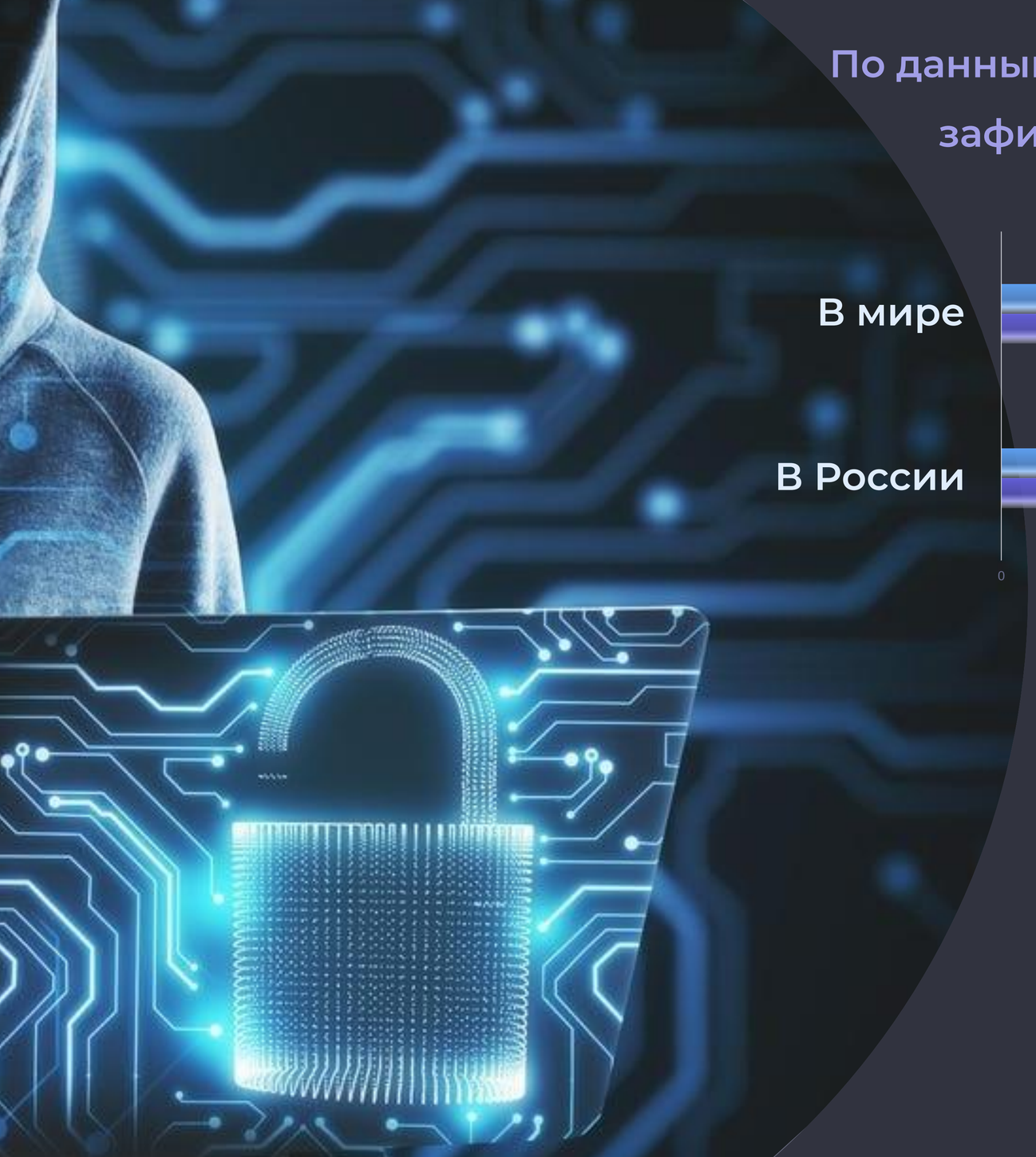
ШИФРОВАНИЕ КАК ПОСЛЕДНИЙ РУБЕЖ ЗАЩИТЫ ИНФОРМАЦИИ

Важность защиты данных

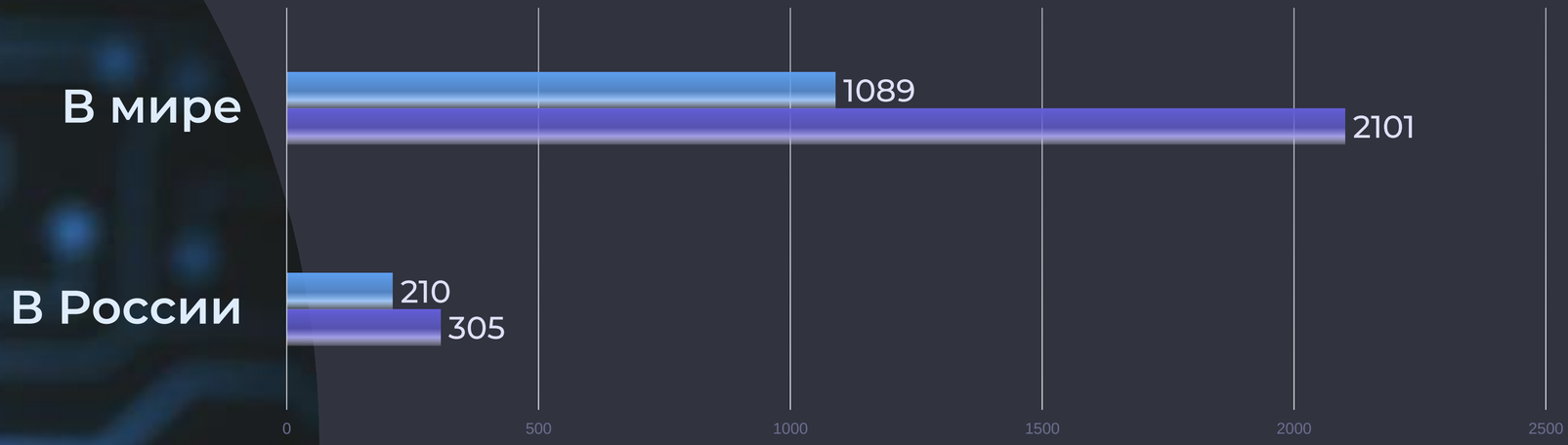
С развитием технического прогресса, растет количество и ОБЪЕМ ДАННЫХ, которые необходимо где-то хранить.

В последнее время ОБЛАЧНЫЕ ХРАНИЛИЩА все активнее применяются для хранения данных.

Одним из важных факторов в эру цифровизации является **БЕЗОПАСНОСТЬ ДАННЫХ**



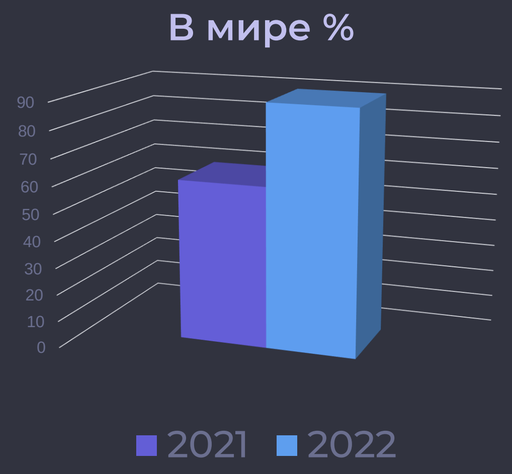
