пермский политех

Вопросы информационной безопасности при цифровизации образовательного учреждения

Докладчик:
Юрий Горбунов,
заместитель начальника
Управления цифровой трансформации
Пермский Политех

пермский политех

Пермский Политех сегодня

- один из ведущих многопрофильных инженерных вузов России
- один из лидеров рейтинга востребованности среди инженерных вузов (по данным МИА «Россия сегодня»)
- в числе ведущих научных и образовательных организаций РФ, имеющих право самостоятельного создания диссертационных советов и присуждения ученых степеней кандидатов и докторов наук
- обладатель гранта программы Приоритет 2030

Статистика инцидентов

- Рост числа фишинговых атак как на организации, так и на частных лиц
- Цель большинства атак –получение конфиденциальной информации (учетные данные, персональные данные, коммерческая тайна) нарушение основной деятельности
- Основные методы: социальная инженерия, фишинг
- Основные типы вредоносного ПО: шпионское, ПО удаленного управления, шифровальщики
- Активное использование инструментов искусственного интеллекта

- Импортозамещение не означает автоматическое повышение уровня безопасности
- Темпы импортозамещения сказываются, в том числе, и на количестве уязвимостей в ПО
- Регулярные обновления важны на всей инфраструктуре, несмотря на сложность и трудоемкость
- Использование open-source решений также не является гарантией отсутствия проблем

Применение ИИ

- Сбор и систематизация информации
- Генерация и проверка скриптов и кода
- Составление фишинговых писем
- Автоматизированное тестирование на проникновение
- Применение дипфейков в социальной инженерии

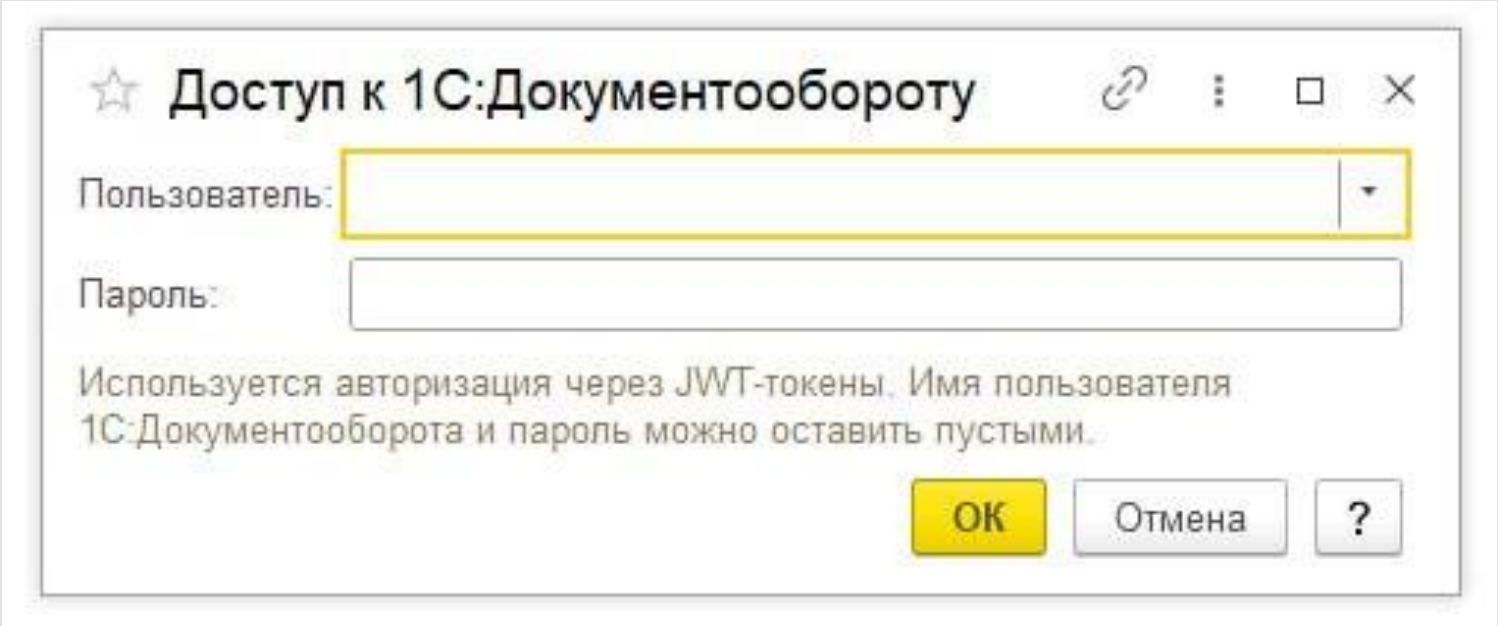
Ужесточение законодательства по ПДн
Проект изменений в КОАП и УК РФ

- оборотные штрафы за повторные утечки — от 1 до 3% годовой выручки за прошлый год
- размер оборотных штрафов — от **20 млн руб.** до 500 млн руб.
- штраф могут снизить, если нет отягчающих обстоятельств, а инвестиции компании в информационную безопасность на протяжении трёх лет составляли не менее 0,1% от выручки и компания соблюдала требования к защите данных
- **штрафы для должностных лиц** при утечках персональных данных составят **до 2 млн руб.**
- нарушение порядка обработки биометрии – штрафы до 2 млн рублей на организацию и до 1 млн рублей на должностных лиц
- за кражу и незаконное использование персональных данных вводится уголовная ответственность до 10 лет лишения свободы

