Функция риска для многофакторной аутентификации в Интернете вещей

Беззатеев С.В.[1], Волошина Н.В.[1], Афанасьева А.В.[1], Бакунова А.В.[2], Зыбин В.А.[3], Петров В.И.[4]

1 Санкт-Петербургский государственный университет аэрокосмического приборостроения

2 Москва, Корпорация Intel

3 Хиллсборо, Орегон, Корпорация Intel

4 Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича

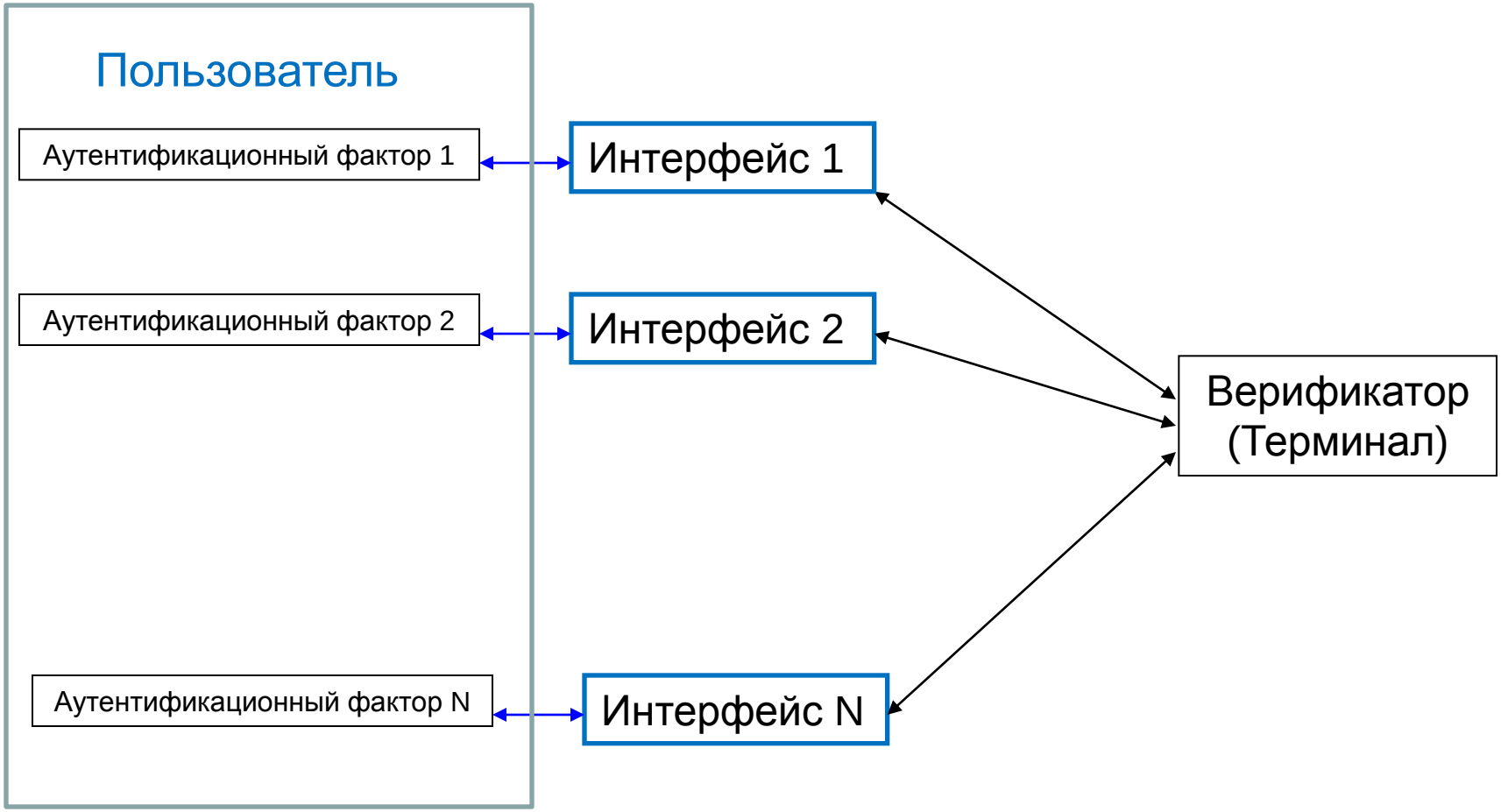
РусКрипто 2016

22 – 25 марта, г. Солнечногорск.

