Обнаружение заимствований и информационная безопасность

Ивахненко Андрей Александрович,

к.ф.-м.н.,

компания Антиплагиат

Информационная безопасность системы Антиплагиат

Безопасность данных пользователей

- За 16 лет ни одной подтвержденной утечки данных
  - по каждому обращению производится расследование всех обстоятельств;

- Матрица рисков включает в себя десятки пунктов:
  - атака внешними силами;
  - атака сотрудником компании;
  - выход из строя оборудования;
  - авария в датацентрах;
  - пандемия;

  и т.д.

Безопасность данных пользователей

Действие

или

Бездействие

пользователя системы

Проверки быстро заканчиваются…

- Причины

  - кроме пользователей организации есть еще и пришлые «нахлебники»;

  - пользователи организации используют проверки в своих личных целях;

  - пользователи организации тратят проверки нерационально

Источник: https://www.yaplakal.com/forum7/topic1980229.html

Проверки быстро заканчиваются…

- Причины
  - кроме пользователей организации есть еще и пришлые «нахлебники»;
  - пользователи организации используют проверки в своих личных целях;
  - пользователи организации тратят проверки нерационально

- Опасности
  - внезапная необходимость пересмотра бюджета организации;
  - использование более дорогого тарифа, чем можно было бы

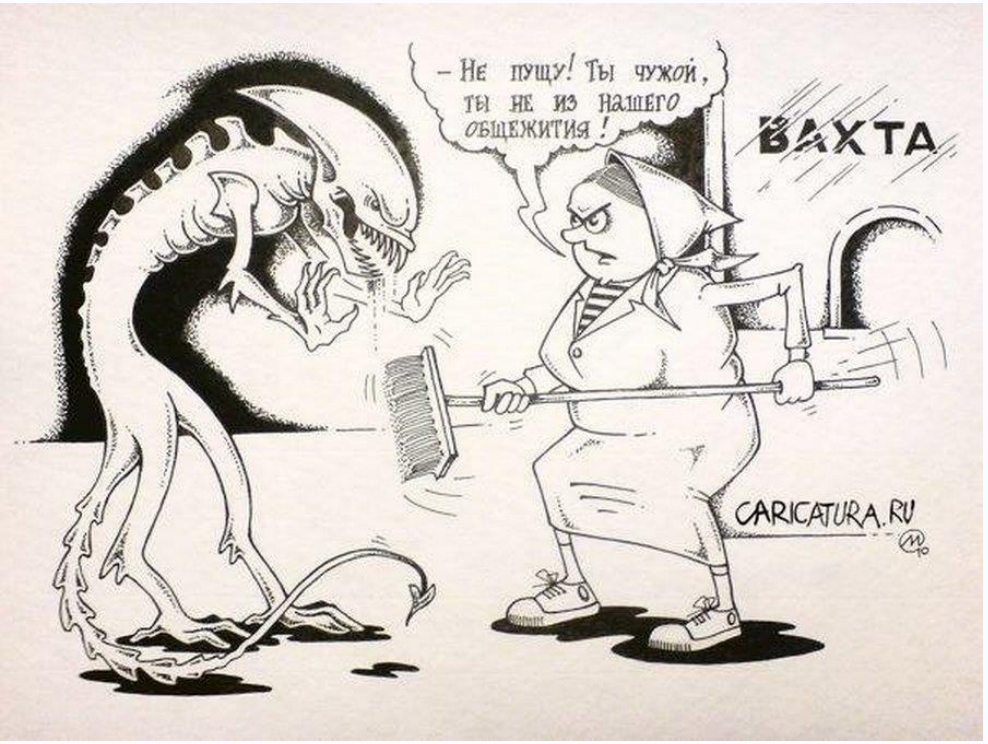
Источник: https://www.yaplakal.com/forum7/topic1980229.html

Проверки быстро заканчиваются…

- Причины
  - кроме пользователей организации есть еще и пришлые «нахлебники»;
  - пользователи организации используют проверки в своих личных целях;
  - пользователи организации тратят проверки нерационально
- Опасности
  - внезапная необходимость пересмотра бюджета организации;
  - использование более дорогого тарифа, чем можно было бы
- Последствия
  - перерасход средств в организации

