Инфраструктура доверия

Ключевые компоненты для построения безопасной доверенной ИТ-инфраструктуры

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

РАНХиГС, 2024 г.

Изменение и переоценка киберугроз после начала СВО

- С чем столкнулись после 2022 г?
  - Беспрецедентный рост успешных атак
    - Одна из причин (1) - неправильно спроектированная и реализованная **аутентификации** пользователей, использование паролей (ПРОСТАЯ аутентификация вместо 2ФА или СТРОГОЙ)
    - Вторая причина (2) - **удалённый доступ** - использование небезопасного "самопала"
    - ✓ **После инцидента - начинается устранение последствий, а не причин**
  - Массовые утечки баз данных и персональных данных
    - Причины - вместо **обезличивания** ПДн и **защиты** самих критически важных данных - **главных информационных активов**, усиливают защиту периметра, средства мониторинга и аналитики
  - Переоценка рисков и угроз (политических, архитектурных), от которых зависит работоспособность всех наших ИТ-инфраструктур
    - Главный приоритет - **выявление и устранение точек отказа**
    - Вместо этого часто движемся по инерции - боремся с навязанными нам угрозами ("плохие парни" - хакеры, вирусы-шифровальщики…)
    - ✓ **Необходимо сфокусироваться на главном, на всё не хватит ни сил, ни средств**
- Мир изменился, мы перестали доверять Западу и их технологиям
  - Нам необходимо самим создавать свою безопасную **доверенную** ИТ-инфраструктуру
    - Сначала на базе того, что уже есть - и этому **надо как-то доверять**
    - Потом - на базе своего, **доверенного** - ПО, "железа", микроэлектроники…
    - ✓ **Ключевое слово во всём этом - доверие**

Что такое **доверие** и зачем оно нам?

Постоянно слышим про доверие

Начинаем сами про него твердить

Большинство не понимает ЧТО ЭТО, КАК обеспечивается, и ЗАЧЕМ оно нам?

Из-за этого часто происходит **подмена понятий и целей**, и мы начинаем делать не то, что нужно

Что такое ДОВЕРИЕ

- Доверие
  - Между людьми
    - Это уверенность в порядочности и ответственности другого, что он не воспользуется полученной от нас информацией нам во вред
  - В ИТ-инфраструктуре
  - Это уверенность в том, что
    - Каждый элемент (объект) ИТ-инфраструктуры работает так, как мы ожидаем
    - Этот элемент не подменили
    - Мы можем доверять получаемой от него информации и обмениваться с ним важной для нас информацией
    - Доступ в ИС получили только легальные пользователи (субъекты)
  - Доверие обеспечивается идентификацией и аутентификацией каждого элемента инфраструктуры
    - Объектов (оборудования, ПО)
    - Субъектов (пользователей)

Уровни доверия в ИС

Уровни доверия в ИС

- **Значения**
  - Низкий
  - Средний
  - Высокий (на уровне гарантий)
- **Определяются**
  - По уровню **значимости** обрабатываемой информации
  - По риску возникновения **недопустимого события** ИБ и размеру возможного **ущерба** в случае инцидента ИБ (несанкционированного доступа, утечки, искажения, уничтожения, блокирования доступа к информации)
- **Зависят**
  - От правильности реализации системы идентификации и аутентификации
    - Достаточно много инцидентов (взломов ИС, утечек персональных данных и др.) происходит именно из-за неправильно реализованной (слабой) системы аутентификации пользователей, отсутствия или некорректной реализации механизмов аутентификации оборудования и используемого ПО (объектов) ИТ-инфраструктуры
- **Правила определения уровней доверия к идентификации и аутентификации, к всей ИС**
  - Система считается доверенной, когда каждый её элемент является доверенным
  - Уровень доверия напрямую влияет на уровень безопасности в ИС
  - Уровень доверия к системе определяется по её самому слабому звену - по самому низкому уровню доверия элементов, составляющих ИС

Уровень доверия

- это совокупность действий, которые должны быть выполнены для достижения необходимой уверенности

(не определяется численными показателями / ГОСТ)

Требования доверия в ИС

Риск недопустимого события ИБ,
размер возможного ущерба

Уровень значимости информации в ИС

Уровни доверия в ИС	Низкий	**Средний**	**Высокий**
Высокий	Средний	**Высокий**	**Высокий**
Средний	Низкий	Средний	**Высокий**
Низкий	Низкий	Низкий	Средний

- Гос. организации
- Федеральные структуры
- Организации КИИ
- Крупный и ср. бизнес
- Операторы ИСПДн (оборотные штрафы)

Здесь важнее не доверие, а ГАРАНТИИ

Примеры недопустимых событий ИБ:

- Подмена транслируемого контента с целью дестабилизации социально-политической обстановки
- Полная или частичная потеря данных из государственных фондов, реестров и ведомственных баз данных
- Утечка персональный данных и выплата штрафа в размере 3% от оборота компании

Для достижения требуемого уровня доверия в ИС необходимо обеспечить **соответствующий** уровень доверия к результатам идентификации и аутентификации

Что такое ДОВЕРИЕ

- Доверие
  - Можно ли его как-то измерить и оцифровать?
- Понятие доверия на русском
  - Скудность языка или проблемы с переводом?
  - Понятие **снег**
    - В русском языке - 1 слово - СНЕГ
    - У эскимосов, чукчей - 500

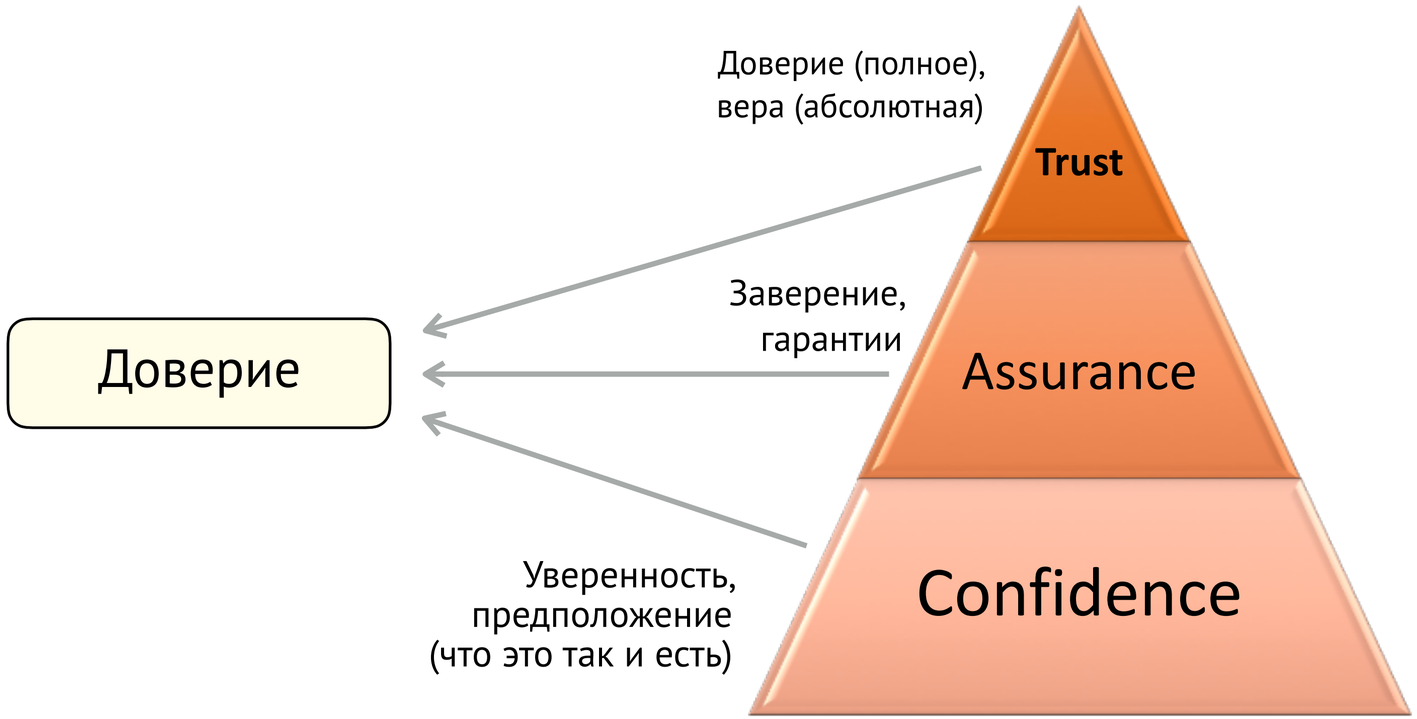
tlapa powder snow
tlacringit snow that is crusted on the surface
kayi drifting snow
tlapat still snow
klin remembered snow
naklin forgotten snow
tlamo snow that falls in large wet flakes
tlatim snow that falls in small flakes
tlaslo snow that falls slowly
tlapinti snow that falls quickly
kripya snow that has melted and refrozen
tliyel snow that has been marked by wolves
tliyelin snow that has been marked by Eskimos
blotla blowing snow
pactla snow that has been packed down
hiryla snow in beards
wa-ter melted snow
tlayinq snow mixed with mud
quinaya snow mixed with Husky shit
quinyaya snow mixed with the shit of a lead dog
slimtla snow that is crusted on top but soft underneath
kriplyana snow that looks blue in the early morning
puntla a mouthful of snow because you fibbed
allatla baked snow
fritla fried snow
gristla deep fried snow
MacTla snow burgers