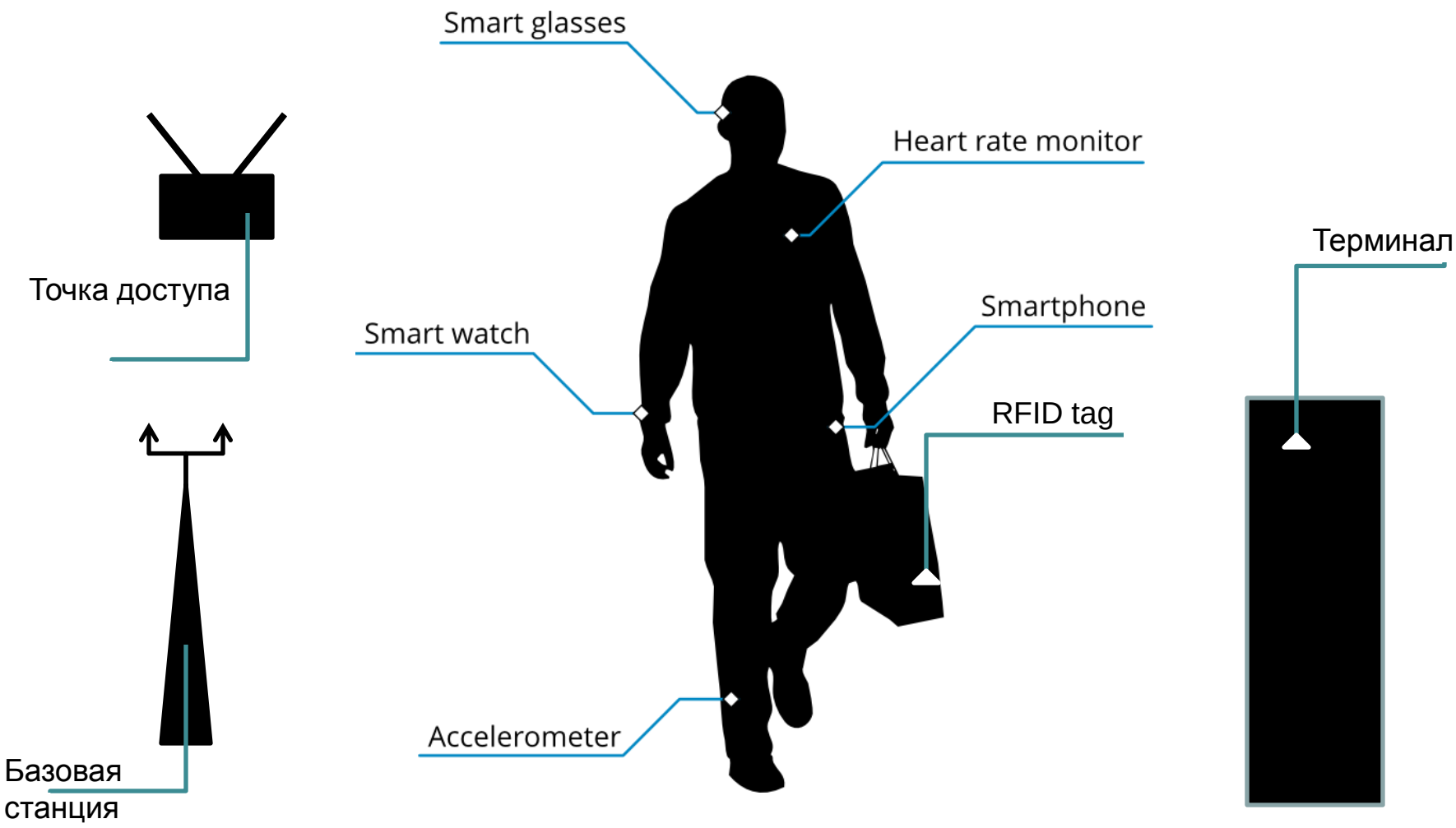
Однофакторная аутентификация

Фактор	Примеры
Пользователь знает (фактор знания)	Пароль, персональный номер идентификации (PIN), ключевая фраза, имя, номер телефона, и т.д.
Пользователь имеет (фактор владения)	Смарт карта, токен, одноразовый пароль, водительские права и т.д.
Пользователь есть (неотъемлемый фактор)	Отпечаток пальца, линии ладони, радужная оболочка глаза, ДНК, голос и т.д.
Пользователь характеризуется (фактор поведения)	Поведение, походка, клавиатурный почерк и т.д.