Источник: https://www.yaplakal.com/forum7/topic1980229.html

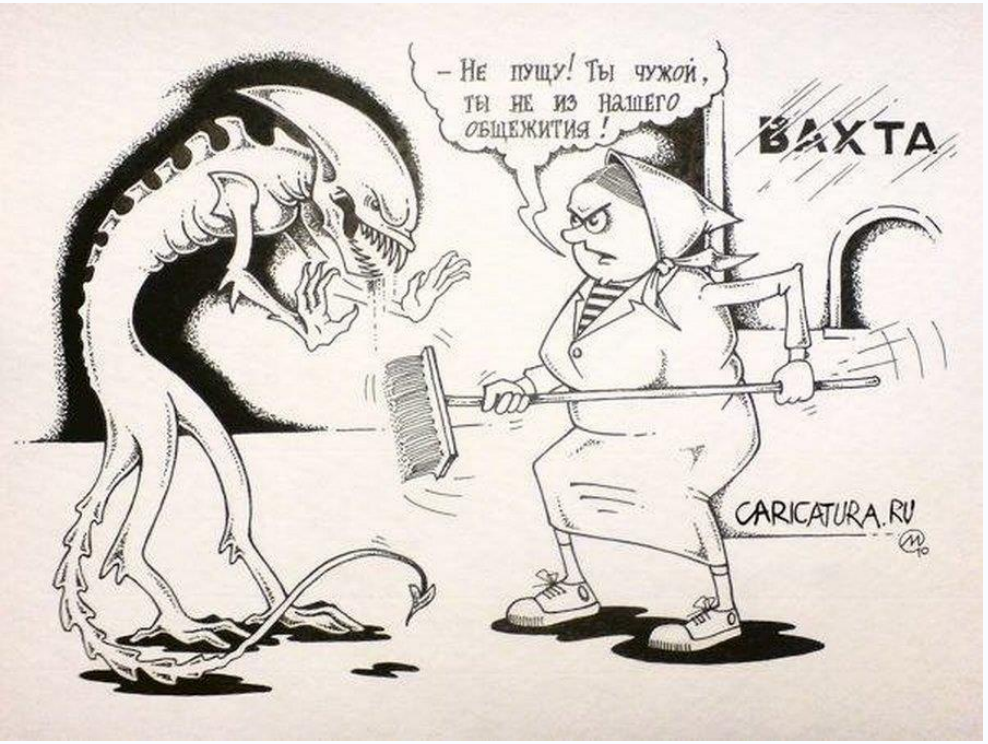
Чужие пользователи внутри организации...



Источник: https://ribalych.ru/2018/05/01/o-bednom-chuzhom-zamolvite-slovo/

- Причины
  - разглашение учетных данных пользователями системы
  - удалось обмануть процесс создания пользователя в организации

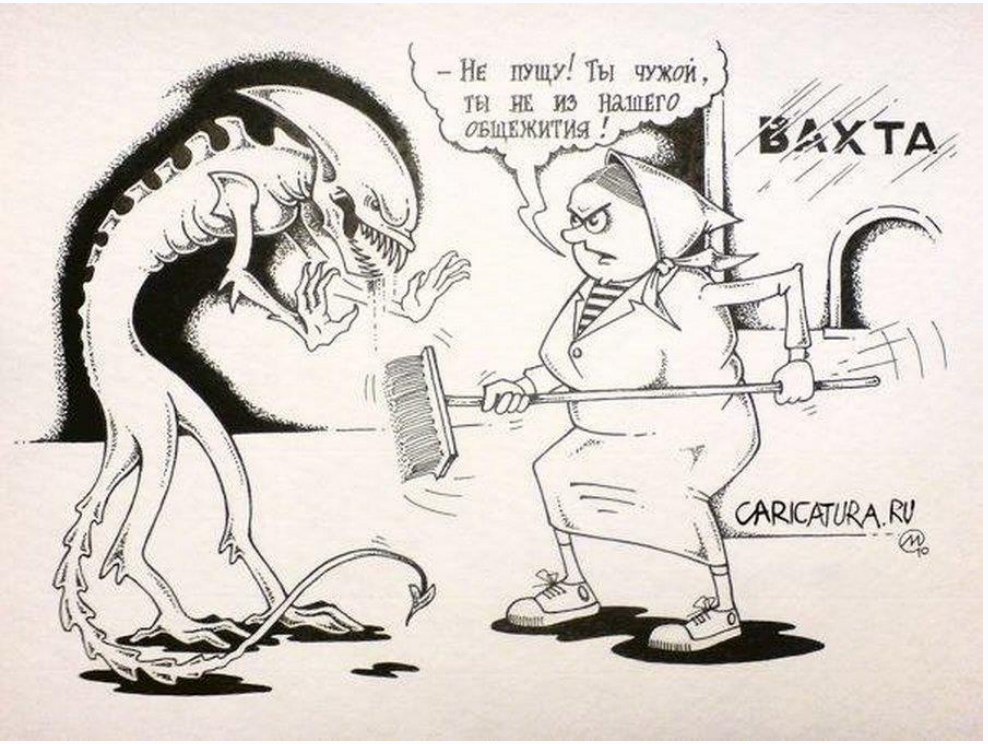
Чужие пользователи внутри организации...