atla snow between your fingers or toes, or in groin-folds
dinliltla little balls of snow that cling to Husky fur
sulitlana green snow
mentlana pink snow
tidtla snow used for cleaning
ertla snow used by Eskimo teenagers for exquisite erotic rituals
kriyantli snow bricks
hahatla small packages of snow given as gag gifts
semtla partially melted snow
priyakli snow that looks like it's falling upward
chiup snow that makes halos
blontla snow that's shaken off in the mudroom
tlalman snow sold to German tourists
tlalam snow sold to American tourists
tlanip snow sold to Japanese tourists
protla snow packed around caribou meat
attla snow that as it falls seems to create nice pictures in the air
sotla snow sparkling with sunlight
tlun snow sparkling with moonlight
astrila snow sparkling with starlight
clim snow sparkling with flashlight or headlight
tlapi summer snow
krikaya snow mixed with breath

rinkyi first snow of the year
tronkyin last snow of the year
shiya snow at dawn
katiyana night snow
tlinro snow vapor
nyik snow with flakes of widely varying size
ragnitla two snowfalls at once, creating moire patterns
akitla snow falling on water
privtla snow melting in the spring rain
chahatlin snow that makes a sizzling sound as it falls on water
hootlin snow that makes a hissing sound as the individual flakes brush
geltla snow dollars
briktla good building snow
striktla snow that's no good for building
erolinyat snow drifts containing the imprint of crazy lovers
chachat swirling snow that drives you nuts
krotla snow that blinds you
tlarin snow that can be sculpted into the delicate corsages Eskimo girls pin to their whale parkas at prom time
motla snow in the mouth
sotla snow in the south
maxtla snow that hides the whole village
tlayopi snow drifts you fall into and die
truyi avalanche of snow
tlapripta snow that burns your scalp and eyelids
carpitla snow glazed with ice
tla ordinary snow
intla snow that has drifted indoors
shlim slush
warintla snow used to make Eskimo daiquiris
mextla snow used to make Eskimo Margaritas
penstla the idea of snow
mortla snow mounded on dead bodies
ylaipi tomorrow's snow
nylaipin the snows of yesteryear ("neiges d'antan")
pritla our children's snow
nootlin snow that doesn't stick
rotlana quickly accumulating snow
skriniya snow that never reaches the ground
bluwid snow that's shaken down from objects in the wind
tlanid snow that's shaken down and then mixes with sky-falling snow
ever-tla a spirit made from mashed fermented snow, popular among Eskimo men
talini snow angels
tronkyin last snow of the year
shiya snow at dawn
katiyana night snow
tlinro snow vapor

tlapa powder snow
tlacringit snow that is crusted on the surface
kayi drifting snow
tlapat still snow
klin remembered snow
naklin forgotten snow
tlamo snow that falls in large wet flakes
tlatim snow that falls in small flakes
tlaslo snow that falls slowly
tlapinti snow that falls quickly
kripya snow that has melted and refrozen
tliyel snow that has been marked by wolves
tliyelin snow that has been marked by Eskimos
blotla blowing snow
pactla snow that has been packed down
hiryla snow in beards
wa-ter melted snow
tlayinq snow mixed with mud
quinaya snow mixed with Husky shit
quinyaya snow mixed with the shit of a lead dog
slimtla snow that is crusted on top but soft underneath
kriplyana snow that looks blue in the early morning
puntla a mouthful of snow because you fibbed
allatla baked snow
fritla fried snow
gristla deep fried snow
MacTla snow burgers
jatla snow between your fingers or toes, or in groin-folds
dinliltla little balls of snow that cling to Husky fur
sulitlana green snow
mentlana pink snow
tidtla snow used for cleaning
ertla snow used by Eskimo teenagers for exquisite erotic rituals
kriyantli snow bricks
hahatla small packages of snow given as gag gifts
semtla partially melted snow
ontla snow on objects
intla snow that has drifted indoors
shlim slush
warintla snow used to make Eskimo daiquiris
mextla snow used to make Eskimo Margaritas
penstla the idea of snow
mortla snow mounded on dead bodies
ylaipi tomorrow's snow
nylaipin the snows of yesteryear ("neiges d'antan")
pritla our children's snow
nootlin snow that doesn't stick
rotlana quickly accumulating snow

Что такое ДОВЕРИЕ (применительно к ИТ и ИС)



ISO/IEC 15408

Что такое ДОВЕРИЕ (применительно к ИТ и ИС)

Доверие

Доверие (полное), вера (абсолютная)

Заверение, гарантии

Уверенность, предположение (что это так и есть)

Иерархия общества и управления им

Заповедь #1 - вера в Господа

6-я чакра (исключительное доверие для избранных)

Всевидящее око

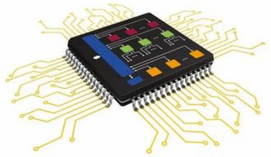
Господа

Рабы

Пирамида масонов:

организация общества на Земле и 10 заповедей

Что такое ДОВЕРИЕ (применительно к ИТ и ИС)



Доверенная электроника, собственный дизайн, производство, протоколы (**всё своё**)

доверие для действительно критических систем

Доверие (полное), вера (абсолютная)

Trust

Заверение, гарантии

Assurance

Больше доказательств и **гарантий**

Без правильной реализации первых двух уровней доверия использование доверенной электроники (ПК, процессоров, сборки, дизайна) ничего не даст

Доверие

Больше атрибутов и **свидетельств**

Что даёт гарантии?

Криптография (гарантированная или известная стойкость

PKI, безопасность хранения закрытого ключа

Уверенность, предположение (что это так и есть)

Confidence

Сейчас мы здесь

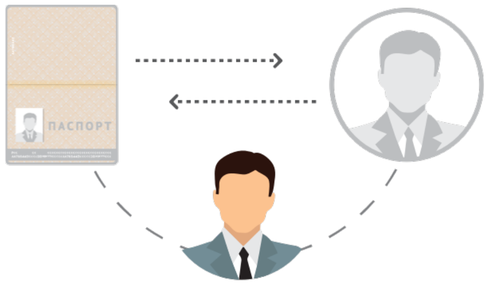
- уверены, предполагаем
- получаем свидетельства, заверения, гарантии

Основа доверия в ИС

- идентификация и аутентификация

Идентификация и аутентификация

Что такое идентификация



- Это ответ на вопрос - ты кто?
- Это способ или процесс определения личности пользователя (субъекта) или элемента ИС (объекта)

Что такое аутентификация

- Это **доказательство** того, что ты - это ты
- Это процедура "установление подлинности"

✓ **Идентификация и аутентификация неразрывно связаны между собой**

✓ **Доверие к результатам идентификации может достигаться с помощью механизмов аутентификации, поскольку одной из целей аутентификации является подтверждение идентификационной информации**

◆ Понятия, определения, требования

- Определены в национальных стандартах* РФ, основные из них:
  - ГОСТ Р 58833-2020 (Идентификация и аутентификация. Общие положения)
  - ГОСТ Р 70262.1-2022 (Идентификация и аутентификация. Уровни доверия идентификации)
  - ГОСТ Р 70262.2-2024** (Идентификация и аутентификация. Уровни доверия идентификации)

* - разработаны компанией "Аладдин"
** - проект стандарта, ожидается присвоение такого номера в 2024 г.

Нац. стандарты по идентификации и аутентификации

- Действующие стандарты
  - ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения
  - ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. **Уровни доверия идентификации**
  - ГОСТ Р 59381-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции
  - ГОСТ ISO/IEC 24760-2-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования.
  - ГОСТ Р 59382-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы
  - ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом
  - ГОСТ Р 59515-2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности
- Проекты стандартов
  - Защита информации. Идентификация и аутентификация. **Уровни доверия аутентификации**
  - Защита информации. Идентификация и аутентификация. Управления идентификацией и аутентификацией
  - Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости идентификации и аутентификации
  - Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией

Идентификация

Виды и цели идентификации

- Первичная идентификация
  - Проводится **один раз** в момент регистрации в ИС нового пользователя или объекта
    - Может обновляться периодически или по мере необходимости (по запросу)
  - По времени может быть достаточно длительной
  - Цель:
    - Удостовериться, что новый пользователь (или объект) является тем, за кого себя выдаёт (или чем является)
    - Присвоить уникальный (для ИС) идентификатор (ID, логин, учётная запись)
    - Зарегистрировать пользователя (или объект) в ИС и связать с ним его идентификатор
    - Хранить и поддерживать в актуальном состоянии идентификационную информацию
- Вторичная идентификация
  - Проводится **каждый раз** при новом запросе на доступ пользователя или объекта в ИС
  - По времени должна выполняться достаточно быстро
  - Цель:
    - Распознавание пользователя (или объекта) при его запросе на доступ к ресурсам ИС
    - Проверка предъявленного идентификатора по списку зарегистрированный в ИС