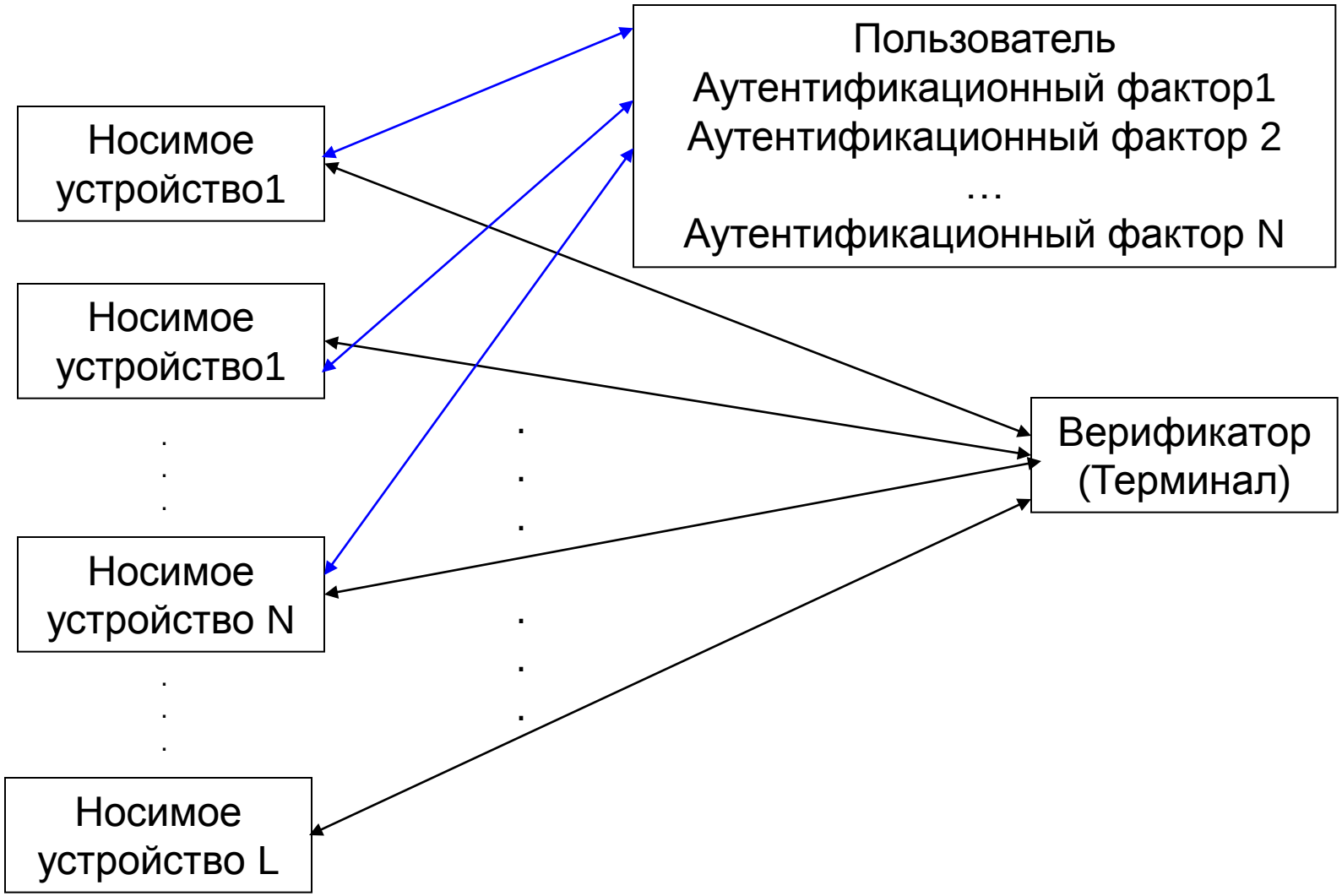
Многофакторная аутентификация



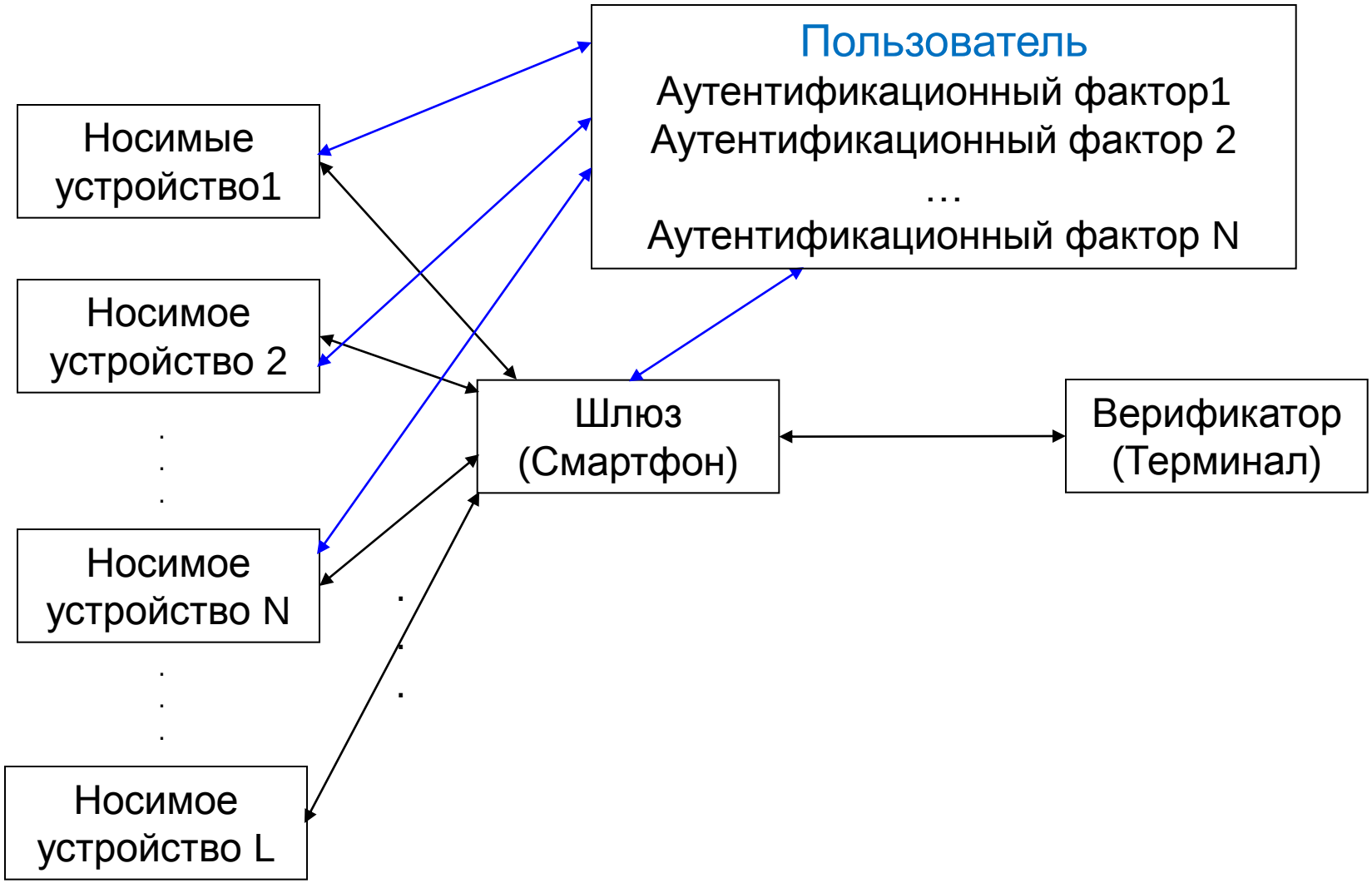