Пароли и учетные записи

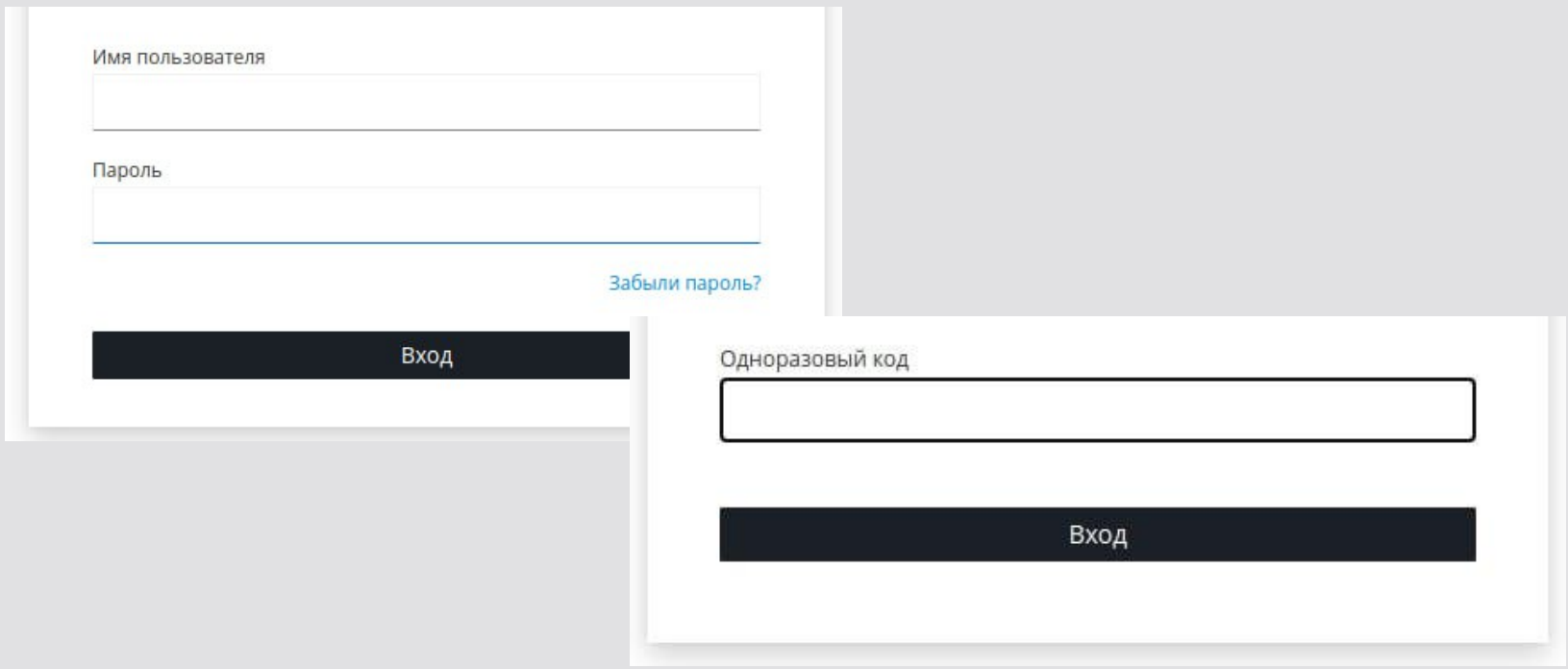
- Потребность в IDM (Identity Management) системе - централизованное управление учетными записями и правами пользователей
- Проверка паролей на наличие в утекших базах
- Многофакторная аутентификация в сочетании с единой точкой входа (single sign-on), дифференцированная в зависимости от сервиса и уровня доступа к нему
- Контроль действий привилегированных учетных записей

- Интеграция с 1С:Документооборот через JWT-токены



Практические применение

- Аутентификация в 1с посредством OpenID Connect
- SSO и двухфакторная аутентификация

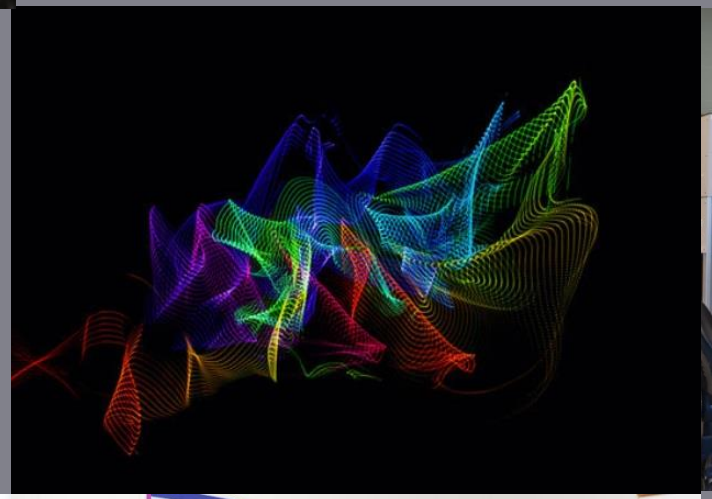


Рекомендации

- Непрерывное обучение пользователей и повышение осведомленности по вопросам ИБ
- Мониторинг событий информационное безопасности
- Инвентаризация информационных систем, сервисов и инфраструктуры
- Управление обновлениями и уязвимостями
- Управление учетными данными
- Сегментация сети
- Защита веб-приложений

пермский политех

Спасибо за внимание!



Юрий Горбунов,
заместитель начальника
Управления цифровой трансформации
Департамент ЦТиСК
Контакты: +7 (342) 2-198-537,
yuri.gorbunov@pstu.ru