

## Как защищать информацию с доверием

Информационные системы всё глубже проникают в нашу жизнь, с ними современный человек сталкивается на каждом шагу и в профессиональной деятельности и в быту. Мы перестали бояться предоставлять им то, что имеет для нас значительную ценность: персональные данные, финансы и многое другое. На чем же основывается наша вера в то, что самими информационными системами или через них нам не будет нанесен вред или более правильно ущерб, что нас убеждает в безопасности ИС?

В тех областях, где вопросы безопасности регулирует государство, а это государственные информационные системы, информационные системы персональных данных, системы критических приложений, криптографическая защита информации – ответ напрашивается такой: «потому, что они защищены в соответствии с требованиями нормативных правовых документов». И по форме это верно, а по сути? Является ли это утверждение основанием для **доверия** к безопасности информационных систем? А как обрести доверие к безопасности информационных систем тем, на кого не распространяется действие нормативных правовых актов по защите информации? Давайте попробуем с этим разобраться.

Но предварительно необходимо сделать одно важное замечание. Мы отнюдь не хотим посеять недоверие к принятым в государстве нормативным правовым актам и сомнения в необходимости их соблюдения. Нет и ещё раз нет. Нормативные правовые акты требуют от нас принятия необходимого базового комплекса мер, направленных на обеспечение безопасности информации и информационных систем и, соответственно, обеспечивают базовый уровень доверия к безопасности. Но тот, кто хочет иметь **большую** уверенность в своей защищенности может принимать направленные на это дополнительные меры безопасности, которые обеспечивали бы **большую** уверенность в безопасности. Тому, как этого достичь с использованием современных стандартов и лучших мировых практик и будет посвящена открываемая рубрика «Тем, кто хочет защищать информацию с доверием».

На чем основывается наше доверие к чему-то? Например, к автомобилю, самолету или электронному устройству? На репутации производителя, на результатах испытаний, обязательной или добровольной сертификации, на отзывах. Мы знаем, что японские автомобили и электроника, немецкая бытовая техника надежные, а автомобили, электроника и бытовая техника некоторых других производителей, не будем упоминать каких, не совсем. А почему? А потому, что разные производители по-разному относятся к процессам разработки и производства своих продуктов и систем, по-разному их

организовывают, затрачивают разные ресурсы и средства на отработку и испытания, используют различные комплектующие. У них разная система качества разработки и производства продукции. И мы, как правило, с недоверием относимся к продукции, хотя и имеющей очень богатый функционал, но произведенной не внушающим доверия производителем, потому что знаем, что они могут скоро вообще перестать работать и намучаешься их ремонтировать.

Доверие к продукции, её высокое качество, заслуга ли это только её производителя? Нет, в этом значительную роль играет государство, которое посредством своей нормативной правовой деятельности определяет требования к производителям, к их системам качества, сертифицирует их и осуществляет за ними государственный контроль и надзор. Как говорил Глеб Жеглов: «правопорядок определяется не наличием воров, а умением властей их обезвреживать!»

Вернемся теперь к защищенности информационных систем. Какую информационную систему можно считать защищенной? ГОСТ Р 51624—2000. Защита информации. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. Общие требования дает следующий ответ на этот вопрос: «Автоматизированная система в защищенном исполнении — автоматизированная система, реализующая информационную технологию выполнения установленных функций **в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации**». Ответ точный, но не очень информативный. Как в анекдоте про летящих на воздушном шаре, потерявших ориентацию и спрашивающих человека, над которым пролетают: «Мы где?». Ответ получают абсолютно точный и абсолютно бесполезный: «Вы на воздушном шаре».

Другое определение защищенной АС дается в Специальной публикации NIST 800-53 «Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций»:

*Доверенная информационная система - система, которая способна к действию в границах определенных уровней риска, несмотря на экологические разрушения, человеческие ошибки, структурные отказы и целеустремленные атаки, которые, как ожидается, могут произойти в среде её эксплуатации.*

В чём разница между этими определениями? Первое верно по форме, а по сути, с точностью до совершенства стандартов и/или иных нормативных документов по защите информации. Второе верно по сути, но по форме может не обеспечивать соответствие требованиям установленных стандартов и/или иных нормативных документов по защите информации.