Носимые устройства



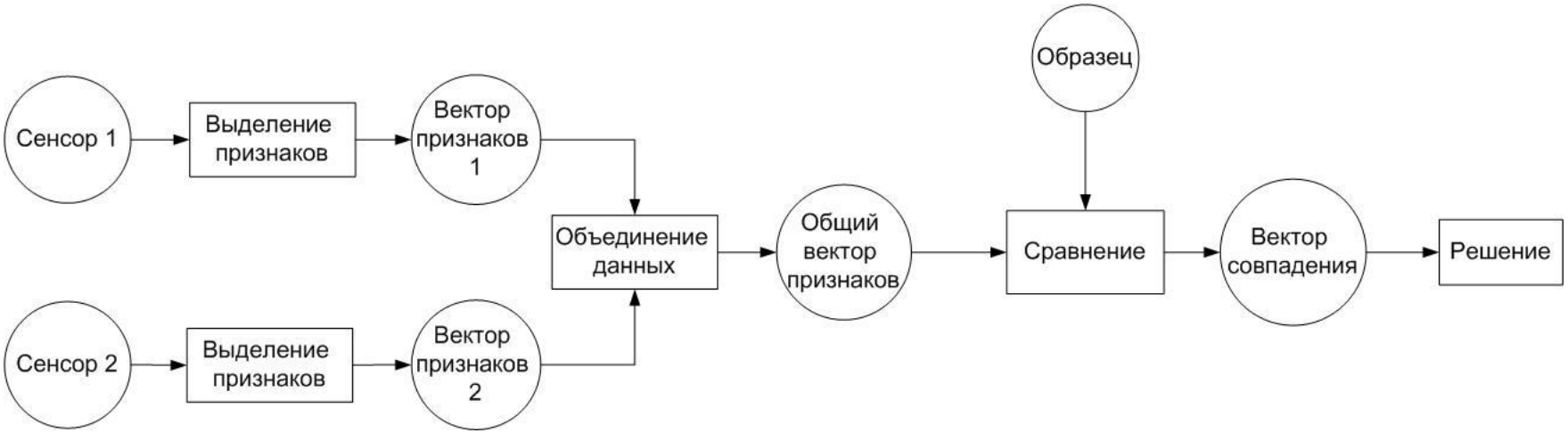
Аутентификация с использованием носимых устройств