Источник: https://ribalych.ru/2018/05/01/o-bednom-chuzhom-zamolvite-slovo/

- Причины
  - разглашение учетных данных пользователями системы
  - удалось обмануть процесс создания пользователя в организации
- Опасности
  - чрезмерное расходование проверок;
  - возможность утечки документов организации;
  - возможность утечки персональных данных пользователей

Чужие пользователи внутри организации...



Источник: https://ribalych.ru/2018/05/01/o-bednom-chuzhom-zamolvite-slovo/

- Причины
  - разглашение учетных данных пользователями системы
  - удалось обмануть процесс создания пользователя в организации
- Опасности
  - чрезмерное расходование проверок;
  - возможность утечки документов организации;
  - возможность утечки персональных данных пользователей
- Последствия
  - утечка интеллектуальной собственности организации
  - перерасход средств организации

Почему так происходит?

Низкая культура информационной безопасности пользователей

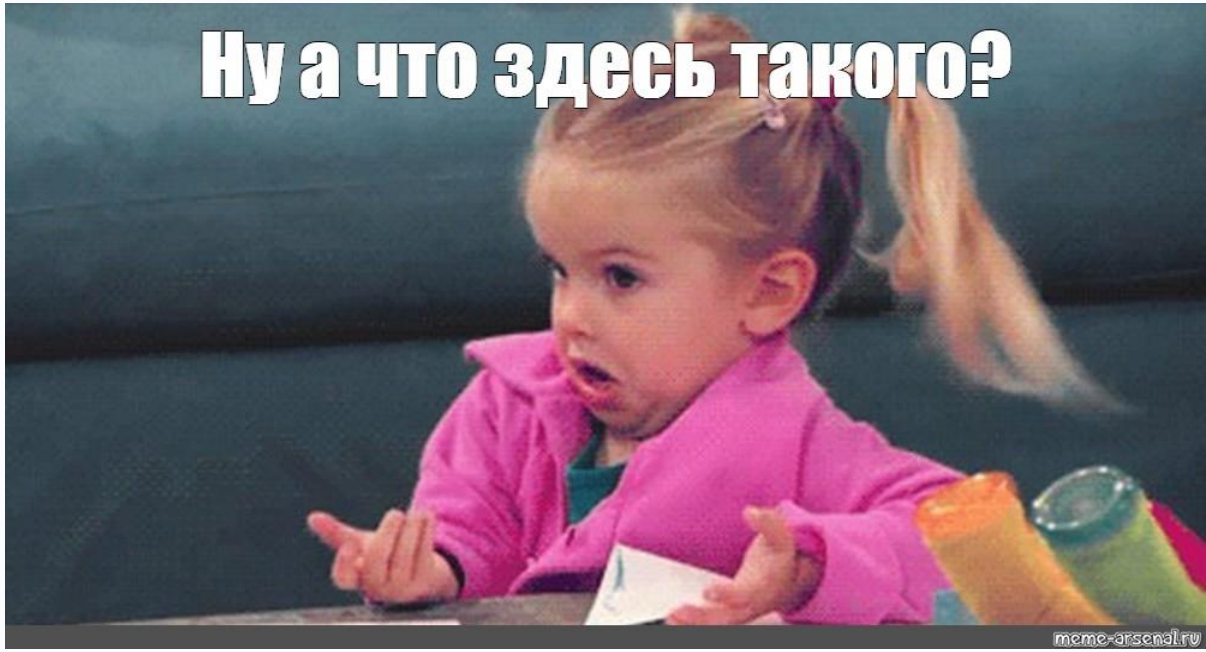
- Преподаватель раздает свои учетные данные студентам: «Проверьте сами»
- Корневой Администратор пересылает письмо со своими учетными данными всем запросившим доступ
- Учетные данные пишутся на стикере и крепятся на монитор

Источник: https://avatanplus.com/detail/resource-97387

Почему так происходит?

