

# Особенности реализации мер по идентификации и аутентификации **на объектах КИИ**



**Владимир Иванов**

Директор по развитию  
Компания «Актив»

# Меры обеспечения безопасности значимого объекта

## Идентификация и аутентификация (ИАФ)

Обозначение и номер	Название
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИАФ.5	Идентификация и аутентификация внешних пользователей
ИАФ.6	Двусторонняя аутентификация
ИАФ.7	Защита аутентификационной информации при передаче

# Идентификация определения

<b>Методический документ «Меры защиты информации в государственных информационных системах»</b>	<b>ГОСТ Р 58833-2020 Защита информации ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ Общие положения</b>	<b>ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер</b>
Присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов	Действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов	Присвоение для осуществления логического доступа субъекту (объекту) доступа уникального признака (идентификатора); сравнение при осуществлении логического доступа предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов

# Аутентификация

## определения



<p><b>Методический документ «Меры защиты информации в государственных информационных системах»</b></p>	<p><b>ГОСТ Р 58833-2020 Защита информации ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ Общие положения</b></p>	<p><b>ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер</b></p>
<p>Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)</p>	<p>Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации</p>	<p>Проверка при осуществлении логического доступа принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)</p>

# ИАФ.0 Регламентация правил и процедур идентификации и аутентификации

## Организационная мера

- Политика информационной безопасности
- Правила и процедуры идентификации и аутентификации **пользователей, процессов, устройств**
- Документы, регламентирующие жизненный цикл учетных записей пользователей
- Документы, регламентирующие жизненный цикл средств аутентификации
- Документы, регламентирующие применение тех или иных способов и средств аутентификации пользователей, процессов и устройств
- Должностные инструкции сотрудников отделов ИБ в части, касающейся идентификации и аутентификации

# Уровни доверия аутентификаторам

Уровень доверия	Тип	
НИЗКИЙ	Запоминаемый секрет	
	Поисковый секрет	
	Внеполосный аутентификатор	
	Однофакторное OTP устройство	
СРЕДНИЙ	Многофакторное OTP-устройство	
	Однофакторное криптографическое программное средство аутентификации	
	Однофакторное криптографическое аппаратное устройство	
ВЫСОКИЙ	<b>Многофакторное криптографическое программное средство аутентификации</b>	
	<b>Многофакторное криптографическое аппаратное устройство (карта, токен)</b>	

# ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов

## Техническая мера

- IdP (Identity Provider) разного рода. Могут включать средства, предоставляемые операционными системами, службами каталогов, средствами доверенной загрузки
- СЗИ от НСД
- IDM и IAM системы
- SSO системы
- PAM системы
- Системы мониторинга
- Средства PKI для аутентификации процессов

# ИАФ.2 Идентификация и аутентификация устройств

## Техническая мера

- MAC и IP адреса **не обеспечивают доверия**
- Применение профилей устройств (fingerprint)
- Применение аппаратных SAM модулей
- Применение служебных PKI сертификатов для аутентификации устройств
- Системы контроля съемных носителей информации
- DLP системы
- Применение стандарта IEEE 802.1X



# ИАФ.3 Управление идентификаторами

## Техническая мера

- IdP (Identity Provider) разного рода. Могут включать средства, предоставляемые операционными системами, службами каталогов, средствами доверенной загрузки
- СЗИ от НСД
- IDM и IAM системы
- Межсетевые экраны

# ИАФ.4 Управление средствами аутентификации

## Техническая мера

- Службы каталогов
- Системы управления жизненным циклом средств аутентификации (системы управления токенами и картами и т.п.)
- СЗИ от НСД

# ИАФ.5 Идентификация и аутентификация внешних пользователей

## Техническая мера

- IdP (Identity Provider) разного рода. Могут включать средства, предоставляемые операционными системами, службами каталогов, средствами доверенной загрузки
- СЗИ от НСД
- IDM и IAM системы
- SSO системы
- PAM системы
- Системы мониторинга

# ИАФ.6 Двусторонняя аутентификация

## Техническая мера

- Встроенные механизмы операционных и прикладных систем, аппаратных средств, активного сетевого оборудования
- Применение TLS с двусторонней аутентификацией
- Межсетевые экраны

# ИАФ.7 Защита аутентификационной информации при передаче

## Техническая мера

- Защита аутентификационной информации при вводе
- Шифрование аутентификационной информации при передаче (например через TLS)



## **Владимир Иванов**

Директор по развитию  
Компании «Актив»

✉ [vov@rutoken.ru](mailto:vov@rutoken.ru)