В идеале нужно и то и другое. То есть, необходимо, чтобы информационная система удовлетворяла требованиям установленных стандартов и/или иных нормативных документов по защите информации, но и понимать, обеспечивает ли это требуемый уровень риска нарушения информационной безопасности или, по-другому, достигается ли необходимая степень доверия к безопасности информационной системы.

В том, как обеспечивать качество продукции, доверие к ней, особого секрета нет, все секреты изложены в международных стандартах по системам качества известной серии международных стандартов ISO/IEC 9000. Есть такая серия стандартов и в области информационной безопасности - ISO/IEC 27000, а также такие требования есть в специализированных стандартах по безопасности информационных систем, ISO/IEC 19791, и продуктов информационных технологий, ISO/IEC 15408. В приложении к безопасности информационных технологий эти требования так и называются: требования доверия (assurance requirements).

Что же такое доверие по отношению к безопасности продуктов и систем информационных технологий? С точки зрения информационной безопасности доверие это степень уверенности в том, что сущность, важная для безопасности, будет вести себя предсказуемым образом, удовлетворяя определенному набору требований безопасности при указанных условиях, подвергаясь разрушениям, человеческим ошибкам, сбоям, отказам и целеустремленным атакам, которые могут произойти в среде эксплуатации.

Требования доверия направлены на то, чтобы обеспечить принятие разработчиком и эксплуатирующей организацией таких мер, которые обеспечивали бы достаточный уровень уверенности в безопасности информационной системы. Таким образом, чем жестче требования доверия, тем большую уверенность мы можем испытывать в безопасности информационной системы.

В действующей российской нормативной базе в области безопасности информационных систем вопросам обеспечения доверия к безопасности информационных систем почему-то уделяется недостаточное внимание. Они полностью отсутствовали в нормативной базе образца 90-х годов, не нашли они, к сожалению, прямого отражения и в последних нормативных актах по безопасности информационных систем. Следует отметить, что в отношении продуктов информационных технологий такие требования к счастью есть и содержатся они в принятом руководящем документе ФСТЭК России «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ». Критерии оценки безопасности информационных технологий», и выпускаемых в последнее время ФСТЭК России документах по конкретным видам продуктов информационных технологий.

А вместе с тем, в нормативной базе ведущих зарубежных стран доверию к безопасности информационных систем уделяется определяющее значение. Вот, например, как трактует значение доверия к безопасности информации и информационных систем нормативный документ американского Национального института стандартов и технологий 800-53 «Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций»:

*При возрастании значимости безопасности для организации и повышении восприимчивости информационных систем к постоянным развивающимся угрозам нарушителей с высоким потенциалом не только имеют смысл, но требуются повышенные уровни доверия. Кроме того, поскольку организации становятся более зависящими от внешних сервисов информационных систем и поставщиков, доверие становится всё более важным, обеспечивая большую способность проникновения в суть и степень уверенности организаций в понимании и проверке возможностей безопасности внешних поставщиков и услуг, предоставленных федеральному правительству. Таким образом, когда потенциальное воздействие на деятельность и активы организаций, людей, другие организации или Нацию является большим, увеличивающийся уровень усилия должен быть направлен на обеспечение доверия.*

Таким образом, подводя итог можно сказать, что защищенной может называться любая информационная система, которая удовлетворяет требованиям действующих в государстве стандартов и/или иных нормативных документов по защите информации, а вот доверенными можно считать только те из них, для которых разработчики и эксплуатирующие организации принимают необходимые меры доверия, соответствующие положениям современных международных стандартов и лучшим мировым практикам.

В настоящем разделе мы будем помещать материалы, которые будут помогать добросовестным разработчикам и эксплуатирующим организациям применять меры обеспечения безопасности которые обеспечивали бы доверие к их информационным системам.

Одновременно с собственно нормативными и методическими документами по безопасности информационных систем мы будем публиковать также и некоторые законодательные акты, характеризующие политику государств в сфере информационной безопасности, определяющую выпуск соответствующих нормативных документов.