Сергей Груздев: переоценка киберугроз, выявление и устранение точек отказа при построении безопасной доверенной ИТ-инфраструктуры

На прошедшей с 12 по 14 сентября 2023 года XXI международной конференции по проблематике инфраструктуры открытых ключей и электронной подписи (PKI-форум) прозвучало немало ярких докладов, вызвавших глубокий интерес участников. Одним из наиболее резонансных стало выступление генерального директора компании „Аладдин" Сергея Львовича Груздева. В состоявшейся по завершении форума беседе с ним мы не только попросили его более подробно раскрыть проблематику выступления, но и затронули ряд «смежных» с ней вопросов.

Сергей, тема вашего выступления на PKI-форуме была не вполне традиционной для этого мероприятия. Регламент не позволил обсудить его непосредственно в зале, но сразу же по завершении сессии многие участники конференции подходили к вам за дополнительной информацией. Расскажите, пожалуйста, об этом.

Действительно, я затронул довольно больную тему, которая на конференциях обычно не поднимается, но в свете текущей ситуации стала особенно актуальной. Она имеет непосредственное отношение к программам импортозамещения, в соответствии с которыми мы вынуждены переходить на ОС Linux. Однако начну чуть издалека.

На ключевой дискуссии PKI-форума

На последних конференциях по информационной безопасности, проходивших после начала СВО, активно обсуждались проблемы, связанные с ушедшими зарубежными вендорами и необходимостью замещения их решений российскими. Также систематически фиксируется рост успешных атак на наши организации, утечек персональных данных, баз данных, содержащих критическую информацию.

Такое ощущение, что для многих на рынке информационной безопасности ничего не изменилось. Вместо смещения фокуса нашего внимания на разработку и внедрение средств, направленных на недопущение утечек и успешных атак, по-прежнему предлагаются продукты по мониторингу атак, разбору инцидентов, улучшению инструментов для получения статистики и аналитики атак и инцидентов.

Мы все еще движемся по инерции, боремся с «плохими парнями», пытающимися взломать наши информационные ресурсы, эксплуатировать уязвимости, подсаживать нам

вирусы-шифровальщики, улучшаем защиту периметра, каналов связи…

Да, все это надо делать и улучшать. Только мы совершенно упускаем из внимания, что мир кардинально изменился. И те риски и угрозы, которыми мы позволяли себе пренебрегать до СВО и считали их ничтожными, теперь «сыграли» по полной и стали нашей главной головной болью, часто затмевая все остальные.

Большинство до сих пор не до конца понимает, кто наш враг: кто нас атакует и от кого надо защищаться? Многие до сих пор искренне считают, что их-то уж точно пронесет. Выполнил на бумаге основные требования регуляторов и дело с концом!

Сегодня для всех должно стать совершенно очевидным, что мы неправильно оценивали политические риски, архитектурные уязвимости, критические технологические зависимости и продолжаем тратить наши ИБ-бюджеты на борьбу с навязанными нам угрозами.

Так вот, сейчас, как мне кажется, самое время остановиться, системно и всерьез переоценить риски и угрозы для наших ИТ-инфраструктур. Подумать, что и как мы понастроили под сладкие рассказы западных вендоров, в том числе про облачные сервисы, Security-as-a-Service и прочие модные веяния, обнаружить и устранить точки отказа.

И какова цель такого анализа?

Вспомним принятую в марте этого года новую национальную стратегию кибербезопасности США. Сейчас не ручаюсь за точность приведенных в ней формулировок, но суть в целом передам верно:

- не дожидаться кибератак на объекты критической инфраструктуры США, а действовать на упреждение;
- приоритетные цели для атаки на инфраструктуру противника – это объекты энергетики, органы государственного и военного управления, транспортная инфраструктура;
- для блокирования и вывода из строя ИТ-инфраструктуры организаций КИИ противника задействуются все имеющиеся возможности.