Неправильно организованные процессы

- Учетные данные вывешиваются в библиотеке или публикуются в соцсетях
- Используются многопользовательские учетные записи
- Выбывшие пользователи не блокируются
- Заявки на подключение новых пользователей выполняются по обычному электронному письму



Источник: https://www.meme-arsenal.com/create/meme/2651843

Почему так происходит?

Неправомерные действия пользователей

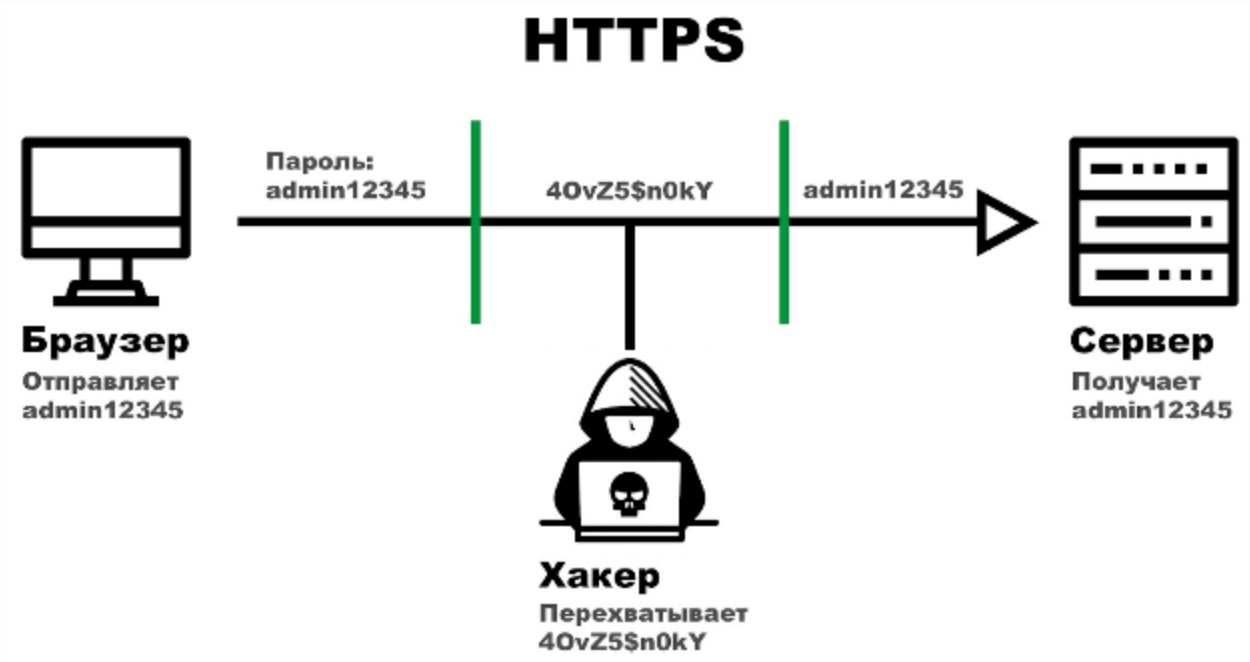
- Тюнингуют свои и чужие работы
- Экспериментируют с различными способами технического обхода системы
- Проверяют чужие работы на заказ
- Передают доступ к системе третьим лицам

Источник: https://antijob.net/class_war/id590

Безопасность данных

Какие меры предпринимает компания Антиплагиат?

- Взаимодействие с сервисом только по протоколу https
  - все данные зашифрованы при передаче между браузером и сервером



Источник: https://ssl.com.ua/blog/http-vs-https/

Безопасность данных

Какие меры предпринимает компания Антиплагиат?

