КОМПАНИЯ АКТИВ

Особенности реализации мер по идентификации и аутентификации на объектах КИИ

Владимир Иванов

Меры по обеспечению безопасности (239 Приказ ФСТЭК)

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

ИАФ.0 Регламентация правил и процедур идентификации и аутентификации

Организационная мера

- Политика информационной безопасности
- Правила и процедуры идентификации и аутентификации **пользователей, процессов, устройств и других сущностей** в соответствии с имеющимися угрозами
- Документы, регламентирующие жизненный цикл учетных записей пользователей и других идентификаторов
- Документы, регламентирующие жизненный цикл средств аутентификации
- Документы, регламентирующие применение тех или иных способов и средств аутентификации пользователей, процессов, устройств и других сущностей
- Инструкции для сотрудников отделов ИБ в части, касающейся идентификации и аутентификации
- Инструкции для персонала по соблюдению мер безопасности, в частности, при обращении с аутентификаторами

ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов

Техническая мера

- Реализуются при помощи IdP (Identity Provider) разного рода. Могут включать средства, предоставляемые операционными системами, службами каталогов, средствами доверенной загрузки
- Следует учитывать специфику прикладных систем
- Следить за правильностью применения средств аутентификации
- Следует избегать применения «самодельных» систем аутентификации

- Под процессами можно понимать как исполняемый код приложений, так и бизнес-процессы, реализуемые прикладными системами
- Аутентификацию исполняемого кода по фактору знания (статические и динамические пароли) нельзя реализовать безопасным способом
- Контроль целостности исполняемого кода не гарантирует его аутентичности. Нужно применять криптографические средства – проверку подписи исполняемого кода

ИАФ.2 Идентификация и аутентификация устройств

Организационные и технические меры

- MAC и IP адреса не обеспечивают доверия в качестве самостоятельных идентификаторов
- Применение профилей устройств (fingerprint)
- Для аутентификации требуется применение криптографических методов и соответствующих протоколов
- Применение аппаратных SAM и TPM модулей для хранения ключей аутентификации
- Применение служебных PKI сертификатов для аутентификации устройств
- Применение стандарта IEEE 802.1X

ИАФ.3 Управление идентификаторами

Организационные и технические меры

- Определение лица, ответственного за процессы идентификации
- Организация процессов сбора и верификации идентификационной информации (атрибутов) сущностей
- Создание и обеспечение уникальности идентификаторов в пределах домена
- Присвоение и уничтожение идентификаторов, изменение атрибутов
- Технические реализации управления жизненным циклом идентификаторов в IdP

ИАФ.4 Управление средствами аутентификации

Организационные и технические меры

- Определение лица, ответственного за процессы управления средствами аутентификации и их безопасность
- Создание, инициализация, персонификация, выдача, замена, обновление, блокирование, изъятие и другие процессы жизненного цикла аутентификаторов нужно автоматизировать
- Техническая реализация - системы управления жизненным циклом средств аутентификации (системы управления токенами и картами и т.п.)
- Нельзя сохранять аутентификационную информацию, в том числе и при использовании многофакторной аутентификации (запоминание PIN-кодов в прикладном ПО, пароли в конфигурационных файлах и скриптах и т.п.)

ИАФ.5 Идентификация и аутентификация внешних пользователей

Техническая мера

- Повышенные требования к идентификации
- Персонифицированные учетные записи для всех внешних пользователей
- Организация доступа через защищенные каналы
- Повышенные требования к аутентификации

ИАФ.6 Двусторонняя аутентификация

Техническая мера

- Применение протоколов, обеспечивающих взаимную аутентификацию субъекта и объекта доступа (например, TLS)
- Как правило, реализуется при помощи криптографических методов
- Требует PKI
- Где хранить ключи аутентификации процессов, сервисов, устройств и т.д.?
- Двусторонняя аутентификация с участием пользователей требует применения способов **строгой аутентификации**

ИАФ.7 Защита аутентификационной информации при передаче

Техническая мера

- Исключение передачи аутентификационной информации в открытом виде и через незащищенные каналы
- Шифрование аутентификационной информации при передаче (например через TLS)

КОМПАНИЯ АКТИВ

Владимир Иванов

info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90