Несмотря на все события последних полутора лет, мы до сих пор верим, что этого не произойдет, а ведь многое уже сделано, вопреки экономике, здравому смыслу и нашим ожиданиям: заблокирована работа западных платежных систем, ряд крупных банков отключен от SWIFT, «перекрыт кислород» производству российских процессоров и другой электроники на фабрике TSMC. А чего мы ждали и зачем сложили все яйца в одну корзину? Нам отключили облачные сервисы, в том числе и критичные для бизнеса – облачную аутентификацию корпоративных пользователей.

Однако это далеко не полный АРСЕНАЛ СРЕДСТВ, имеющийся в ИХ распоряжении. И здесь уместно вспомнить про знаменитую фразу Барака Обамы, сказанную им в 2015 году: «Россия изолирована, а ее экономика разорвана в клочья. Это свидетельствует о лидерстве США, которого они добиваются не пустыми словами, а принятием последовательных и уверенных решений». Тогда над ней многие посмеялись. Но это были не пустые слова…

Например, документы PPD-20 и Cloud Act, подписанные администрацией США, регламентировали:

- возможность закладки в объекты КИИ недружественных государств кибербомб, которые при необходимости можно привести в действие для вывода из строя системы командования и контроля вооруженных сил противника, объектов его критически важной инфраструктуры;
- обязанность американских вендоров осуществлять сбор и передачу в АНБ, ЦРУ и ФБР так называемой телеметрии;
- запрет американским вендорам на передачу и/или раскрытие исходных кодов ПО и прошивок «железа» другим государствам;
- задание ЦРУ на разработку маскировочных программных средств проведения компьютерных атак, в том числе под «чужим флагом».

США задолго до начала СВО начали готовиться к серьезному противостоянию с Россией: знания о том, на каком оборудовании и в какой среде работает та или иная информационная система, о заложенных в ее компоненты уязвимостях и закладках позволят быстро и эффективно парализовать ее работу и вывести из строя данный объект КИИ.

Все это должно было стать для нас серьезным звоночком. Тем более что американцам свойственно, если посмотреть в историю, заранее «разогревать публику», готовить позиции с точки зрения формирования общественного мнения. Очень бы хотелось надеяться, что этого не произойдет, но… все равно есть ощущение, что нас пока лишь пугали. А раз так, с нашей стороны фокус сейчас должен быть сосредоточен на обеспечении живучести и работоспособности имеющейся ИТ-инфраструктуры и устранении узких мест, способных ее «положить».

И вот мы подошли к тому, с чего я начал: насколько уязвима наша инфраструктура, и при чем здесь PKI. Цифровой суверенитет, говоря попростому, – это когда мы сами понимаем, как устроена наша инфраструктура, когда никто не сможет удаленно нажать на красную кнопку и остановить всю работу. Поэтому начинать надо с ответа на вопрос: а есть ли у нашей ИТ-инфраструктуры ахиллесова пята, воздействие на которую способно ее вырубить.

Судя по всему, есть?

Увы… Ключевой и самый критичный элемент практически в каждой российской ИТ-инфраструктуре – это корпоративный центр выпуска и обслуживания цифровых сертификатов Microsoft CA (*Certificate Authority*).

CA – это основа доверенного взаимодействия всех объектов и компонентов в корпоративной сети. CA выпускает и ПРОВЕРЯЕТ ***машинные*** сертификаты для аутентификации серверов, роутеров, маршрутизаторов, точек доступа и всего прочего оборудования в сети, а также программные и пользовательские сертификаты доступа.

Проблема № 1 состоит в том, что работоспособность практически лю-

Сергей Груздев на трибуне PKI-форума

бой нашей ИТ-инфраструктуры на 100 % зависит от работоспособности MS CA.

В 2022 году Microsoft ушла из России, представительство закрыто, поддержки MS CA больше нет, купить его тоже нельзя. С 30 сентября текущего года Microsoft перестала продлевать подписки корпоративным клиентам из России, что является серьезной миной замедленного действия, по крайней мере, хотелось бы надеяться, что замедленного.