- Пароли не хранятся на сервере Антиплагиата
  - обрабатываем пароли необратимой функцией (хешируем) и храним хеши;
  - восстановить пароль из хеша практически невозможно

- Администратор больше не может задавать пароли вручную
  - пароль задается самим пользователем при первом входе;
  - пароль знает только сам пользователь;
  - если учетной записью пользуется кто-то еще, это сделано с ведома или попустительства пользователя!

Безопасность данных

Какие меры предпринимает компания Антиплагиат?

- Автоматическая блокировка пользователей с подозрительной активностью
  - пользователь блокируется, если он нарушает правила добросовестной работы с системой;
  - алгоритмы машинного обучения на основе выявленных прецедентов подготовили модель (нейросеть), которая и принимает решение о блокировке;
  - вновь выявленные прецеденты нарушений добавляются в обучающую выборку, и модель регулярно обновляется

Безопасность данных

Какие меры предпринимает компания Антиплагиат?

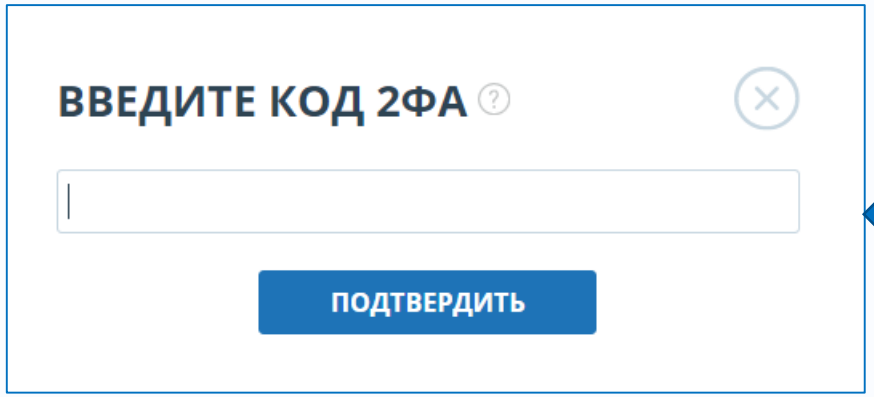
- Квоты на проверки
  - квота на проверку по умолчанию;
  - индивидуальная квота пользователя

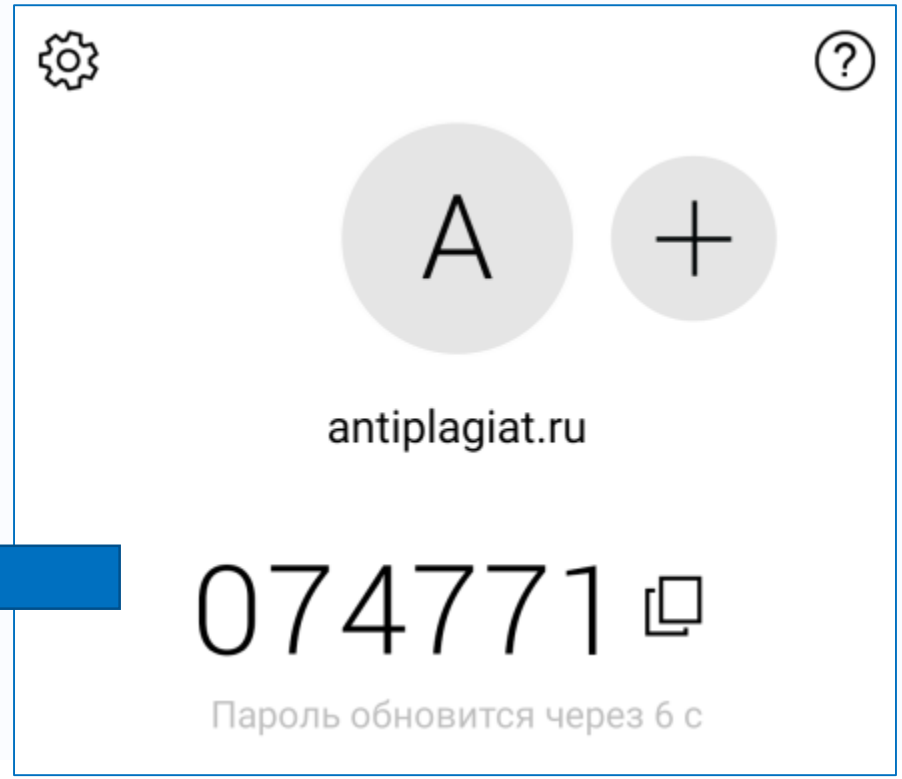
- Второй фактор аутентификации с помощью мобильного устройства
  - такая же процедура, как и при работе в интернет-банках: для совершения некоторых операций необходимо ввести дополнительный код, который генерирует ваш телефон;
  - даже зная ваш пароль, без вашего телефона нельзя получить учетную запись пользователя в вашей организации

Двухфакторная аутентификация для Администраторов

Что нужно подтверждать через второй фактор?

