УЦСБ

USSC.RU

ZERO TRUST

Современное прочтение правила «доверяй, но проверяй»

Вадим Гаврилов
Начальник отдела систем обеспечения информационной безопасности

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

Эволюция воззрений

Защита периметра

Сильный защитный периметр вокруг сети, внешние пользователи и системы не имеют доступа к внутренней сети, внутренние пользователи и системы считаются доверенными и имеют доступ к внутренним ресурсам.

Эшелонированная оборона

Несколько независимых уровней (эшелонов) защиты, каждый из которых дополняет другие и предназначен для защиты от разных типов угроз. Если один уровень безопасности окажется уязвимым или не справится с атакой, другие уровни продолжают защищать систему, что повышает общую надежность и снижает вероятность успешного проникновения злоумышленника.

Концепция нулевого доверия

Пользователи и устройства не являются доверенными по умолчанию, даже если они были предварительно проверены и подключены к внутренней сети.

История возникновения

1994

Появление термина «нулевое доверие»

2001

1-я версия OSSTMM, доверие как уязвимость

2007

3-я версия OSSTMM, развитие идеи, отдельная глава о доверии, описание применения элементов управления OSSTMM в зависимости от уровня доверия

2010

Возникновение термина «модель нулевого доверия»

2018

Публикации документа NIST SP 800-207 — «Архитектура нулевого доверия»

Нулевое доверие (Zero Trust, ZT) — совокупность концепций и идей, призванных снизить неопределённость при принятии точных решений о доступе по запросу в информационных системах и сервисах в условиях, когда сеть считается скомпрометированной

Архитектура нулевого доверия (Zero Trust Architecture, ZTA) — это план обеспечения кибербезопасности предприятия, в котором используются концепции нулевого доверия и который включает в себя взаимодействие компонентов, планирование рабочих процессов и политики доступа

Архитектура нулевого доверия — что это?

Основы ZTA

Проверять явно

Всегда выполняйте аутентификацию и авторизацию на основе всех доступных данных

Использовать наименьшие привилегии

Ограничьте доступ пользователей с помощью технологий Just-In-Time и Just-Enough-Access (JIT/JEA), адаптивных политик на основе оценки рисков и защиты данных

Предполагать нарушения

Минимизируйте поверхность атаки и доступ к сегментам. Обеспечьте сквозное шифрование и используйте аналитику для контроля, обнаружения угроз и повышения уровня защиты

Базовые принципы ZTA

01 Презумпция нарушения

02 Минимизация привилегий

03 Контроль устройств

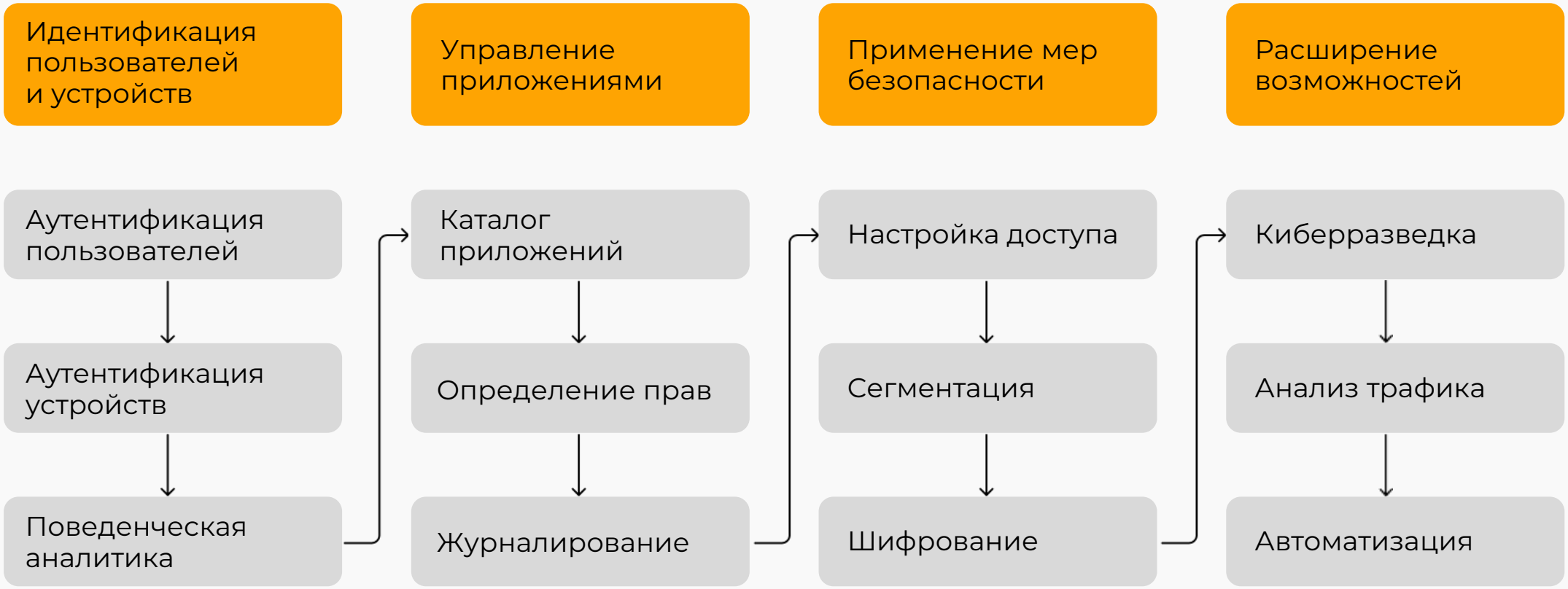
04 Многофакторная аутентификация

05 Микросегментация

06 Мониторинг и проверка

- Сущности
- Устройства
- Сети
- Приложения
- Данные

Направления внедрения



Плюсы и минусы

- Прозрачные принципы
- Безопасное подключение
- Последовательный динамичный подход
- Визуализация доступа
- Единые правила
- Ограничение горизонтального перемещения злоумышленников
- Повышение уровня конфиденциальности

- Сопротивление сотрудников
- Длительное время внедрения
- Возможные проблемы с доступом
- Требования к эффективности процессов
- Сложность обработки исключений
- Сложность внедрения
- Не решает всех проблем

ZTA в требованиях регуляторов

Приказ ФСТЭК №239
«Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

Требования ЦБ РФ (ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»

Приказ ФСТЭК № 17
«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Приказ ФСТЭК № 21
«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ZTA — очередной маркетинговый ход или необходимость?

УЦСБ

USSC.RU

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

Спасибо за внимание!

Вопросы?

Вадим Гаврилов

Начальник отдела систем обеспечения информационной безопасности

vgavrilov@ussc.ru