50 оттенков «красной кнопки»

Как выясняется, существуют стратегические технологии в области IT и ИБ, которыми «западные коллеги» с отечественными разработчиками не желали делиться даже до начала геополитической турбулентности



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

«Это важная тема, которую необходимо обсудить в подробностях», — так отреагировала председатель Банка России **Эльвира Набиуллина** на выступление **Юрия Максимова,** сооснователя компании Positive Technologies и Фонда развития результативной кибербезопасности Cyberus, в ходе пленарной сессии на FINOPOLIS еще в 2024 году.

Речь шла о так называемом функционале «красной кнопки», когда 19 июля 2024 года ИБ-компания CrowdStrike распространила ошибочное обновление своего ПО безопасности Falcon Sensor, которое вызвало массовые проблемы с компьютерами на Microsoft Windows. В результате примерно 8,5 млн систем вышли из строя, а инженеры не смогли сразу должным образом перезапустить их. Эта катастрофа была названа крупнейшим отключением в истории IT.



И снова Microsoft

В мае 2025 года некоторые детали обещанной дискуссии попали в публичное поле, и стало понятно, что «кнопка»-то не одна, их множество. В частности, эксперты указывали на массовый сбор неназванными западными спецслужбами чувствительной зашифрованной переписки, с тем чтобы при появлении достаточно производительных квантовых компьютеров взломать шифр. А вот американские конгрессмены прямо сейчас разрабатывают законопроект, который обяжет производителей графических карт отслеживать места использования своей продукции. А еще в последнее время неожиданно стали массово происходить самые неприятные случаи с представителями криптоиндустрии. Все эти и другие факты говорят о централизованном управлении этими если не кибератаками, то чувствительными инцидентами с вполне понятными целями.

Но вот тот факт, что подобная практика западных вендоров по отношению к России и другим странам началась довольно давно, по разным причинам не афишировался. Возможно, первым, кто поднял эту тему публично и без обиняков, помимо Юрия Максимова оказался генеральный директор компании «Аладдин Р.Д.» **Сергей Груздев.**

Он признал тот факт, что в случае намеренного или случайного отключения такого компонента ОС Microsoft, как Certificate Authority (CA), отвечающего за аутентификацию пользователей, компьютеров и организаций, а также являющегося ключевым компонентом в инфраструктуре открытых ключей (PKI), практически любая IT-инфраструктура, базирующаяся на Microsoft, буквально за сутки может развалиться на независимые компоненты и перестанет функционировать.

На начало 2025 года, по словам Сергея Груздева, «почти все российские IT-инфраструктуры имели точку отказа и “рубильник” для отключения из-за рубежа благодаря повсеместному использованию Microsoft CA» (цитируется по CNews).

На вебинаре 15 мая 2025 года «Аутентификация — от паролей к 2ФА, биометрии и адаптивной МФА» эксперт напомнил, что многолетняя работа в экосистеме Microsoft притупила чувство бдительности, поскольку все верили американскому вендору в части вопросов идентификации и аутентификации, включая двухфакторную. Не было оснований полагать, что служба Certificate Authority в один прекрасный момент перестанет быть «третьей доверенной стороной» и строгая аутентификация перестанет быть возможной для IT-инфраструктур enterprise-уровня.

Linux для домохозяек

Итак, что может «отвалиться» в любой момент: собственно, CA, отвечающий за выпуск и валидацию сертификатов, служба каталогов MS Active Directory, необходимая для доменной аутентификации, а также клиент PKI и двухфакторная аутентификация (Smart Cart Logon).

Встает естественный вопрос: «А почему в импортозамещенной экосистеме Linux нельзя было раньше сделать так, как в Microsoft?». Ответ простой и удручающий: «В Linux нет полноценного PKI enterprise-уровня, а без PKI Linux превращается в историю для физлиц и домохозяек». Поэтому бесшовно перевести, например, банк или страховую компанию на Linux до начала 2025 года было тем еще квестом, а выполнить требования регулятора в части строгой аутентификации и безопасного доверенного взаимодействия и коммуникаций всех IT-систем и пользователей как внутри, так и снаружи банка невозможно. Известно, что театр начинается с вешалки, а ИБ — с идентификации! На этом можно было ставить точку.