- Список действий, подтверждаемый 2ФА (не чаще раза в 15 минут)
  - создание/пакетное создание/изменение пользователя;
  - изменение пароля пользователю;
  - разблокировка/восстановление пользователя;
  - имперсонирование в пользователя





Безопасность данных в ваших руках

Что делать администратору?

- Один пользователь – одна учетная запись!
  - в системе нет ограничения на число пользователей;
  - работа нескольких пользователей через одну учетную запись – неправильный подход с точки зрения обеспечения информационной безопасности

- Регулярный аудит пользователей:
  - удаление/блокировка выбывших пользователей;
  - роль «Администратор» только у тех, кто должен управлять другими пользователями;
  - подключайте авторизацию через каталоги пользователей AD, ADFS, LDAP, Google Workplace, RUNNetAAI, FEDUrus

Безопасность данных в ваших руках

Что делать администратору?

- Устанавливайте квоты на проверку для пользователей:
  - квота по умолчанию – для всех пользователей;
  - расширенные, но не бесконечные квоты для особых случаев

- Подтверждение списка пользователей на создание:
  - организовать процесс так, чтобы заявки приходили через внутреннюю систему задач или систему документооборота;
  - использовать для управления имеющиеся каталоги пользователей организации (AD, LDAP и т.д.);
  - самостоятельно найти контакты ответственного лица подразделения и убедиться, что заявка действительно пришла из указанного подразделения

Безопасность данных в ваших руках

Что делать администратору?

- Анализ действий подозрительных пользователей:

  - анализ статистики, отчет «Интенсивность работы пользователей» для выявления подозрительных пользователей;

  - добавить себе роль «Супервизора», которая позволяет смотреть историю действий пользователей, адреса и время входов

- Утечка учетной записи без явных действий администратора - невозможна:

  - анализ статистики, отчет «Интенсивность работы пользователей» для выявления подозрительных пользователей;

  - добавить себе роль «Супервизора», которая позволяет смотреть историю действий пользователей, адреса и время входов

Безопасность данных в ваших руках

Что делать администратору?

- Разблокировка пользователей – ответственная задача!

  - изучите «Принципы добросовестной работы» с системой;

  - перед разблокированием пользователя проанализируйте его действия и загруженные им документы, убедитесь, что проверки были в рамках учебного процесса вашей организации;

  - убедитесь, что пользователь является сотрудником вашей организации и имеет право использовать систему;

  - проведите беседу с пользователем об основах информационной безопасности, убедитесь, что пользователь понимает недопустимость распространения личной учетной записи;

  - смените пароль для учетной записи и разблокируйте ее;

  - в случае повторного или вопиющего нарушения сообщите об обнаруженных фактах своему руководству.

Цели

Зачем все это?

- Снизить нагрузка на систему

  Проверки будут выполняться быстрее
- Снизить расходы организации на использование Антиплагиата

  Нам выгодно, чтобы организация закупала ровно столько проверок, сколько ей нужно
- Снизить количество случаев «тюнинга» работ

  Вырастет качество образования и научной деятельности
- Снизить число «утечек» акканутов

  Теперь действия третьих лиц в аккаунте возможны только с ведома владельца аккаунта

  При очередном продлении договора будет подключен 2ФА.