Уровни доверия идентификации в ИС

- Уровни доверия идентификации
  - Низкий (определённая уверенность)
  - Средний (достаточно высокая уверенность)
  - Высокий (очень высокая уверенность)

Уровни доверия к идентификации в 2017 г. ввёл NIST* (Аутентификация и управление жизненным циклом (руководство по цифровой идентичности)

- Требования к уровням доверия идентификации в различных ИС

Риск недопустимого события ИБ,
размер возможного ущерба

Уровень **значимости** информации в ИС

Уровень доверия идентификации	Низкая	**Средняя**	**Высокая**
Высокий	Средний	**Высокий**	**Высокий**
Средний	Низкий	Средний	**Высокий**
Низкий	Низкий	Низкий	Средний

- Гос. организации
- Федеральные структуры
- Организации КИИ
- Крупный и ср. бизнес
- **Операторы ИСПДн** (уголовная и административная ответственность, оборотные штрафы)

* - NIST Special Publication 800-63B, https://doi.org/10.6028/NIST.SP.800-63b

Аутентификация

- Аутентификация
  - Это процедура "установление подлинности" (объекта или субъекта ИС)
- Цели аутентификации в ИС
  - **Подтверждение идентификационной информации** (1)
  - **Установление доверительных отношений** (2) между всеми участниками обмена
    - Аутентификация источника данных (односторонняя аутентификация)
    - Аутентификация сторон (элементов ИТ-инфраструктуры - взаимная аутентификация)
  - **Предоставление доступа** (3) в ИС или в ИТ-инфраструктуру
  - **Подтверждение идентификационной информации** (4)
    - Для подтверждения личности владельца ЭП
    - Для проверки наличия полномочий на право подписи
    - Для фиксации неотказуемости при выполнении процедуры подписи эл. документа владельцем ЭП, факта доступа к ИС (или к её критическим ресурсам), факта выполнения определённых действий в ИС

Факторы аутентификации

- Фактор аутентификации
  - Вид (форма) аутентификационной информации, предъявляемой пользователем (субъектом) в процессе аутентификации
  - Существует всего 3 фактора:
    - **Фактор знания** - знание общего с ИС секрета (пароль, PIN-код, графический или одноразовый пароль)
    - **Фактор владения** - обладание определённым устройством/предметом, содержащим аутентификационную информацию
    - **Биометрический фактор** - свойственный конкретному человеку (субъекту) определённый признак ("контактная биометрия" - отпечатки пальцев, геометрия руки, шаблон поведения и пр.)

✓ **Типичные ошибки**

- Факторы аутентификации часто путают с дополнительными атрибутами идентификации (SMS-код, Push, QR-код и пр.)
- Использовать "бесконтактную биометрию" - лицо, голос в качестве фактора аутентификации в ИС не допускается (из-за современных возможностей генеративного искусственного интеллекта)

Факторы и виды аутентификации

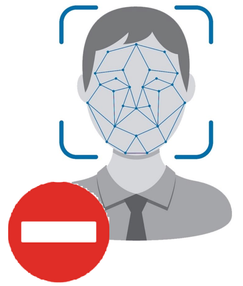
- Однофакторная
  - С помощью запоминаемого и вводимого вручную пароля (фактор знания общего секрета)
- Двухфакторная (2ФА или 2FA)
  - С помощью персонального аппаратного устройства (фактор владения) и ввода PIN-кода (фактор знания секрета чтобы воспользоваться своим аппаратным устройством)
  - С помощью персонального аппаратного устройства (фактор владения), ввода одноразового пароля (сгенерированного им на основе общего с ИС секрета) и запоминаемого статического пароля (фактор знания общего секрета)
  - Примеры
    - USB-токен, смарт-карта, содержащие пользовательский идентификатор (профиль) или сертификат, доступ к которым возможен только после ввода правильного PIN-кода
    - OTP-токен, U2F-токен, смартфон с установленным приложением для генерации одноразового пароля

Факторы и виды аутентификации

- Трёхфакторная (3ФА или 3FA)
  - С помощью персонального аппаратного устройства (фактор владения), встроенной биометрической подсистемы (биометрический фактор) и ввода PIN-кода (фактор знания общего секрета)

✓ **Важно:**

- Биометрические данные, в целях безопасности и повышения доверия пользователей, должны храниться и обрабатываться внутри персонального аппаратного устройства (в распределённой базе данных) без передачи их в ИС по каким-либо каналам связи и без хранения и обработки в единой централизованной базе данных
- Использование бесконтактной биометрии, применяемой в ЕБС (лицо, голос), в качестве биометрического фактора аутентификации в ИС не допускается (из-за современных возможностей ИИ)
- Использование алгоритмов распознавания отпечатков пальцев на базе обучаемых нейросетей настоятельно не рекомендуется (На каком множестве данных, кто и как обучал нейросеть? Как будет вести себя алгоритм на других данных, с другим качеством, в другой среде? Как доказать надёжность и стабильность работы алгоритма?)
- Биометрия, в силу вероятностной природы, должна использоваться как дополнительное **доказательство принадлежности данного устройства его владельцу** и **неотказуемости** от факта проведения транзакции (доступа в ИС, подписания документа или финансовой транзакции своей ЭП)

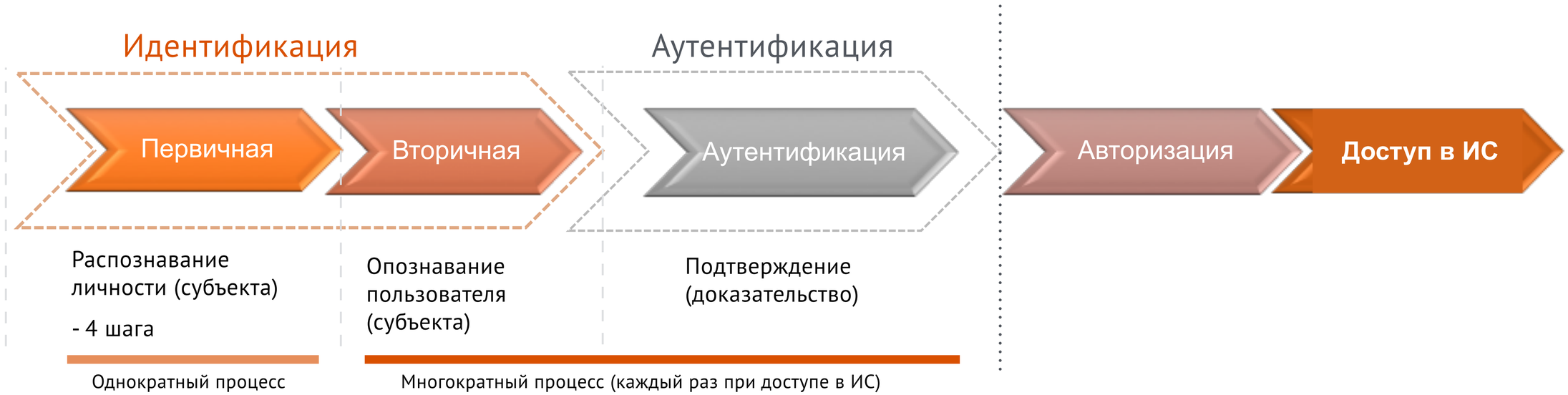


Процесс аутентификации

- Производится
  - После вторичной идентификации
- Выполняется
  - **Аутентификация** (1)
    - При каждой попытке доступа в ИС
    - По времени должна выполняться достаточно быстро (1-2 с) - обмен данными, валидация, принятие решения о предоставлении доступа

Организация процесса доступа в ИС

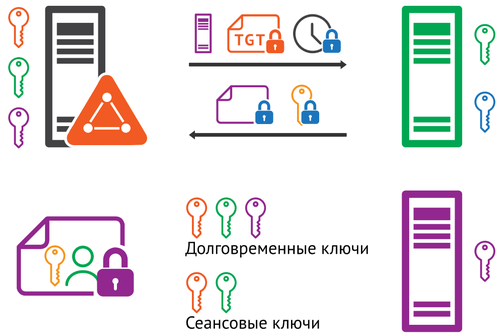
- Доступ в ИС
  - Производится в 4 этапа
    - Идентификация
    - Аутентификация
    - Авторизация
    - Предоставление доступа



Типы аутентификации в ИС

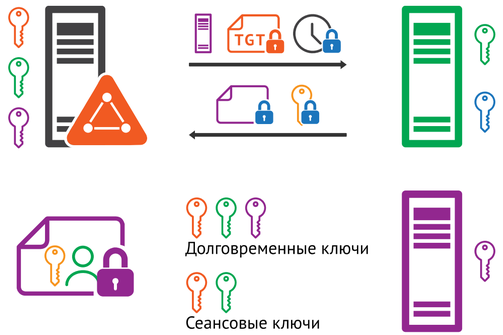
Для каждого типа ИС - свой тип аутентификации