По данным экспертно-аналитического центра InfoWatch зафиксирован ЗНАЧИТЕЛЬНЫЙ РОСТ утечек в 2022

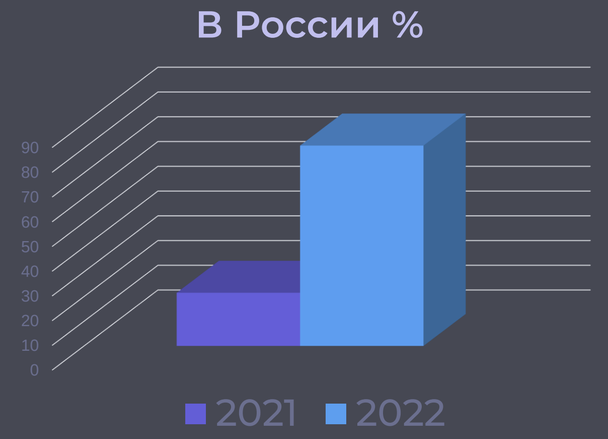


ТИПЫ УТЕЧЕК

Резко выросла доля утечек, спровоцированных действиями ВНЕШНИХ НАРУШИТЕЛЕЙ

- Ослабление контроля за информационными активами сотрудников в период пандемии Covid-19
- Резкий всплеск хакерской активности после 24 февраля 2022 года, а также повышение доступности инструментов для участия в кибератаках
- Увеличение доли скрытых внутренних нарушений