Довольно долго отечественные вендоры ОС не могли преодолеть колоссальных сложностей при ликвидации ИБ-пропасти между Windows и Linux. На сегодня большинство компонентов полного стека PKI и многофакторной аутентификации реализованы. Поэтому, видимо, и пришло время вендорам рассказать о том, по краю какой пропасти пришлось проходить.

Почему же на этот раз не очень-то помогло наше все — Open Source? Те финансовые организации, которые пошли в тему импортозамещения MS CA, порой даже превосходят уровень классического enterprise-уровня, и для них не существовало достаточно производительных решений.

Функционал «красной кнопки» был заложен в свое время компанией Microsoft, а технологии тщательно оберегаются от попадания в руки геополитических конкурентов



Сергей Груздев: После пяти минут приятного общения, когда выяснилось, что звонят из России, разговор немедленно прекратился

30–40% ПО в данном сегменте, хоть и представлено под лицензией Open Source, но по факту им не является, поскольку поставляется в бинарном виде, рассчитанном на разные технологические стеки. Поэтому все «валилось» даже у самых опытных внедренцев уже при превышении нагрузки от 200 пользователей.

И вот главное, что рассказал Сергей Груздев: «Еще до начала СВО мы занялись проблемой PKI и, зная, что существует несколько enterprise-проектов на базе Linux, попытались договориться с одним из них, голландско-французского происхождения. После пяти минут приятного общения, когда выяснилось, что звонят из России, разговор немедленно прекратился. Это стратегическая технология, и обсуждению с вами она не подлежит!».

Иными словами, функционал «красной кнопки» был заложен здесь в свое время компанией Microsoft, а технологии тщательно оберегаются от попадания в руки геополитических конкурентов партнерами этого вендора и отчасти конкурентами. Это было даже до начала СВО!

Что имеем на выходе?

Первый публичный кейс в сфере CA был представлен в ходе 25-го Международного форума по электронным финансам iFin-2025 в феврале 2025 года. Им поделился Т-Банк, завершивший миграцию с центра сертификации Microsoft CA на отечественное решение SafeTech CA.

Пилотный проект в кредитной организации продлился 4,5 месяца. В ходе тестирования было проверено множество различных сценариев использования CA во внутренней инфраструктуре банка, возможности API в части интеграции во внутренние бизнес-процессы и даже возможности команды разработки вендора на предмет доработок тех или иных дополнительных функций.

Главное, что продемонстрировал этот кейс: в таком крупном банке на практике удалось показать, что для миграции можно какое-то время работать параллельно с обоими CA, постепенно переводя всю инфраструктуру, сотрудников и клиентов на отечественное решение.

Компании «РЕД СОФТ» и «Аладдин» внедрили свой совместный продукт для ключевого заказчика в лице оператора IT-инфраструктуры группы «Газпром» — «Газпром информ», а Сбер, как обычно, решил проблему своими силами.

Что касается российских альтернатив Microsoft Active Directory, то уже есть из чего выбрать и на какие кейсы ориентировать. Убедиться в этом можно из эфира AM Live от 16 мая 2025 года, где свои решения представили компании Avanpost, «РЕД СОФТ», «Группа Астра», «НТЦ ИТ РОСА» и другие.

Почему это важно? На службы каталогов завязана работа множества других ИБ-систем, в частности решений в области защиты от утечек данных DLP, что в свете ужесточения регулирования ПДн немаловажно. Важно и то, что для СМБ остались доступны Open Source-продукты — FreeIPA, Samba, OpenLDAP. Таким образом, целая отрасль нашла защиту от одной из «красных кнопок», приобретя при этом колоссальный опыт, доступный ранее лишь избранным вендорам. **Б.О**