- Локальная
  - Службы аутентификации и валидации (принимающая решение о предоставлении доступа) находятся на каждом локальном устройстве (ПК, смартфон и пр.)
- Прямая
  - Владелец ресурса доверяет одному валидатору, расположенному внутри защищённого периметра
  - Все пользователя локальной сети проходят процесс аутентификации и валидации напрямую
    - Применяется в небольших организациях численностью до 20-30 рабочих мест
- Доменная
  - Владельцы многих ресурсов в локальной сети доверяют одному валидатору, расположенному внутри защищённого периметра локальной сети
    - Применяется в сегментах малого и среднего бизнеса
- Иерархическая
  - Отличается от доменной наличием подчинённых доменов, доступ пользователям могут предоставляться ими, однако в центре имеется база данных учётных записей всех пользователей и право управления доступом
    - Применяется в организациях с филиальной сетью



Типы аутентификации в ИС

- Распределённая сетевая
  - Отличается от доменной наличием множества доменов, связанных между собой трастовыми (доверенными) отношениями
  - В каждом домене независимо производится процесс аутентификации и принимается решение о доступе
    - Применяется в крупных корпорациях и холдингах
- Мостовая
  - Отличается от распределённой сетевой наличием доверенной третьей стороны (ДТС)
    - Применяется для межведомственного взаимодействия с развитым электронным документооборотом (ЭДО)
- Браузерная
  - Отличается от мостовой механизмом аутентификации, основанном на организации защищённого канала связи клиент-сервер на сессионном уровне
  - ДТС может находится на том сервере
    - Применяется для порталов госуслуг
- Браузерная с трансляцией доверия
  - Отличается от браузерной транслированном доверия к аутентификации, которую пользователь успешно прошёл в первичной ИС, в другие публичные/облачные ИС
  - Решается с применением федеративной системы трансляции доверия
    - Применяется для ведомственных, региональных порталов (ФНС, mos.ru и др.) с трансляцией доверия, например, от портала gosuslugi.ru



Требования к аутентификации в различных ИС

- Требуемые виды аутентификации в ИС

Вид аутентификации в ИС должен определяться

- по уровню **значимости** информации
- по риску возникновения недопустимого события ИБ и размеру возможного **ущерба** в случае взлома и утечки
  - Достаточно большой процент взломов и утечек происходит из-за неправильно выбранной и реализованной системы идентификации и аутентификации, поэтому крайне важно устранять причину, а не последствия - построить правильную систему идентификации и аутентификации

Риск недопустимого события ИБ,
размер возможного ущерба

Уровень **значимости** информации в ИС

Вид аутентификации	Низкая	**Средняя**	**Высокая**
Высокий	Усиленная	**Строгая**	**Строгая**
Средний	Простая	Усиленная	**Строгая**
Низкий	Простая	Простая	Усиленная

- Гос. организации
- Федеральные структуры
- Организации КИИ
- Крупный и ср. бизнес
- **Операторы ИСПДн** (уголовная и административная ответственность, оборотные штрафы)

Для кого:
- Для всех пользователей и администраторов ИС
- Для удалённых пользователей

Требования
к видам аутентификации пользователей ИС

Простая аутентификация

Простая аутентификация

Уровень доверия - низкий

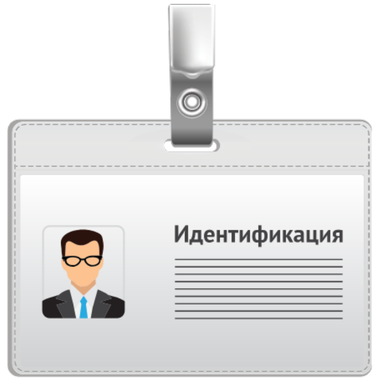
Низкий уровень доверия

AAL-1 (NIST)

- Может применяться
  - В ИС с низким уровнем значимости информации и несущественным размером возможного ущерба

Требования к идентификации

- Уровень доверия идентификации - низкий
  - Определяется уровнем доверия первичной идентификации
  - Зависит от результатов (успеха) вторичной идентификации и конкретной среды функционирования (должен устанавливаться на основе анализа рисков ИБ)
- Первичная идентификация
  - Может не проводиться (для доступа в ИС без регистрации как анонимный пользователь)
  - Может проводится **удалённо, без личной явки** пользователя на регистрацию или без предъявления объекта (оборудования), или лично
  - Регистрация идентификационных данных производится без проверки (верификации), такими, какими их заявили
- Вторичная идентификация
  - Может проводиться с использованием общеизвестного идентификатора ("Аноним")
  - Производится в один этап с предъявлением идентификатора, уникального для данной ИС, без дополнительной проверки
    - Предполагается (с определённой уверенностью), что предъявленный идентификатор каким-то образом связан с пользователем



Простая аутентификация

Требования к аутентификации

- Простая
  - **Однофакторная**
    - Пароль - запоминаемый и вводимый вручную (фактор знания общего с ИС секрета)
    - Одноразовый код доступа, присылаемый из ИС на устройство пользователя
    - Электронный идентификатор, не требующий ввода PIN-кода (фактор владения)

✓ **Использование биометрии в качестве единственного фактора не допускается** (например, отпечаток пальца, снятый сканером, встроенным в компьютер пользователя)

  - **Односторонняя**
    - Передача аутентификационной информации осуществляется в одном направлении - от субъекта (пользователя) к объекту доступа (ИС)

✓ **Опасность:** пользователь не может быть уверен, что аутентифицируется и получает доступ именно в ту ИС, в которую надо, что её не подменили

Усиленная аутентификация

Усиленная аутентификация

Средний уровень доверия

AAL-2 (NIST)

Уровень доверия - средний

- Может применяться
  - В ИС со средним уровнем значимости информации и существенным размером возможного ущерба

Требования к идентификации

- Уровень доверия идентификации - средний
  - Предполагается (с умеренной уверенностью), что предъявленный идентификатор действительно принадлежит данному пользователю
  - Определяется уровнем доверия первичной идентификации
  - Зависит от результатов (успеха) вторичной идентификации и конкретной среды функционирования
    - Должен устанавливаться на основе анализа рисков ИБ и соответствовать требованиям и регламентам нормативных документов организации

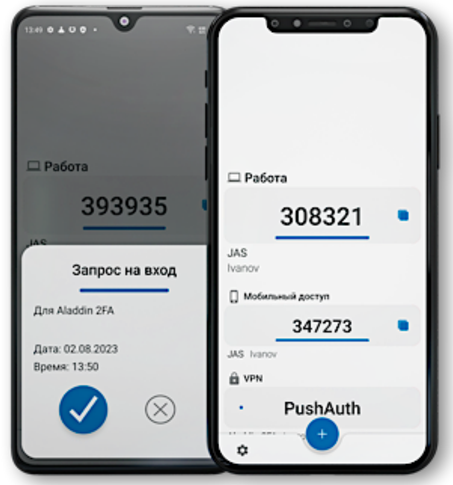
Дополнительные атрибуты / факторы

Двухэтапная проверка

Средний уровень доверия

- Код доступа
  - **Подтверждения личности пользователя с использованием фактора ЗНАНИЯ** (общего секрета)
  - Однократно используемый секрет, присылаемый ИС, на связанный с пользователем номер его мобильного телефона (Push-, SMS)
  - Одноразовый пароль, сгенерированный в приложении, установленном на связанном с пользователем мобильном телефоне, с загрузкой общего с ИС секретного ключа
    - Секретный ключ может быть загружен в приложение при инициализации, при сканировании QR-кода или другим способом
  - Примеры:
    - **Aladdin 2FA** (решена проблема безопасной передачи секрета на устройство пользователя)
    - Яндекс Ключ
    - Google Authenticator (не рекомендуется, противоречит российскому законодательству)
  - Опасность:
    - Мобильный телефон, независимо от установленной ОС, является недоверенным и небезопасным
    - Перехват кодов доступа, извлечение из телефона секретного ключа для генерации OTP способно дискредитировать всю ИС, дать злоумышленникам доступ в неё под видом легальных пользователей
    - Первичная идентификация может быть выполнена без личной явки пользователя к администратору (**удобство в ущерб безопасности**)

Содержит секрет



Второй фактор аутентификации

- Электронные идентификаторы

Средний уровень доверия

  - **Подтверждения личности пользователя с использованием фактора ВЛАДЕНИЯ** (персонального аппаратного устройства, содержащего уникальный идентификатор)

  - **iButton** (Dallas Touch Memory), имеющий уникальный серийный номер (идентификатор) и защищённую энергонезависимую память (опция) для хранения идентификатора пользователя
  - Опасность:
    - Относительная простота устройств и интерфейса позволяет их клонировать
    - Ряд китайских компаний наладили выпуск клонов iButton и универсальных программаторов для них

