных СЗИ, импортные СКЗИ и т.п. Действительно важный вопрос заключается в том, кто и каким образом оценивает риски в каждом конкретном случае, какие возникают риски и что с ними делать. На этот главный вопрос вам не смогут дать ответ ни законодатели ни регуляторы. Этот ответ каждой организации приходится искать самостоятельно.