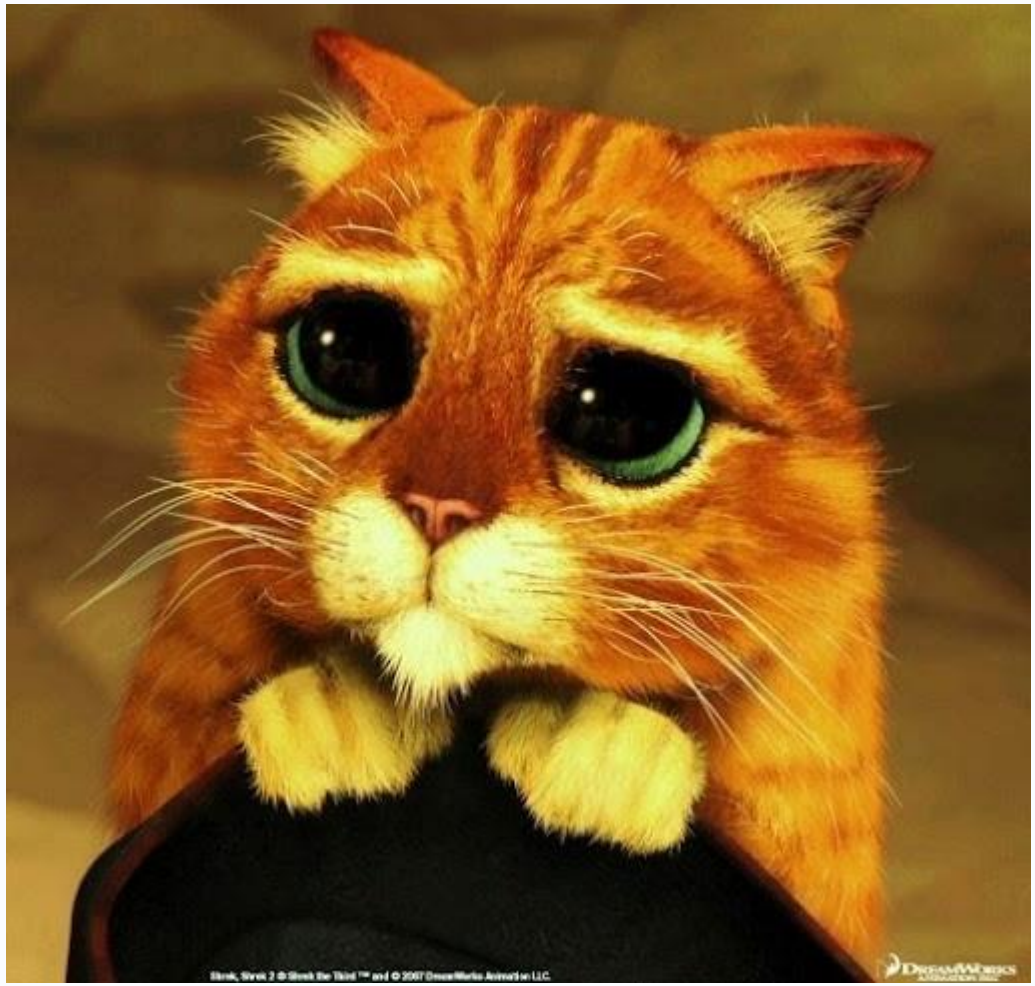
Памятка

Что делать администратору?

- Управляйте пользователями через каталоги пользователей: ADFS, RUNNetAAI, FEDUrus, Google Workspace (GSuite);
- Поддерживайте число «Администраторов» в системе на минимально необходимом уровне;
- Используйте двухфакторную аутентификацию для администраторов;
- Один пользователь – одна учетная запись;
- Установите квоту «по умолчанию», настройте квоты для «выдающихся» пользователей;
- Регулярно анализируйте действия подозрительных пользователей и тех, кто просит снять ограничение (роль «Супервизор» и отчеты о работе системы).

Нам нужна ваша помощь!

- Мы делаем все, что в наших силах для того чтобы ответственность за некорректное поведение пользователей была персональная
- Нужны изменения в регламентах работы организации, чтобы дисциплинарная ответственность наступала неотвратимо
- Обезопасим данные вместе!



Источник: https://www.meme-arsenal.com/memes/1772e2771492e7e1fc04a4ed973b8263.jpg

Бесплатный тестовый доступ

Тестовый доступ можно получить обратившись:

- по электронной почте: sales@antiplagiat.ru
- через форму: https://www.antiplagiat.ru/corporate/access/test
- по телефону: 8 800 777-81-28

Спасибо за внимание!

Ваши вопросы?

Андрей Ивахненко,
руководитель отдела внедрения и эксплуатации,
Компания Антиплагиат
E-mail: ivakhnenko@antiplagiat.ru