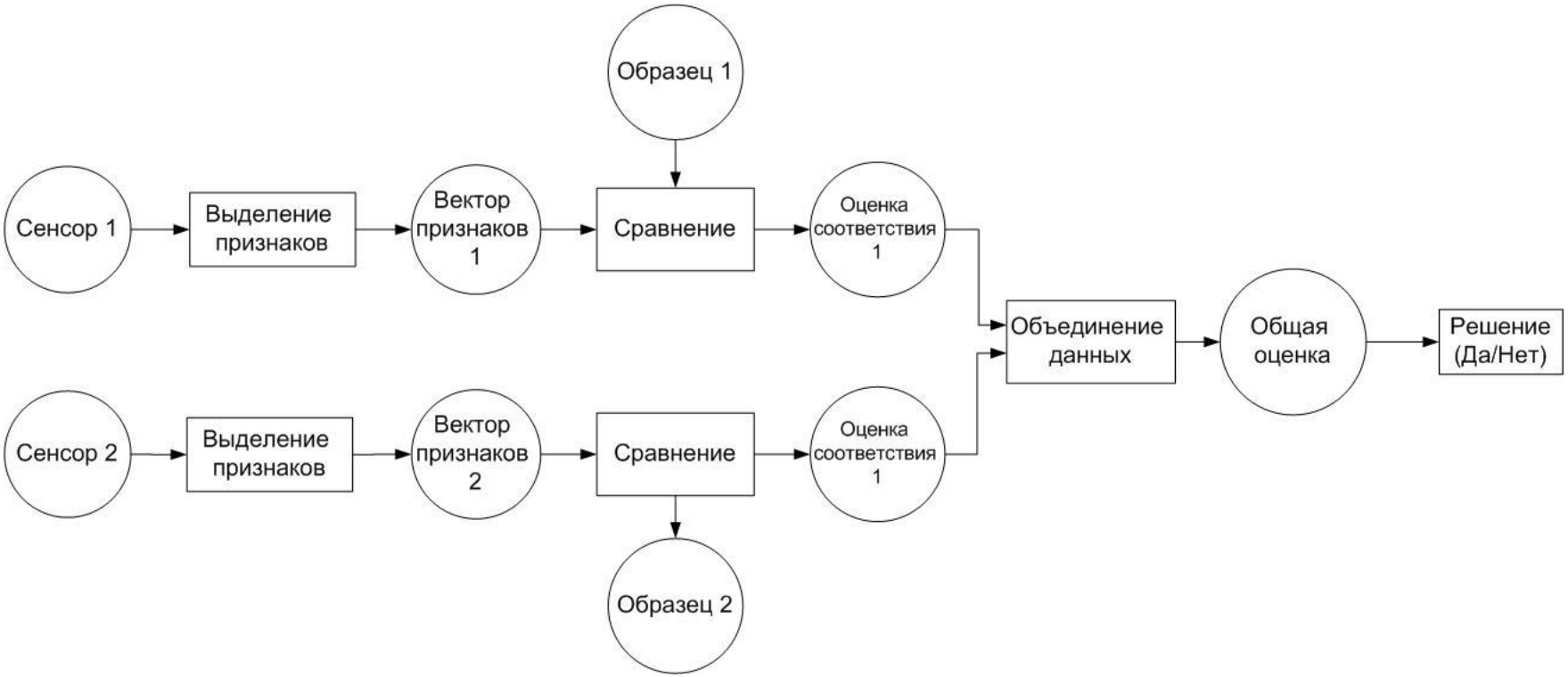
Аутентификация с использованием носимых устройств



