Дмитрий Кибенко
Dmitrii Kibenko

Технический директор ООО «Поволжский удостоверяющий центр»

Эксперт в области информационной безопасности

CTO Volga region certification center

Тема выступления: **Оптимизация безопасности - эффективные методы разграничения доступа в веб-системах.**

Topic of the speech: **Effective methods of access control in web systems**

Термины и определения

Идентификация

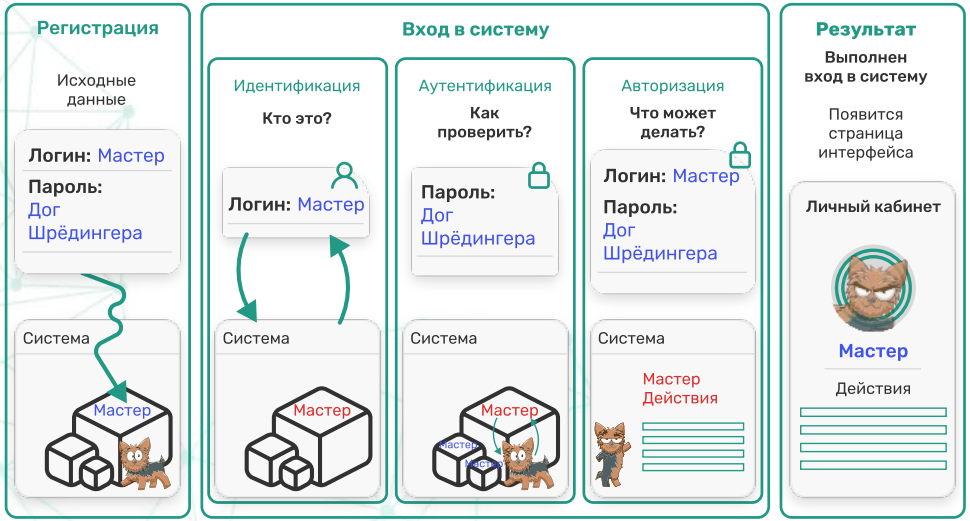
Присвоение для осуществления логического доступа субъекту (объекту) доступа уникального признака (идентификатора); сравнение при осуществлении логического доступа предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов.

Аутентификация

Проверка при осуществлении логического доступа принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Авторизация

Проверка, подтверждение и предоставление прав логического доступа при осуществлении субъектами доступа логического доступа.



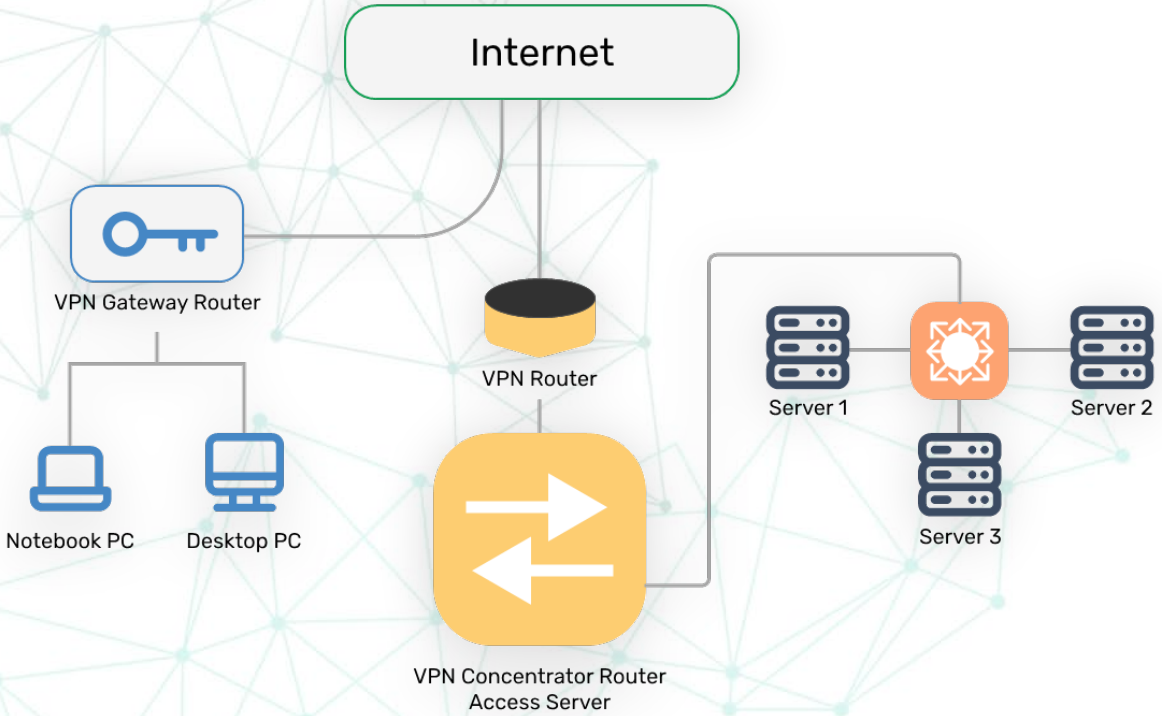
itglobal.com/wp-content/uploads/2021/05/gost-57580.1-1.pdf