То же касается и программных сертификатов. Проблему уже могли почувствовать на себе компании, у которых Microsoft отозвала девелоперские сертификаты, как, кстати, и у нас. На мое обращение о причинах такого шага прислали вежливое письмо: мол, извините, но ваша организация признана работающей на правительство.

Судя по всему, мы подобрались к упомянутому в начале беседы импортозамещению и переходу на Linux?

Совершенно верно! И с этим связана проблема № 2: полноценной альтернативы или аналога MS CA под Linux нет, наши надежды на OpenSource не оправдались. Здесь поляна зачищена, то, что на ней можно взять, – это «колбасные обрезки»: 200–300 пользователей, и все начинает рушиться. Это либо «завлекалки», либо поделки, собраннные на старых технологических стеках и платформах, не масштабируемые, без перспективы их сертификации (порядка 40 % проектов – в «бинарниках», без исходных кодов), плохо собираемые и плохо работающие под российскими ОС, массу всего надо переписывать. Словом, это совсем не для Enterprise.

По поводу «завлекалок» корпоративных CA… Есть несколько интересных проектов CA действительно Enterprise-уровня, но все они закрытые и коммерческие. Удалось узнать цену (правда, только на базовый модуль – центр выпуска сертификатов): она космическая.

Кроме того, ни один коммерческий CA Enterprise-класса в Россию не поставляется ни под каким предлогом. Связывались за год до СВО, было сказано (дословно): *«Это стратегический товар, продать корпоративный PKI в Россию – это хуже, чем поставить ядерные технологии в Ирак, словом, забудьте!»*.

Чувствуется, что перечень проблем еще не исчерпан. Какова следующая?

И не одна!

Проблема № 3 – мы вынуждены мигрировать с Windows на Linux, но в Linux'е нет PKI. И здесь мне часто приходится разрушать сложившуюся у очень многих «картину мира», почти как в фильме «Стиляги». Помните сцену в конце фильма, когда герой возвращается из США и говорит другу: «У меня для тебя плохие новости: в Америке нет стиляг».

У меня примерно то же самое: *«Ребята, у меня для вас плохие новости: в Linux нет PKI. А без него это лишь консьюмерская история, а не полноценный Enterprise. Столь же хорошо, когда все необходимое органично встроено и доступно из всех сервисов, удобно, безопасно, то есть так, как это сделано в Windows и к чему мы все привыкли, без поддержки PKI в Linux никогда не будет»*.

В Linux (как в российских, так и в международных проектах) отсутствует не только полноценный аналог MS CA, но и клиентская часть PKI, включая поддержку строгой двухфакторной аутентификации (2ФА) пользователей с применением цифровых сертификатов, как это реализовано, например, в MS Smartcard Logon.

Напомню, что строгая двухфакторная аутентификация пользователей для критических и госсистем – это требование российских ГОСТов по идентификации и аутентификации. Большинство успешных атак и утечек происходит именно из-за неправильно реализованной подсистемы аутентификации пользователей или неиспользования 2ФА и корпоративной PKI.

Это одна из ключевых и критически важных подсистем наших ИТ-инфраструктур, сделать ее правильно – одна из первоочередных задач. Решив таковую, мы сможем предотвратить большое количество инцидентов, и здесь хорошо работает правило Парето: 20 % усилий (и ИБ-бюджета) даст 80 % результата.

Проблема № 4 – совместимость с разными экосистемами.