Слияние данных при аутентификации- I



Слияние данных при аутентификации- II

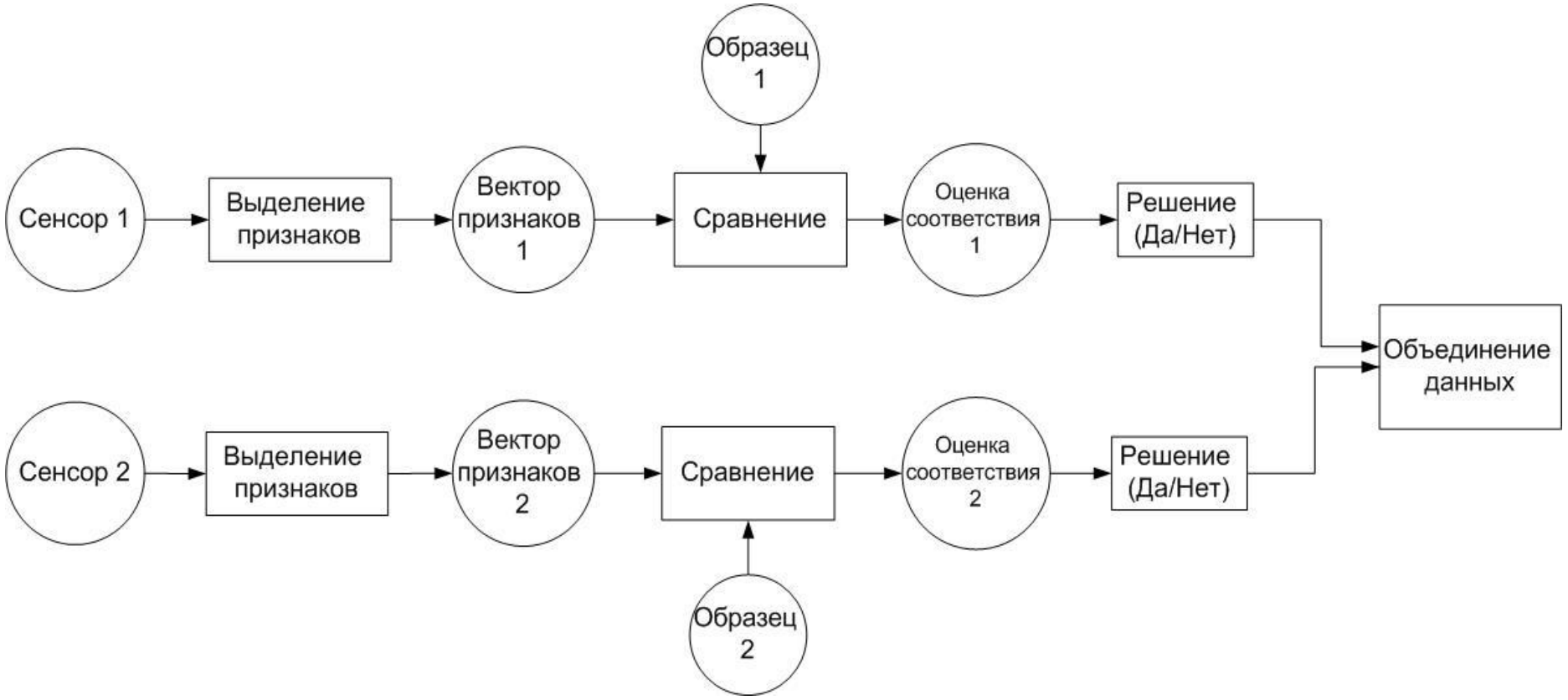


Оценочный уровень принятия решения

- Вероятностная оценка данных
  - Теорма Байеса
  - Одномерная функция плотности Гаусса
  - Функция β-распределения
- Фильтр Калмана
- Нечеткая логика
- Нейронные сети

Слияние данных при аутентификации- III

Уровень принятия окончательного решения



Уровень принятия окончательного решения

- И
- ИЛИ
- Пороговая схема
- Простое мажоритарное решение
- Взвешенное мажоритарное решение

Гипотезы принятия решения и отказа

Гипотеза H0 – нелегальный пользователь;

Гипотеза H1 — легальный пользователь.

Эти гипотезы составляют полное пространство событий и несовместны между собой:

$$P(H0) + P(H1)=1.$$

Принятие положительного решения об аутентификации происходит при условии (x>X) , тогда:

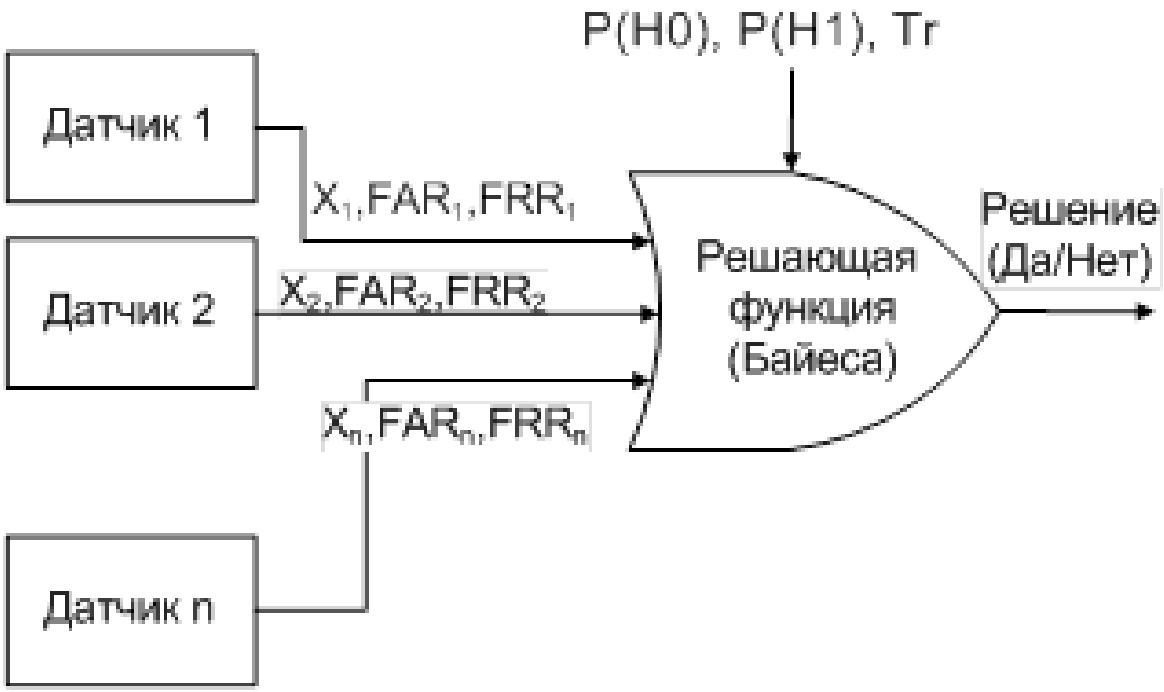
FAR (вероятность ложной тревоги(False Acceptance Rate))

$$FAR(X)=Prob(x>X/H0)= 1-Prob(x\leq X/H0)=1-F(X/H0)$$

FRR (вероятность пропуска цели(False Rejection Rate))

$$FRR(X) = Prob(x\leq X / H1)=\Phi(X/H1),$$

Многофакторная аутентификация



Tr - пороговое значение для принятия решения.

Датчики с функциями Байеса

После получения X в зависимости от своего типа датчик возвращает:

- (АНАЛОГОВЫЙ ДАТЧИК) соответствующие этому X и выбранной гипотезе значения :

  гипотеза H0: $Prob(x \le X / H0)$ и $Prob(x \le X/H1)=FRR(X)$.

  гипотеза H1: $Prob(x \le X / H0) = 1 - FAR(X)$ и $Prob(x \le X/H1)$.

- (БИНАРНЫЙ ДАТЧИК) соответствующие этому X и выбранной гипотезе значения :

  решение X' в зависимости от положения точки X относительно операционной точки OP :

  если $X<OP$, то $X'= 0$

  и $Prob(0/H0)= 1 - FAR(OP)$, $Prob(0/H1)= FRR(OP)$,

  если $X \ge OP$, то $X' = 1$

  и $Prob(1/H0)= FAR(OP)$, $Prob(1/H1)= 1 - FRR(OP)$,

Принятие решения для многофакторной схемы

1. Решение об аутентификации принимается по пороговому правилу

$P(H1/X) > Tr \Rightarrow$ Access, иначе Reject,

где Tr - пороговое значение для принятия решения(дополнительный параметр системы).

2. Решение об аутентификации принимается по правилу

$P(H1/X) > P(H0/X) \Rightarrow$ Access,

$P(H1/X) < P(H0/X) \Rightarrow$ Reject

Использование функции риска

- Средние прямые потери(ADL)

$$ADL = FAR * AvCost * n,$$

- Средние косвенные потери (AAL)

$$AAL = FRR * AlCost * n.$$

- Функция риска (RF)

$$RF = ADL + AAL.$$

Процедура обратной связи

После установления требуемого RF

- Нахождение FAR и FRR
- Подбор параметров функции Байеса:
  Tr, P(H0), P(H1)

СПАСИБО
ЗА
ВНИМАНИЕ!