Требования ФСТЭК России

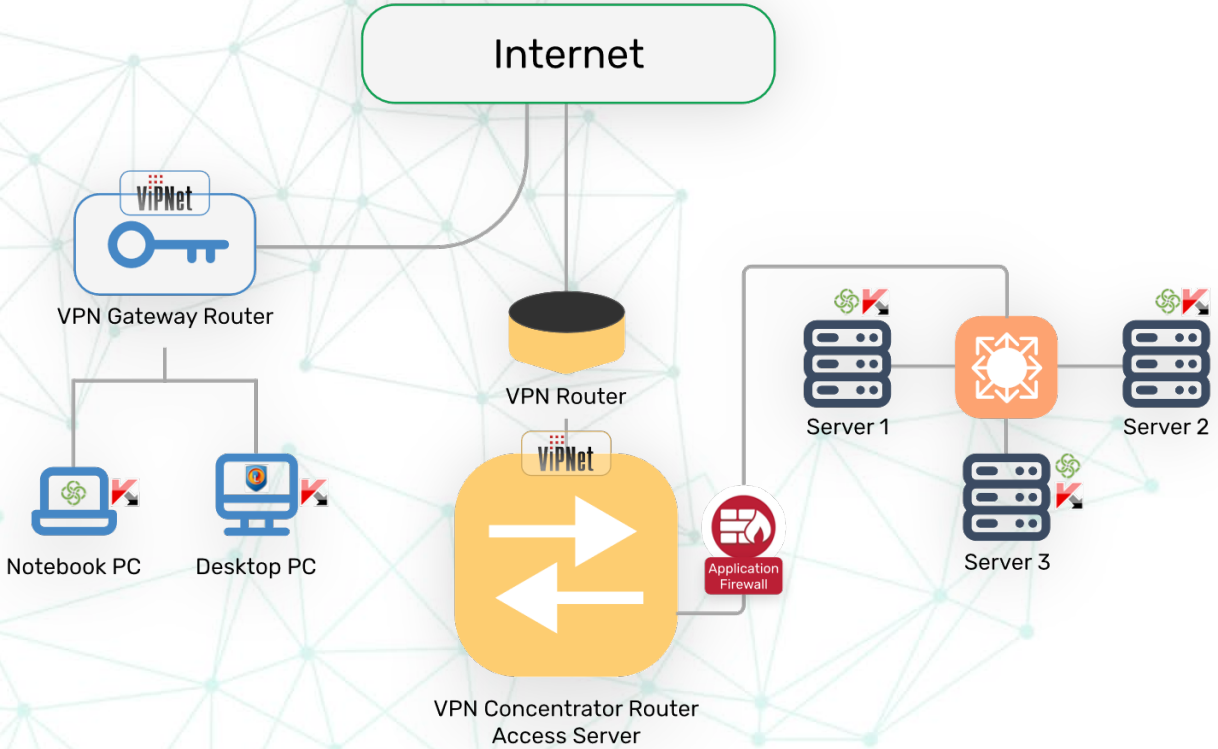
Приказы 17/21/239

- Идентификация и аутентификация субъектов доступа и объектов доступа .
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
- Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему.
- Ограничение числа параллельных сеансов доступа
- И др.