Многие российские вендоры создают собственные экосистемы. Я не очень люблю это понятие. Существует несколько определений, одно из которых гласит, что *экосистема – это замкнутое, самодостаточное и довольно хрупкое образование (пространство), и любое вмешательство извне способно его разрушить.*

Windows – это тоже замкнутая, большая и вполне устойчивая экосистема. Мы живем и работаем в ней много лет, привыкли, создали множество приложений, и теперь взять и одномоментно перейти в другую замкнутую экосистему (на Linux) никто не сможет. Мы обречены еще достаточно долго поддерживать каким-то образом экосистему Windows, пользоваться ее сервисами и приложениями, которые еще не портированы под Linux, и пытаться работать сразу в двух – Linux и Windows. Наверное, не только наши дети, но и внуки будут вынуждены работать в обеих этих системах, поэтому речь, скорее, надо вести о гетерогенности.

Необходимость параллельной работы в двух экосистемах требует разработки не просто аналога MS CA и MS Smartcard Logon, а гораздо более сложного инфраструктурного ПО, умеющего работать в двух параллельных «мирах», совместимого с раз-

ными домен-контроллерами и службами каталогов: MS Active Directory, Samba DC, FreeIPA, ALD Pro, РЕД АДМ, Альт Домен.

Выходит, построить доверенную ИТ-инфраструктуру Enterprise-уровня и выполнить требования регуляторов для организаций КИИ без разворачивания PKI не получится?

Верно, не получится. Попробую объяснить почему.

Начну с ДОВЕРИЯ. К сожалению, в последнее время это понятие (и термин) сильно замусолили.

Что такое доверие?

В мире людей – *это открытые взаимоотношения между субъектами, предполагающие уверенность одного в порядочности другого, в возможности поделиться с ним личной или сокровенной информацией, в его ответственности не воспользоваться этой информацией вам во вред.*

Применительно к ИТ-технологиям и информационной безопасности это определение тоже работает: *если мы строим безопасную доверенную ИТ-инфраструктуру государственной организации, КИИ, то каждый ее элемент должен быть доверенным, а значит, надежно (гарантированно) идентифицирован и аутентифицирован.*

Здесь мне хочется процитировать В. В. Путина: «*В деле, которым я занимаюсь, нужно оперировать другими категориями – здесь вопрос не в доверии, а в гарантиях*».

Для ИБ также *важнее не доверие, а гарантии.*

Необходимые гарантии дает криптография: гарантированная стойкость, PKI (централизованная инфраструктура открытых ключей), безопасность закрытых ключей в средствах 2ФА – USB-токенах и смарт-картах с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом.

Основа доверительных отношений – надежная АУТЕНТИФИКАЦИЯ всех субъектов ИТ-инфраструктуры: «железа» (серверов, роутеров, маршрутизаторов и т. п.), ПО (ОС, системного, прикладного, служб, сервисов и пр.), пользователей.

Согласно действующим российским ГОСТам по идентификации и аутентификации (которые, кстати, разрабатывала наша компания), имеется три типа аутентификации с разными уровням доверия:

1) простая – обеспечивающая некоторую уверенность в том, что данный пользователь является тем, за кого себя выдает (как правило, в информационных системах – это пара «логин – пароль»);

2) усиленная – обеспечивающая достаточно высокую уверенность, которую дает, как правило, наличие второго фактора (токена или смарт-карты);

3) строгая – обеспечивающая очень высокую степень уверенности, добиться которой можно только с использованием криптографических средств 2ФА.

Для организаций с высоким уровнем значимости информации в ИС, высокой вероятностью и размером возможного ущерба, а это госорганизации, КИИ, необходимо применять СТРОГУЮ аутентификацию.

Как мы помним, реализовать строгую аутентификацию пользователей в ИС можно только с использованием средств 2ФА: USB-токенов и смарт-карт с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом – невзламываемых и неклонируемых, разворачиванием инфраструктуры открытых ключей (PKI), главным компонентом которой и является корпоративных центр выпуска и обслуживания сертификатов доступа (аутентификации) – СА, а также поддержкой средств 2ФА и PKI на клиентском ПО.

Напомню, что в Windows – это Microsoft CA (CS) на сервере (входит в состав Windows Server в качестве «бесплатного сыра») и MS Smartcard Logon, предоставляющий пользователям простой и понятный интерфейс для 2ФА.