Протоколы аутентификации

Обмен аутентификационной информацией [ITU-T X.1035]

Пользователь		Терминал
	Пользователь и терминал обмениваются: Секретный пароль ← pw → Параметры протокола (DH) ← {g,N} →	
x=random() , $R_u = g^x \bmod N$, $H_{1U}= H_1$(User,Terminal, pw), $U= H_{1U} \cdot R_u$, $H_{2U}= H_2$(User,Terminal, pw),		y=random() , $R_T = g^y \bmod N$, $H_{1T}= H_1$(User,Terminal,pw), $T= H_{1T} \cdot R_T$, $H_{2T}= H_2$(User,Terminal, pw),
Инициализация		
	U →	
		$U / H_{1T} = g^x \bmod N = R_u$, $S= R_u^y \bmod N$, $T= H_{2T} R_T$, $A_1=H_3$(User | Terminal | pw | R_T |S),
	← {A_1, T}	
$R_T = T/ H_{2U}$, $S= R_T^x \bmod N$ H_3(User | Terminal | pw | R_T |S) =?= A_1 ,		
Аутентификация терминала		

Обмен аутентификационной информацией [ITU-T[ITU-T X.1035]

Пользователь		Терминал
$A_2=H_4(User \mid Terminal \mid pw \mid R_U \mid S)$,	U →	
		$H_4(User \mid Terminal \mid pw \mid R_u \mid S) =?= A_2$
Аутентификация пользователя		

Простой обмен степенью ключа

Пользователь		Терминал
	Пользователь и терминал обмениваются: секретный ключ ← pw → Общий модуль для протокола (DH) ← N →	
x=random() , $R_u = f(pw)^x \bmod N$,		y=random() , $R_T = f(pw)^y \bmod N$,
Инициализация		
	R_u → ← R_T	
$K_U = H(R_T^x) = K$		$K_T = H(R_U^y) = K$
	← $\{A_1, T\}$	
C_U = random()		
	$E_K(C_U)$ →	
		C_T = random()
	← $E_K(C_U, C_T)$	
$D_K(E_K(C_U, C_T))$, C_U правильное?		
Аутентификация терминала		

D. P. Jablon: Strong password-only authenticated key exchange, *ACM Computer Communications Review*, October 1996.

Простой обмен степенью ключа

Пользователь		Терминал
	$E_K(C_T)$ →	
		$D_K(E_K(C_T))$, C_T правильное ?
Аутентификация пользователя		

Secure Remote Password protocol [IETF RFC 2945]

Пользователь		Терминал
<salt>= random(), x = SHA(<salt> | SHA(<username> | ":" | <raw password>)), <password verifier> = g^x mod N	Пользователь и терминал обмениваются: Числом для протокола (DH) ←N → Пользователь отправляет терминалу { <username>, <password verifier>, <salt> }→	
Инициализация		
	<username>→	s=<salt>
	← s	
a = random() A=g^a mod N		
	A →	
		v = <password verifier> , b = random(), B = (v + g^b) mod N
	←B	

T. Wu, "The Secure Remote Password Protocol", In Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security, San Diego, CA,pp. 97-111.

Secure Remote Password protocol [IETF RFC 2945]

Пользователь		Терминал
p = <raw password> , x = SHA(s | SHA(U | ":" | p)), $S = (B - g^{x})^{(a + u \cdot x)} \bmod N$, K = SHA_Interleave(S)		$S = (A \cdot v^{u})^{b} \bmod N$, K = SHA_Interleave(S)
K – парный ключ для пользователя и терминала		
M_{user} = H(H(N) XOR H(g) | H(U) | s | A | B | K)	M_{user} →	$M_{terminal}$= H(H(N) XOR H(g) | H(U) | s | A | B | K) M_{user}=?= $M_{terminal}$
Аутентификация пользователя		
L_{user} =H(A | M | K) L_{user}=?= $L_{terminal}$	← $L_{terminal}$	$L_{terminal}$ =H(A | M | K)
Аутентификация терминала		

T=T[0]T[1]T[2]T[3] ... T[19], T[i] – i-th byte,

E = T[0] | T[2] | T[4] … F = T[1] | T[3] | T[5] ... , G = SHA(E), H = SHA(F) ,

SHA_Interleave(T) = G[0] | H[0] | G[1] | H[1] | ... | G[19] | H[19]

Аутентификация и выработка общего ключа с использованием пароля

Пользователь		Терминал
	Пользователь и терминал обмениваются: Числа для протокола (DH) ← $N=rq+1$, $g \in Z_q$ →	
h=raw password, amplified password =$a=g^h \bmod N$,	a →	
Инициализация		
x=random(), $G_1=g^x \bmod N$	G_1 →	
		y=random() $G_2 = (G_1 a)^y = g^{(x+h)y} \bmod N$ $c=G_1^y \bmod N$
	← G_2	
$u=(x+a)^{-1} x \bmod q$, $b=G_2^u \bmod N = g^{xy} \bmod N$, $K_1 = H(b)$		
	K_1→	
		$K_2 = H(c)$, $K_1 =?= K_2$
Аутентификация пользователя		

T.Kwont: Authentication and Key Agreement via Memorable Password, *IACR*, e-print, August 2000