  - **OTP-токен**, в который загружен **общий секретный ключ** (известный ИС), с помощью которого генерируется одноразовый пароль, синхронизируемый с ИС
    - Один OTP-токен позволяет подключаться только к одной ИС
    - Для работы с OTP-токенами на стороне ИС **требуется сервер аутентификации**
    - Пример: JAS (JaCarta Authentication Server)
  - Опасность:
    - Взлом одного OTP-токена и извлечение из него секретного ключа способно дискредитировать всю ИС и дать злоумышленникам доступ в неё под видом легальных пользователей (инцидент со взломом RSA SecurID)

Второй фактор аутентификации

Средний уровень доверия

- Электронные идентификаторы
  - **U2F-токены**, поддерживающие стандарт FIDO/FIDO-2
    - Предназначены для отказа вводимых вручную запоминаемых паролей
    - В основном используются ВНЕШНИМИ пользователями различных сервисов (чаще с Web-интерфейсом)
    - В отличие от OTP-токенов, один U2F-токен может использоваться для доступа к множеству различных Web-ресурсов
    - Для каждого нового сервиса генерируется свой идентификатор
  - Примеры:
    - JaCarta U2F
    - ePass U2F FIDO2 A4B
  - Ограничение и опасность:
    - Не для корпоративных ИС (закрытого типа)
    - Предполагается САМОСТОЯТЕЛЬНУЮ регистрация пользователей эл. сервиса, без участия администраторов (первичная идентификация без явки к администратору)
    - Подходит только для ИС открытого типа, ИС с браузерной аутентификацией и ограниченного набора сценариев использования

✓ **Удобство в ущерб безопасности (в корпоративных ИС)**

Второй фактор аутентификации

- Электронные идентификаторы

Средний уровень доверия

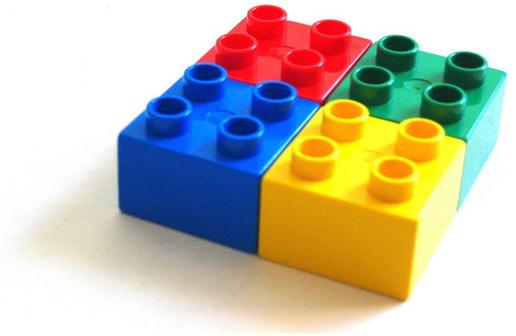
  - **USB-токен** или **смарт-карта**, в защищённую память которых загружен **файл-контейнер** или **сертификат**, содержащий пользовательский идентификатор
    - Токен или смарт-карта используется как электронный идентификатор ("флешка" с ПИН-кодом)
    - Для работы в ИС требуется предустановленный криптосервиспровайдер (CSP) или библиотека PKCS#11, реализующие криптографические вычисления с использованием зарубежных или российских алгоритмов (программное СКЗИ)
  - Примеры:
    - JaCarta LT
    - Рутокен Lite
  - Опасность:
    - Часто желание сэкономить на средствах идентификации или желание сделать систему идентификации и аутентификации круче, с использованием российской криптографии, приводит к архитектурным ошибкам и **снижению надёжности** (доверия)
    - Контейнер с закрытым ключом программного CSP (СКЗИ) хранится в памяти USB-токена в виде файла - криптоконтейнера, который при работе копируется в память компьютера, закрытый ключ может быть извлечён из него или из памяти компьютера и склонирован, злоумышленники смогу получить доступ в ИС под видом легальных пользователей

JaCarta LT

✓ **Экономия в ущерб безопасности**

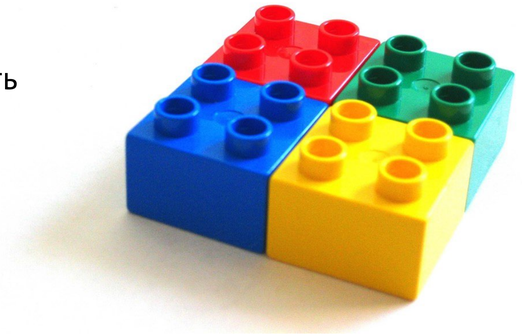
Необходимые компоненты в ИТ-инфраструктуре

- Сервер аутентификации (1)
  - Должен обеспечивать усиленную аутентификацию пользователей
    - По одноразовым паролям с использованием технологий Push, OTP, SMS (дополнительные атрибуты для двухэтапной идентификации)
    - С использованием аппаратных идентификаторов (второго фактора - OTP, U2F-токенов и др.)
    - С использованием мобильных технологий, передачей ключа (кода доступа) с помощью QR-кода и т.п.
  - Примеры:
    - RADUIS-сервер
    - JAS (высокопроизводительный сервер аутентификации Enterprise-класса)
  - Безопасность:
    - База данных с идентификационной и аутентификационной информацией, ключами и профилями пользователей должна быть надёжно защищена (обеспечена конфиденциальность, целостность, неизменность и неотказуемость)
    - Пример:
    - Крипто БД (для защиты баз данных)
    - Secret Disk (для защиты данных на дисках)
- Электронные идентификаторы - аппаратные средства 2ФА (2)
  - Должны иметь
    - Защищённую энергонезависимую память с доступом к сохраняемому в ней идентификатору пользователя по PIN-коду
    - Защиту от взлома, клонирования и подделки
    - Уникальный неизменяемый машиночитаемый и нанесённый на корпус устройства серийный номер



Необходимые компоненты в ИТ-инфраструктуре

- **Система централизованного управления жизненным циклом средств 2ФА (3)**
  - Должна обеспечивать
    - Персонализацию
    - Учёт выдаваемых средств 2ФА
    - Связь с пользователями (кому что выдано)
    - Возможность блокирования средств 2ФА и профилей пользователей
    - Автоматизацию рутинных операций и др.
  - Безопасность:
    - База данных с идентификационной и аутентификационной информацией, ключами и профилями пользователей должна быть надёжно защищена (обеспечена конфиденциальность, целостность, неизменность и неотказуемость)
  - Примеры:
    - Aladdin JMS, KeyBox*
- **Клиентское ПО (4)**
  - Должно обеспечивать возможность полноценной работы со средствами 2ФА
    - На клиентских платформах - ПК и ноутбуках (Linux, Windows, Mac)
    - На мобильных устройствах (Аврора, Android, iOS)
    - Из современных браузеров (для портальных решений)
  - Примеры:
    - SecurLogon (модуль аутентификации для настольных ПК на базе Linux, Windows, Mac)
    - Яндекс.Ключ, Google Authenticator, Aladdin 2FA (приложения для мобильных платформ)
    - Aladdin JC WebClient



* - требования по безопасности хранилища (базы данных) не выполняются

Строгая аутентификация

Строгая аутентификация

- Уровень доверия - высокий

Высокий уровень доверия

  - Предполагается (с очень высокой уверенностью), что предъявленный идентификатор **однозначно связан** с конкретным пользователем (или объектом) и контролируется им
  - **Связанность** предъявленного идентификатора с конкретным пользователем - физическим лицом (или объектом) должна проверяться с помощью дополнительных характеристик
    - **Знание** (общий с ИС секрет)
    - **Владение** (уникальный аппаратный идентификатор)
    - **Биометрические особенности** (уникальные неотъемлемые биометрические характеристики пользователя)
  - Первичная идентификация
    - Должна производиться **только при личной явке с подтверждением личности** пользователя во время регистрации или с предъявлением объекта (оборудования) ИТ-инфраструктуры
    - Должны быть сформированы и выданы дополнительные атрибуты и факторы аутентификации пользователя (аппаратный токен, цифровой сертификат, для биометрии - зарегистрированы отпечатки пальцев пользователя на его персональном устройстве, для обеспечения неотказуемости от факта регистрации - под запись на камеру)
  - Вторичная идентификация
    - Должна проводиться с подтверждением связи пользователя с предъявленным идентификатором с использованием **не менее двух дополнительных атрибутов** идентификации и обязательной их верификацией

✓ **Для целей идентификации пользователей не должно собираться информации больше, чем это минимально необходимо и достаточно**

Дополнительные факторы аутентификации

Высокий уровень доверия

- Персональное электронное устройство* - фактор владения (1)
  - USB-токен или смарт-карта с аппаратной реализацией криптографии и неизвлекаемым закрытым ключом, в защищённую память которых загружен пользовательский сертификат (для PKI)
  - Пример:
    - USB-токены и смарт-карты JaCarta-2 PKI
  - Опасность:
    - Пользователи могут передавать свои токены другим вместе с ПИН-кодами

Secure Element

JaCarta-2 PKI

*- Термин электронный идентификатор в данном контексте не совсем уместен и корректен

Требования к средствам 2ФА

- Персональное электронное устройство - средство 2ФА
  - Должно иметь
    - Аппаратную реализацию криптографии с неизвлекаемым закрытым ключом
    - Энергонезависимую память, достаточную для хранения 2-3х пользовательских сертификатов X.509 (по 2-4 КБ каждый)
    - Защиту от взлома, клонирования и подделки
    - Уникальный неизменяемый машиночитаемый и нанесённый на корпус устройства серийный номер
    - Защищённую энергонезависимую память с доступом к сохраняемому в ней идентификатору пользователя по PIN-коду
    - Устанавливаемую политику для PIN-кодов, запрещающую
      - Использование PIN-кодов, устанавливаемых по-умолчанию (пользователь должен сменить такой PIN-код при первом использовании)
      - Установку ранее использованных PIN-кодов, простых и общеприменяемых PIN-кодов, коротких - менее 6 символов и т.д.
  - Сертификат пользователя
    - Присвоенный пользователю идентификатор должен храниться в цифровом сертификате X.509 в поле "Уникальный идентификатор субъекта"
    - Пользовательский сертификат должен быть выдан доверенным (желательно сертифицированным) корпоративным центром сертификации (не импортным недоверенным MS CA!)