Типовая модель реализации функционала разграничения доступа в веб-системах



Типовая модель реализации функционала разграничения доступа в веб-системах

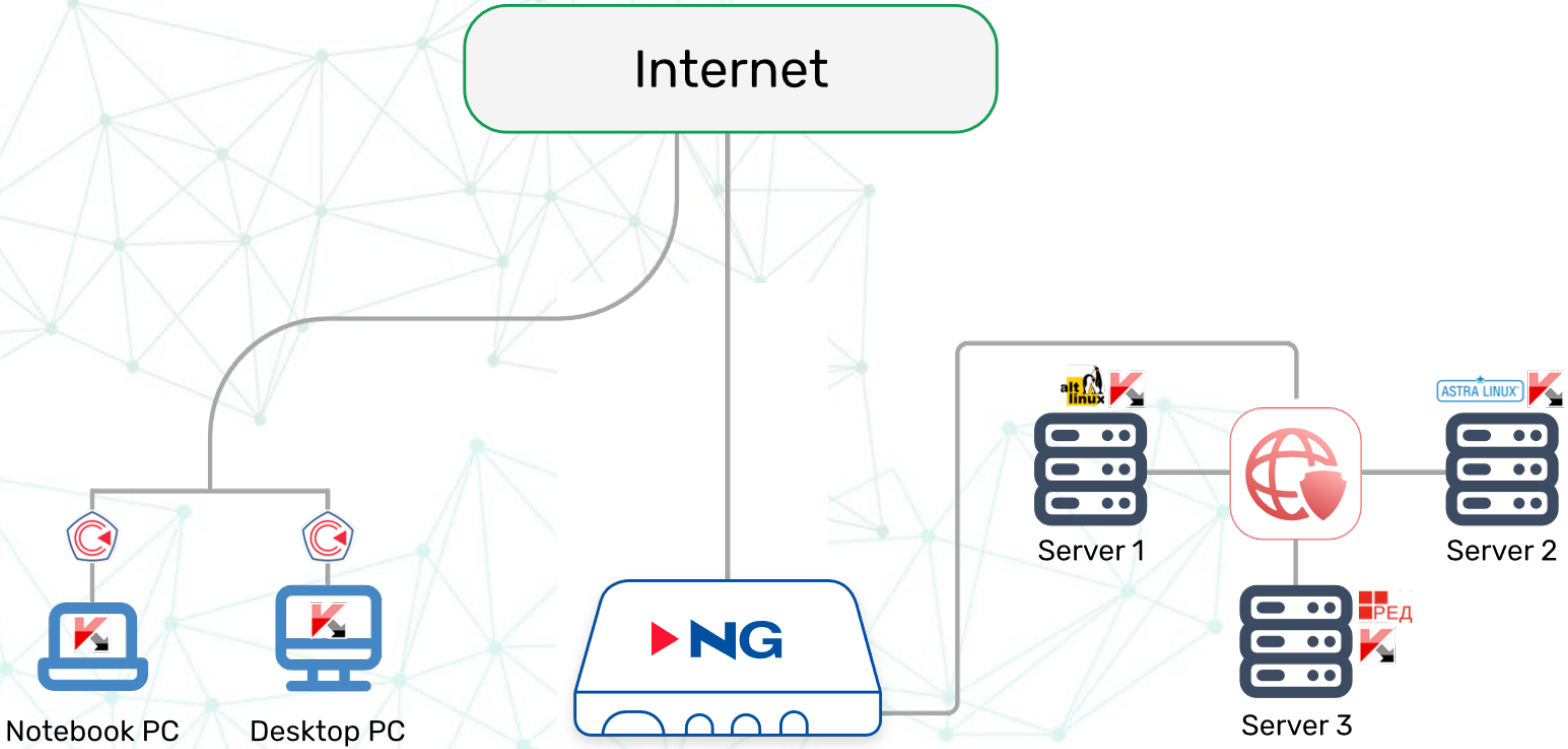


Основные вопросы к системам разграничения доступа

- Нужно ли сертифицировать информационную систему если механизмы аутентификации и авторизации реализованы в ней?
- Как минимизировать изменения в системе или исключить их при этом соответствовать требования безопасности?
- Как реализовать ролевую модель доступа в Web-системе?
- Как реализовать систему аудита действий пользователей и администраторов?
- Как уменьшить время аттестации системы?

WebGard

Современная схема защиты web-систем



WebGard

Программа защиты web-систем от несанкционированного доступа «WebGard 2.0» предназначена для защиты информации, не относящейся к государственной тайне, от несанкционированного доступа в web-системах массового обслуживания.

- Разграничение доступа администраторов к подсистеме управления.
- Фильтрация и аудит HTTP запросов пользователей.
- Система разграничения доступа пользователей к разделам сайта.
- Синхронизация с LDAP, БД web-приложениях и AD.
- Аудит действий администраторов.
- Регистрация событий безопасности.

В чем преимущества?

1. Реализация всех требований к подсистеме разграничения доступа из «коробки»
2. Отсутствует необходимость сертификации механизмов разграничения доступа
3. Контроль действий пользователей для администратора информационной безопасности
4. Интеграция с существующими инструментами аутентификации (AD, LDAP, FreeIPA, др.)

Сертификат соответствия ФСТЭК на ТУ и ТД по 4 уровню доверия

Соответствует ФЗ № 152 «О персональных данных»

Зарегистрирован в Едином реестре российских программ для ЭВМ и БД

АСУ до класса 1Г, в ИСПДн до 1 уровня и в ГИС до класса К1

Реализованные проекты

Ростехнадзор

ФНС России

РЖД

Минздрав РТ

МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Минцифра РТ

ЭТП

Электронная площадка ЭТП

Благодарю за внимание!

Thank you for your attention!

Дмитрий Кибенко
vrca.ru

Казань, 2023