Для Linux же, как я уже говорил, картина совсем иная: доверенный СА Enterprise-класса отсутствует (*подчеркну, не следует путать УЦ под Linux для выпуска и обслуживания сертификатов электронной подписи по 63-ФЗ с корпоративным центром сертификации!*). Полнофункционального аналога MS Smartcard Logon, умеющего работать с сертификатами, тоже нет. Чтобы реализовать поддержку средств 2ФА и аутентификацию в Linux с их помощью, придется самостоятельно доработать, установить и настроить порядка 34 пакетов, а это не каждому под силу.

Понятно, но переход на Linux никто не отменит.

Разумеется, но переходим-то пока неохотно! Одна из главных причин – неготовность инфраструктуры. Но часто сверху спускают KPI по импортозамещению, запрещают закупки продуктов под Windows. Получается, что купить ПО под Windows уже нельзя, а инфраструктура на Linux еще нормально не работает. Как мы постарались решить эту проблему для одного из наших продуктов (Secret Disk – система прозрачного шифрования данных на дисках): сделали единую универсальную лицензию для Windows и для Linux, так, чтобы и закупщики были довольны, выполняя свои KPI по «линуксонизации всей страны», и пока не готова инфраструктура, пользователи могли бы продолжить работы под Windows и защитить там свои данные.

Итак, на текущий момент выполнить требования по реализации строгой аутентификации и построить безопасную доверенную ИТ-инфраструктуру организаций КИИ практически невозможно? Что же делать?

Действительно, с помощью имеющихся средств, предоставляемых разработчиками российских ОС на базе Linux, – нет. Но мы с ними активно работаем в этом направлении и уже выпустили на рынок набор ключевых компонентов, необходимых для разворачивания корпоративной PKI на Linux с поддержкой средств 2ФА.

Первый ключевой компонент для построения безопасной доверенной ИТ-инфраструктуры – это Aladdin Enterprise CA – корпоративный центр выпуска и обслуживания сертификатов. Он позволяет заместить такой критичный элемент в инфраструктуре, как MS CA – единую точку ее отказа, о которой я говорил, объединить все компоненты ИТ-инфра-

структуры в единый домен безопасности, обеспечить их аутентификацию и безопасное взаимодействие, одновременно работать с различными службами каталогов как в Windows, так и Linux.

Aladdin Enterprise CA можно поставить параллельно с Microsoft CA, пока тот работает, и от корневого выпустить подчиненный сертификат, настроить его на автоматический перезапуск всех сертификатов, у которых заканчивается срок действия. И если время позволит, в итоге произойдет постепенное эволюционное замещение одних сертификатов другими.

Второй важнейший компонент – это клиент под Linux – Aladdin SecurLogon, обеспечивающий строгую 2ФА пользователей по цифровым сертификатам с применением выпускаемых нами USB-токенов и смарт-карт JaCarta PKI (и это третий важнейший компонент инфраструткуры).

Отмечу, что SecurLogon позволяет аутентифицироваться и в Linux, и в Windows. Причем, и это принципиально, решение «свой – чужой» и разрешение на вход в систему здесь принимает наше доверенное ПО, а не чужое, как в случае с Windows Smartcard Logon. Важно, что SecurLogon имеет привычный для многих интерфейс, как у Windows Smartcard Logon, так что проблем с переходом не возникнет.

Четвертый компонент также относится к инфраструктурным – это корпоративная система централизованного управления жизненным циклом сертификатов, токенов и смарт-карт, средств криптографической защиты и пр. – JMS (*JaCarta Management System*). Именно она позволяет обеспечить учет и контроль выдаваемых сертификатов, средств 2ФА и ЭП, а также включает в себя сервер аутентификации Enterprise-класса.

Внедрять средства 2ФА и PKI без подобной системы централизованного управления – просто утопия.