Высокий уровень доверия

JaCarta-2 PKI

Требования к средствам 2ФА

- Клиентское ПО или ОС как среда исполнения должны поддерживать все функци PKI, необходимые для работы
- Используемая криптография должна иметь
  - **Известную стойкость** (для зарубежной криптографии) не менее $4*10^{33}$

    или
  - Гарантированную стойкость (для российских ГОСТов)
- Для пользовательских (персональных) устройств рекомендуется использовать
  - RSA с длиной ключа не менее 2048

    или
  - Более современный алгоритм ECDSA с длиной ключа 304 бита (стойкость $4*10^{45}$)

JaCarta-2 PKI

Тип аутентификации определяет тип ЭП в ИС

- Надёжность системы определяется по её самому слабому звену
  - Если в ИС необходимо обеспечить **юридически значимую ЭП**, приравненную к собственноручной, то для получения усиленной квалифицированной ЭП (УКЭП) должна быть обеспечена **СТРОГАЯ** аутентификация пользователей

Необходима аппаратная реализация - токен

Защищенный Secure Element с аппаратной реализацией криптографии

Сейчас УКЭП - это не ЭП, это электронная "печать"
Чтобы ЭП стала действительно персональной, требуется привязка средства ЭП к биометрическим данным пользователя и невозможность отчуждения

Дополнительные факторы аутентификации

- **Биометрическая идентификация пользователя**
  - Подтверждения личности пользователя с использованием биометрических характеристик
    - Подтверждается факт владения пользователем своим персональным устройством (токеном, смарт-картой с поддержкой PKI)
    - Может использоваться как **третий фактор** (вместе с вводом PIN-кода) или как **второй фактор** (вместо ввода PIN-кода)
  - ✓ **Это лучший способ привязки идентификатора к личности пользователя**
  - Тип биометрической идентификации
    - **Контактный - по отпечаткам пальцев** (предпочтительно - более надёжный)
    - **Бесконтактный** - по распознаванию лица или голоса (не рекомендуется из-за бесконтактного способа, высокой стоимости, законодательных ограничений - только через ЕБС)
  - Примеры:
    - USB-токен Aladdin SecurBIO
  - Опасность:
    - Биометрическая идентификация - всегда вероятностный процесс, однозначного ответа "свой-чужой" получить нельзя, только с некой вероятностью (ошибками первого и второго рода)
    - Использование алгоритмов на базе обучаемых нейросетей (ИИ) настоятельно не рекомендуется из-за невозможности доказательства надёжности, повторяемости, настроек, механизмов обучения и принятия решения "свой-чужой"

Высокий уровень доверия

Aladdin SecurBIO-токен

Требования к средствам 2ФА/3ФА с биометрией

- Идентификация по отпечаткам пальцев
  - Должно использоваться персональное защищённое устройство со встроенным в него полупроводниковым сканером (не оптическим!)
  - Все вычисления должны выполняться не на сервере, а **локально** - внутри устройства (первичная регистрация и шаблонизация отпечатков пальцев, сравнение предъявляемого отпечатка пальца с шаблоном, вердикт - "свой-чужой") - технология Match-On-Device
  - Сравнение необходимо производить по типу "1:1", допустимо до "1:10 - 1:100", но с увеличением требований к надёжности
  - Рекомендуемая **надёжность** (значение FAR - "не пустить чужого") - от 10^{-4} до 10^{-6}, оптимально 10^{-5}
  - Вердикт "свой-чужой" не должен передаваться в ИС в виде фиксированного значения, а должен использовать внутри устройства для передачи управления к подсистеме аутентификации
  - Реализованный алгоритм вычисления должен обеспечивать **повторяемость** результата и заданную надёжность на уровне реализации алгоритма (для ошибок первого и второго рода - FAR и FRR)
  - **Использование алгоритмов на базе обучаемых нейросетей настоятельно не рекомендуется**

Высокий уровень доверия

Aladdin SecurBIO-токен

Ключевые компоненты,

обеспечивающие высокий уровень доверия ИТ-инфраструктуры и ИС

Компоненты для обеспечения высокого уровня доверия ИТ и ИС

Корпоративный центр выпуска и обслуживания сертификатов (CA)

- основа обеспечения доверия всех элементов ИТ-инфраструктуры и строгой аутентификации пользователей

Защищённое хранилище сертификатов

(Secure Element, Secure Island, TrustZone - для уровня Trust)

для надёжной аутентификации устройств (серверов, ПК, сетевого оборудования, IIoT, M2M)

USB-токены, смарт-карты

для строгой аутентификации пользователей

Клиент PKI и 2ФА для Linux

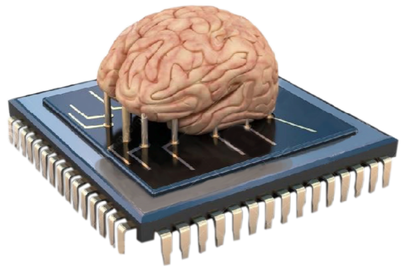
для строгой 2ФА пользователей (аналог MS Smartcard logon)

Корпоративная система централизованного управления токенами, сертификатами

- обязательный компонент для крупной ИТ-инфраструктуры

Компоненты для обеспечения высокого уровня доверия ИС

- Идентификация
  - Правильные процедуры, требования и регламенты
    - С обязательной личной явкой, проверкой предоставленных документов
- Аутентификация (строгая)
  - (1) **Персональный USB-токен или смарт-карта** - второй фактор аутентификации пользователей
    - С ПИН-кодом, установленным самим пользователем (фактор знания)
    - С аппаратной реализацией криптографии с известной стойкостью
    - С неизвлекаемым закрытым ключом
    - С цифровым сертификатом X.509
    - [С биометрическим сканером отпечатков пальцев для идентификации пользователя - владельца аппаратного устройства - второй фактор или третий (с PIN-кодом)] - опция
  - (2) **Secure Element** (**не TPM!**) для доверенного оборудования в критически важных системах (уровень Trust)
    - Для безопасного взаимодействия, дистанционного управления, обновления ПО
    - Для хранения машинного сертификата X.509
    - С аппаратной реализацией криптографии
    - С неизвлекаемым закрытым ключом
  - (3) **Оборудование без Secure Element** (уровень Assurance)
    - С машинным сертификатом X.509, сохраняемым в памяти устройства
    - С поддержкой устройством протоколов IEEE 802.1x, SCEP и др.



Security Island - "островок безопасности на процессоре" позволить себе сегодня не можем, у нас нет таких технологий и возможностей производства

Компоненты для обеспечения высокого уровня доверия в ИС

- Инфраструктура
  - (4) **Корпоративный центр выпуска и обслуживания сертификатов** (CA)
    - **Машинные** (каждое устройство в ИТ-инфраструктуре должно быть идентифицировано и аутентифицировано)
    - **Программные** - разрешённое ПО должно быть подписано не только сертификатом разработчика, но и эксплуатирующей организацией
    - **Пользовательские** (выпущенные на их персональные USB-токены или смарт-карты)
    - С поддержкой работы в двух экосистемах - Linux и Windows

      ✓ **Это не должен быть Microsoft CA - ему больше нельзя доверять!**
  - (5) **Клиентское ПО** (под российские ОС на базе Linux и Windows для совместимости в период миграции)
    - С поддержкой средств 2ФА/3ФА (+BIO)
    - С поддержкой PKI
    - С возможностью одновременно работать и в Linux, и в Windows, с разными домен-контроллерами
    - С возможностью локальной, доменной, браузерной аутентификации (нужного для ИС типа)
  - (6) **Корпоративная система централизованного управления жизненным циклом**
    - Средств 2ФА/3ФА (с возможностью обновления сертификатов и "прошивок")
    - Сертификатов, профилей пользователей, политик безопасности, др. объектов PKI
    - СЗИ, СКЗИ и пр.

Ключевые компоненты

для построения безопасной доверенной ИТ-инфраструктуры
от компании Аладдин

Ключевые компоненты для построения доверенной ИТ-инфраструктуры

NEW

Корпоративный центр выпуска и обслуживания сертификатов

Aladdin Enterprise CA

- основа обеспечения доверия всех элементов ИТ-инфраструктуры

NEW

Клиент PKI и 2ФА для Linux

SecurLogon

- для строгой 2ФА пользователей
- аналог MS Smartcard logon

USB-токены, смарт-карты, Secure Element

JaCarta-2 PKI

- для строгой 2ФА пользователей и устройств (машин)

Корпоративная система централизованного управления токенами, сертификатами

JMS

- обязательный компонент для крупной ИТ-инфраструктуры

MS CA - единая точка отказа для всех наших ИТ-инфраструктур

MS CA - корпоративный центр выпуска и обслуживания сертификатов

- От него зависят
  - Доверенное взаимодействие всех объектов и компонентов ИТ-инфраструктуры
  - Аутентификация всех объектов системы - оборудования, приложений (ПО), пользователей
  - Работоспособность доменов безопасности/службы каталога
  - Работа различных сервисов (удалённого доступа, VDI, VPN, RDP-шлюзы и др.)
- Практически все ИТ-инфраструктуры в России построены на базе MS CA (CS)
  - …и на 100% зависят от его работоспособности
  - В 2022 г. Microsoft ушла из России, представительство закрыто, поддержки MS CA больше нет, купить его тоже нельзя
  - С 30 сентября 2023 г. Microsoft перестаёт продлевать подписки корпоративным клиентам из России
- Полноценных аналогов корпоративного MS CA в Open Source проектах нет
  - Коммерческие Enterprise-версии CA под Linux - стратегический товар - под строгим запретом, в Россию не поставляются

✓ **Не путать корп. CA с УЦ для ЭП (63-ФЗ) — разные задачи и разные требования!**

✓ **Риски блокирования работы сервиса MS CA - достаточно большие**

✓ **MS CA нужно заменять как можно скорее**

Aladdin Enterprise CA

НОВИНКА!

Корпоративный центр сертификации (CA) под Linux
- ключевой компонент
для обеспечения доверия в ИТ-инфраструктуре на базе PKI

Сертификация: по линии ФСТЭК России (до гостайны вкл.)

В Реестре отечественного ПО

Импортозамещение: Microsoft Certificate Services (MS CA)

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

Aladdin Enterprise CA под Linux

- Обеспечивает
  - Создание и функционирование корпоративной инфраструктуры открытых ключей (PKI)
  - Управление жизненным циклом цифровых сертификатов
  - Объединение всех компонентов ИТ-инфраструктуры в **единый домен безопасности,** их аутентификацию и безопасное взаимодействие
  - Обслуживание в **автоматическом** режиме всех объектов и компонентов корпоративной инфраструктуры ключами и цифровыми сертификатами
    - контроллеров доменов
    - серверов, Web-серверов, эл. почты
    - роутеров, маршрутизаторов, межсетевых экранов, VDI, VPN, RDP-шлюзов
    - компьютеров и др. устройств в доменах
    - M2M, IIoT-устройств
    - пользователей
  - Построение доверенной безопасной ИТ-инфраструктуры на базе PKI в сложных гетерогенных, облачных и мультиарендных инфраструктурах с разделением ролей и полномочий
  - Масштабирование, отказоустойчивость и разделение ролей
    - каждая функциональная роль центра сертификации (CA, RA, WebEnrol, CDP, DB и др.) может быть развёрнута на отдельном сервере в отказоустойчивой конфигурации

Aladdin Enterprise CA под Linux

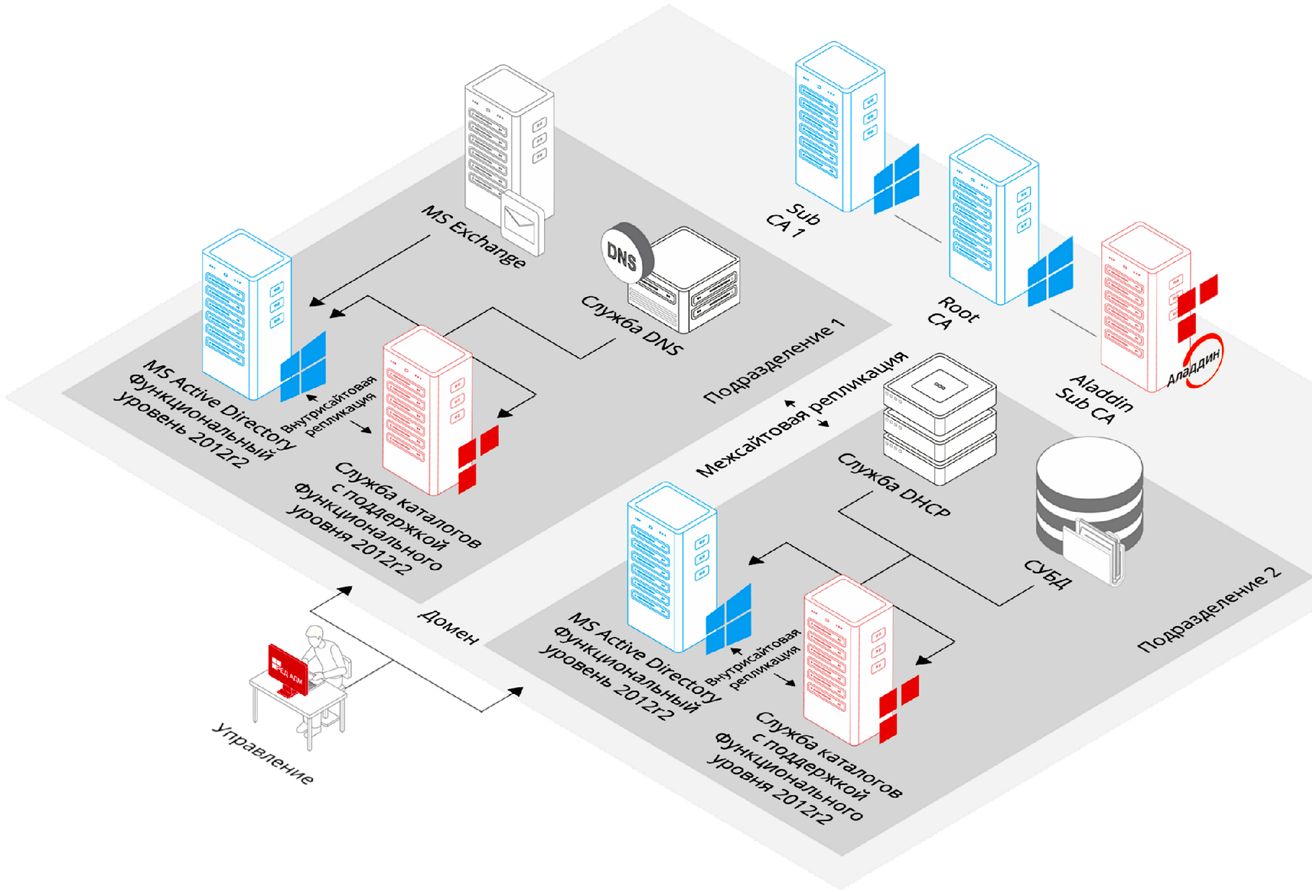
- Позволяет
  - Поставить Aladdin eCA параллельно с действующим MS CA
    - Выпустить на него подчинённый сертификат (от действующего корневого CA)
    - Настроить автоматический выпуск новых сертификатов
    - Импортировать и использовать действующие шаблоны сертификатов Microsoft CA, создавать новые
  - Одновременно работать с различными службами каталогов (**как Windows, так и Linux**)
    - MS Active Directory
    - Samba DC
    - FreeIPA
    - ALD Pro
    - РЕД АДМ (промышленная редакция) - отработаны сценарии бесшовной миграции
    - Альт Домен
  - Интегрироваться с различными внешними системами через REST API
    - IdM, IAM, IGA, SIEM, **JMS** и др.
  - Обеспечить строгую двухфакторную аутентификацию (в т.ч. под Linux)
  - Использовать различные архитектуры аппаратных платформ, отечественные ОС, виртуальные среды

Бесшовная миграция доменов и PKI

Репликация с Microsoft Active Directory

- Структуры домена
- Пользователей (пароли, атрибуты)
- Поддержка групповых политик
- Поддержка работы гетерогенной инфраструктуры (Windows, Linux)
- Шаблоны сертификатов
- Плавный вывод из ИС продуктов Microsoft без остановки сервисов
- Не требуется строить новый отдельный домен/лес

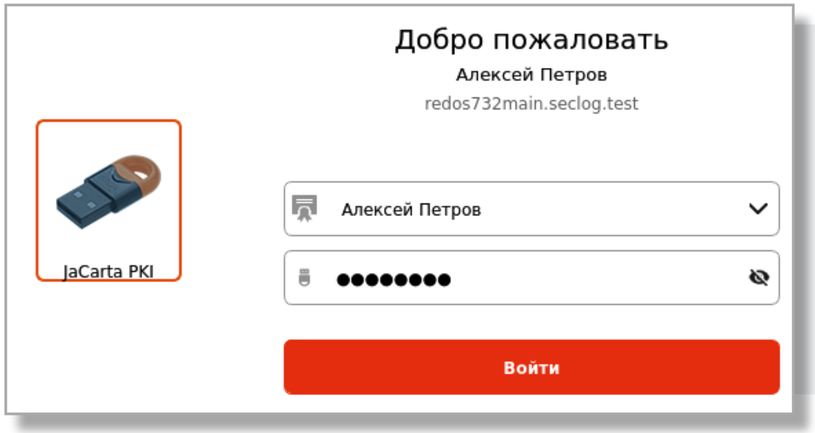
✓ **Бесшовная миграция домена и центра сертификации**



Поддержка PKI и 2ФА на клиенте Linux

Aladdin SecurLogon

НОВИНКА!