И здесь я бы хотел отметить еще один, пятый по счету, важнейший компонент, а точнее, подсистему современной ИТ-инфраструктуры любой достаточно крупной организации, обеспечивающую безопасную дистанционную работу сотрудников.

После выступления было много желающих продолжить беседу

Крайне востребованная в период пандемии «удаленка» прочно вошла в нашу жизнь и по ее завершении. Многие сохранили у себя созданные в период пандемии решения. Однако другие предпочли запретить дистанционную работу сотрудников, понимая, что это была вынужденная и очень опасная мера.

Соглашусь с этим мнением: применяемые многими решения для организации дистанционной работы своих сотрудников на базе «служебного ноутбука» очень небезопасны. Почему? Потому что поверхность атаки такого сложного решения огромна – и через недоверенное «железо», и через заложенные уязвимости в процессорных чипсетах, UEFI, протоколах, спецификациях USB и пр.

Мы же в свое время сделали и сертифицировали специализированное решение для обеспечения безопасной дистанционной работы сотрудников органов исполнительной власти при использовании ими недоверенных средств вычислительной техники – Aladdin LiveOffice.

Это решение позволяет загружать со специализированного защищенного USB-носителя изолированную замкнутую доверенную программную среду практически на любом компьютере, и из нее по защищенному каналу подключаться к своему виртуальному рабочему столу или к своему служебному компьютеру.

Да, и еще один важный момент. Недавно было несколько инцидентов с «прилётом» в министерские башни Москва-Сити: работа на несколько дней парализована, сотрудников отправили на «удаленку».

Какие выводы из этого надо сделать? С учетом того, что я уже говорил про новую стратегию кибербезопасности США? А такие, что теперь организации КИИ и органов госуправления стали целями и мишенями не только для кибервмешательства, но и для точечного физического нападения с целью уничтожения их инфраструктуры и блокирования работы.

А это означает, что у таких организаций на подобный случай (не дай Бог!) должен быть предусмотрен план Б, не допускающий простоя и причинения тем самым неприемлемого ущерба, что вполне реализуемо с применением USB-токена типа Aladdin LiveOffice.

Кстати, другая вполне реальная ситуация: ноутбук вынесен за периметр, потеряли, украли, отдали в ремонт, и данные утекли. Как этому воспрепятствовать?

Шифровать.

Правильно! Но чем? На конференциях у меня с аудиторией часто происходит следующий диалог: Кто шифрует данные? 60–70 % руки подняли. А чем? Как чем, BitLocker'ом, то есть продуктом Microsoft! Что проще: где-то за океаном «убили» ключ, и все данные «накрылись»! Это, по сути, лучший вирус-шифровальщик! Вся служебная информация, выносимая за пределы организации, должна быть зашифрована, но, опять же, средством, которое не получится отключить в месте вне вашей досягаемости. Как пример, упомяну наш продукт для защиты критически важных данных от утечек Secret Disk.

В начале нашего разговора вы упоминали про рост утечек критически важной информации и персональных данных. Вы же давно занимаетесь защитой данных от подобных утечек?

Да, в начале нашего разговора я говорил, что многие аналитики и российские вендоры фиксируют большой рост утечек. Но вместо того, чтобы фокусироваться на защите са-

мих данных, нам опять навязываются какие-то странные решения по мониторингу хакерской активности, отслеживанию действий нарушителей внутри взломанного периметра сети, применение искусственного интеллекта для выявления поведенческих аномалий и пр.

Что, все смирились с неизбежностью таких утечек?

Это не так! Мы отработали эффективную технологию импортозамещения встроенных в иностранные СУБД средств защиты, позволяющую изолировать критически важные данные от самой СУБД и решить проблему со старыми унаследованными приложениями, которых у организации могут быть сотни, и вот так быстро и просто их не перепишешь, не перенесешь на отечественный Postgres Pro. А проблемы с миграцией заключаются именно в этом, а не в самих СУБД.