PKI-клиент и поддержка средств 2ФА в Linux

- замена MS Smart Card Logon

Проблемы:

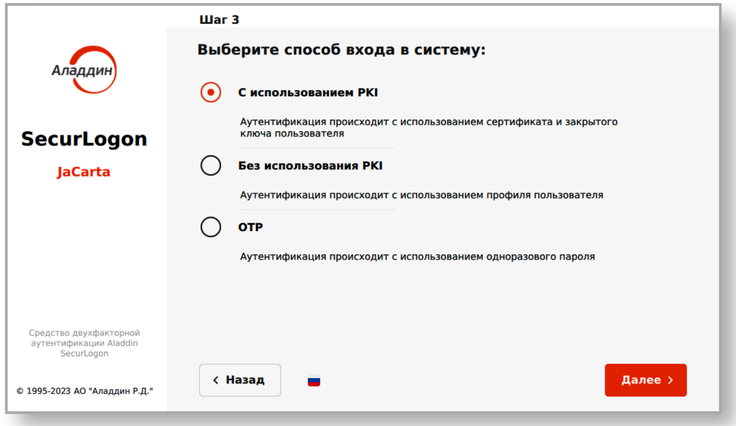
В MS Windows 2ФА пользователей реализует встроенная подсистема Windows Smart Card Logon

В российских ОС на базе Linux подобного механизма нет, всё надо делать руками (34 доп. пакета), но это будет только вход в Linux (замкнутая экосистема)

Aladdin SecurLogon

- Обеспечивает
  - **Полноценную поддержку PKI**, двух- и трёхфакторную **строгую** аутентификацию пользователей в смешанных гетерогенных средах, в ОС на базе Linux, Windows и macOS
  - Работу с доменами Microsoft AD, FreeIPA, Samba DC, ALD Pro
  - Усиленную аутентификацию пользователей с использованием автоматически сгенерированного сложного пароля длиной до 63 символов
    - Для инфраструктур, где **PKI ещё не развёрнута**
  - Применение политик входа на основе принадлежности пользователя к группе безопасности (только токен, токен или пароль, только пароль)
  - Групповое развёртывание и удалённую настройку с рабочего места администратора
  - Защиту удалённых соединений (RDP, SSH)
  - Дополнительные сервисные функции, позволяющие до входа в ОС разблокировать токен, сменить ПИН-код пользователя, кастомизировать окно приветствия и др.

✓ **Полноценная альтернатива Microsoft Smart Card Logon на отечественных ОС на базе Linux**



Работает с USB-токенами и смарт-картами JaCarta

Средства для строгой двухфакторной аутентификации (2ФА) и ЭП

- безопасный доступ в Linux по сертификатам (PKI)

Во многих ИТ-инфраструктурах в РФ до сих пор не используется 2ФА

2ФА - не значит СТРОГАЯ

Строгая аутентификация для Linux

- Что значит СТРОГАЯ
  - Двухфакторная (2ФА), с использованием персонального специализированного защищённого устройства (требования новых ГОСТов)
    - с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом
    - с хранением сертификатов доступа с памяти устройства
    - с возможностью его использования только авторизованным пользователем
    - неклонируемого (Secure by design)
  - Взаимная (аутентификация обеих сторон)
  - С использованием защищённых протоколов
- Требуется
  - Во всех системах, обрабатывающих значимую информацию
    - гос. организации, КИИ, АСУ ТП и др.
  - Для администраторов, пользователей, удалённых пользователей
  - Развёрнутая инфраструктура открытых ключей (PKI)
  - Централизованное управление жизненным циклом сертификатов, средств 2ФА
  - Модуль поддержки средств 2ФА и PKI для Linux
    - **В Linux нет аналога MS Smart Card Logon**

Линейка USB-токенов и смарт-карт JaCarta
(вкл. российские чипы I и II категории)
с сертификацией до КС-3 (ФСБ) и УД-4 (ФСТЭК)

BIO-токен

АНОНС

2ФА на базе смарт-карт и USB-токенов уже недостаточно!

Нужна дополнительная надёжная **биометрическая** идентификация пользователей

ВАЖНО:

Для противодействия ВНУТРЕННЕМУ нарушителю

Чтобы ЭП стала действительно подписью, а не эл. печатью (физически не привязанной к своему владельцу)!

Система централизованного управления
жизненным циклом сертификатов, токенов, СЗИ, СКЗИ

Включает высокопроизводительный сервер аутентификации Enterprise-класса - JAS

Импортозамещение: любого импортного аналога

Версии: Linux, Windows

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

JMS - система централизованного управления Enterprise-класса

- Обеспечивает
  - Учёт и управление жизненным циклом
    - токенов, смарт-карт, "облачных", программных токенов, OTP/PUSH/SMS аутентификаторов, U2F-токенов
    - защищённых съёмных носителей
    - смарт-карт ридеров
    - средств безопасной дистанционной работы
    - СЗИ, СКЗИ, сертификатов, объектов PKI, профилей
  - Автоматизацию большинства рутинных операций и применения политик безопасности (например, требований к ПИН-кодам)
  - Быструю подготовку типовых профилей, конфигураций для разных групп пользователей, ввод в эксплуатацию новых средств, "взятие под управление" выпущенных до внедрения JMS
  - Удобный сервис самообслуживания пользователей (Web-портал)

JMS - система централизованного управления Enterprise-класса

- Позволяет
  - Интегрироваться с внешними ресурсными системами - источниками информации о пользователях и рабочих станциях, с сервисом "облачной" подписи КриптоПро DSS и др.
  - Связывать учётные записи пользователей из различных ресурсных систем
  - Обслуживать сертификаты для аутентификации и ЭП, выданных различными удостоверяющими центрами
  - Вести мониторинг и аудит действий пользователей и администраторов с выгрузкой на сервер Syslog для интеграции с SIEM
  - Автоматически рассылать уведомления
  - Дистанционно и безопасно обновлять "прошивки" устройств (firmware), образы встроенных ОС и приложений (только для своих продуктов!)
  - Добавлять необходимую функциональность за счёт разработки и подключения дополнительных модулей и коннекторов
  - Использовать версию для Linux или для Windows
- Сертификаты
  - ФСТЭК России
  - Минобороны России (для работы с гостайной со степенью секретности "Совершенно секретно")

Давайте делать всё правильно и безопасно!

- Нам дали уникальную возможность сделать всё правильно
  - Не пытаться точечно заместить один продукт другим, а начать с проектирования правильной и безопасной ИТ-инфраструктуры
- На банковском рынке это удалось сделать
  - Россия совершила "квантовый скачок" - перепрыгнула целую эпоху платёжных карт с магнитной полосой, сразу на смарт-карты - и стала одним из лидеров
- У нас есть исторический шанс
  - Спроектировать наши ИТ-инфраструктуры правильно и безопасно, без наследования "родимых пятен"
  - Давайте стараться делать всё правильно и безопасно!
    - *PKI, сертификаты доступа, строгая аутентификация каждого субъекта и объекта ИТ-инфраструктуры и ИС*

Аладдин

Спасибо!

Сергей Груздев

ген. директор
АО "Аладдин"

www.aladdin.ru

О компании

АЛАДДИН – ведущий российский разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов.

Компания работает на рынке с апреля 1995 г.

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, а во многих крупных организациях и Федеральных структурах - стандартом де-факто.

Компания имеет все необходимые лицензии ФСТЭК, ФСБ и Минобороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной, производство, поставку и поддержку продукции в рамках гособоронзаказа.

Большинство продуктов компании имеют сертификаты соответствия ФСТЭК, ФСБ, Минобороны России и могут использоваться при работе с гостайной со степенью секретности до "Совершенно Секретно".

С 2012 г. в компании внедрена система менеджмента качества продукции (СМК), ежегодно проводится внешний аудит, имеются соответствующие сертификаты ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и ГОСТ РВ 0015.002-2020 на соответствие требованиями российского военного стандарта, необходимые для участия в реализации гособоронзаказа.

Ключевые компетенции

- Аутентификация
  - Подготовлено 12 национальных стандартов по идентификации и аутентификации (ГОСТ 58833-2020, ГОСТ Р 70262-2022)
  - Выпущено учебное пособие "Аутентификация – теория и практика"
  - Защищена докторская диссертация
- Доверенная загрузка и технология "стерилизации" импортных ARM-процессоров с TrustZone
- Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, смарт-карт, JavaCard
- Биометрическая идентификация и аутентификация по отпечаткам пальцев (Match On Card/Device)
- PKI для Linux и российских ОС
- Прозрачное шифрование на дисках, флеш-накопителях
- Защита баз данных и технология "опровославливания" зарубежных СУБД
- Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IIoT-устройств, Web-порталов и эл. сервисов.