Возвращаясь к основной теме беседы – чем заменить MS CA… Если проблема настолько глобальна, как же удовлетворить всех?

Действительно, вижу, что после моих выступлений многие начинают осознавать проблему: подходят, задают вопросы. Мы, собственно, этого и добиваемся: обратить на нее внимание, хотим, чтобы нас услышали и начали реагировать.

В целом же рынок, конечно, бесконечен. Интерес к PKI Enterprise-уровня высок и в других странах.

Возможно, появятся и другие игроки с конкурирующими продуктами?

Конечно, мы не одни на рынке, но конкуренция его только расширяет: чем больше разработчиков будет инвестировать в исследования в том или ином сегменте, тем быстрее этот сегмент начнет развиваться. Но, надо понимать, здесь нужны очень глубокие компетенции в области безопасности, потому что PKI – это, в первую очередь, безопасность.

Что бы вы хотели сказать нашим читателям в заключение?

Только то, что говорю обычно: мы с вами живем в интересное время, сейчас нам дали уникальную возможность перезагрузиться, другими глазами посмотреть на то, что нам вещали западные провидцы, что нам так настойчиво насаждали.

Не затыкать дыры, заменяя одни продукты ушедших из России вендоров другими, часто наспех собранными из OpenSource, а начать с проектирования правильной и безопасной ИТ-инфраструктуры.

Например, на банковском рынке удалось это сделать: Россия совершила «квантовый скачок», перепрыгнув через целую эпоху платежных карт с магнитной полосой сразу на смарт-карты, и стала одним из лидеров в этой области.

Так что у нас есть исторический шанс! Давайте, постараемся сделать все правильно, безопасно… и немного «на вырост»! ■

НОВОСТИ

Кто разгадает криптотайну Солинаса?

Филиппо Вальсорда, американский специалист в области криптографии, недавно объявил вознаграждение для человека, который первым взломает семена (сиды) эллиптических кривых NIST и обнаружит оригинальные фразы, которые были использованы для их генерации. Вальсорда собрал необходимую для вознаграждения сумму при поддержке известных лиц в области криптографии и кибербезопасности.

В криптографии на эллиптических кривых (ECC) семена (сиды) – это значения, используемые в качестве первоначального ввода для генерации криптографических ключей. ECC полагается на математическую концепцию эллиптических кривых, определенных по конечным полям, для генерации относительно коротких, но безопасных ключей. Использование кривых гарантирует, что для выбранной на них точки невозможно вычислительно определить скалярное значение, применяемое для их генерации, обеспечивая необходимую основу для шифрования.

Эллиптические кривые NIST (P-192, P-224, P-256, P-384 и P-521), введенные в эксплуатацию в 2000 году и имеющие решающее значение для современной криптографии, были созданы в 1997 году с использованием сидов, предоставленных АНБ. Точное их происхождение остается неизвестным, но существуют исследования, предполагающие, что они являются хэшами определенных предложений на английском языке. Доктор Джерри Солинас, который, по слухам, выбирал их лично, скончался в начале 2023 года, оставив после себя нераскрытую криптографическую тайну.

Опасения в криптографическом сообществе начались много лет назад после скандала с алгоритмом Dual_EC_DRBG. Как утверждали эксперты, АНБ внедрило туда бэкдор.

Помимо исторической значимости, вызов с вознаграждением за взлом эллиптических кривых NIST имеет и практическое значение: решение задачи развеяло бы опасения об их безопасности. Вальсорда считает, что обладая достаточной вычислительной мощностью и опытом можно взломать предполагаемые хэши SHA-1 и восстановить оригинальные фразы.

Первый, кто представит хотя бы одно предложение-прообраз, получит ровно половину награды (6144 долл.), а оставшаяся часть перейдет к первому человеку, который представит все пять. Если же это сделает один и тот же человек, он получит всю сумму награды – 12 288 долл.