B.

компрометация аккаунта одного из сотрудников с последующим выходом в корпоративную сеть вследствие низкой цифровой грамотности сотрудников

A.

взлом серверов, где хранятся данные клиентов, вследствие хакерской атаки

D.

сотрудник компании с доступом к личной информации может вывести ее на внешний носитель и передать в третьи руки

E.

недобросовестные сотрудники, сливающие информацию

Как НЕЙТРАЛИЗОВАТЬ эти механизмы?

Необходим сервис, который сможет защищать информацию в автоматическом режиме, устраняя человеческий фактор

При этом, конфиденциальные данные должны работать исключительно в рамках организации, и даже в случае взлома – ей было бы невозможно пользоваться

Как в нынешних реалиях сохранить КОНФИДЕНЦИАЛЬНОСТЬ данных даже в СЛУЧАЕ УТЕЧКИ?

Защита последнего рубежа

С целью защиты конфиденциальных данных на базе компании Аппаратуры Систем Связи, было разработано такое решение

На данный момент оно представляет собой бета-версию backend-приложения

Данный сервис не отменяет необходимость внедрения иных средств защиты, но при этом защищает данные, если существующие средства защиты не могут обеспечить их надлежащую защиту.

Функциональность разработанного программного обеспечения

Защита данных

не только при хранении, но и при передаче данных с одного устройства на другое

Новая система авторизации

исключает возможные сценарии захвата

Кроссплатформенность

легко интегрируется в любую корпоративную инфраструктуру

Автоматический режим работы

минимизирует человеческий фактор в работе с данными

Способ авторизации

Если использовать логин пользователя, то теряется анонимность решения, как следствие – снижается защищенность данного решения

Если заменить логин каким-нибудь абстрактным идентификатором, то суть остается та же

Решение - метод с плавающим идентификатором **FloatId**

решается проблема однозначного установления пользователя через сканирование пакетов

решается проблема однозначного установления пользователя backend-приложением.

КЛЮЧИ ШИФРОВАНИЯ И КАК ИХ ЗАЩИТИТЬ

В случае компрометации аккаунта сотрудника злоумышленник ничего не получит – потому что у него отсутствует первый ключ шифрования

В случае взлома сервера и получении файлов злоумышленник также ничего не может сделать с данными – по причине отсутствия первого ключа шифрования

При разработке прототипа сервиса использовались алгоритмы симметричного блочного шифрования и хеширования

Дополнительные слагаемые КОНФИДЕНЦИАЛЬНОСТИ

Пароль пользователя хранится в виде хеша в базе данных

пароль применяется только в одном случае – если был просрочен JWT токен

JWT токен также применяется при авторизации

токен годен ограниченное количество времени – после, генерируется новый токен случайным образом

Данные хранятся на сервере

есть возможность полного отключения возможности выгрузки файлов

Метаданные хранятся в базе данных

Большую часть работы с файлами пользователь проводит с метаданными

Команды пользователя

1. Получение списка файлов
2. Добавление, удаление, переименование, перемещение файлов
3. Изменение разрешений файлов
4. Получение содержимого файла
5. Запрос floatId

ДОПОЛНИТЕЛЬНАЯ ФУНКЦИОНАЛЬНОСТЬ разработанного программного обеспечения, настраиваемая в процессе ИНТЕГРАЦИИ

01

возможность формирования групп пользователей с различными уровнями допуска

02

формирование журнала активности пользователей

03

авторизация вне backend-приложения

04

разработка клиентского приложения согласно ТЗ заказчика

Количество утечек информации стремительно растет с каждым годом

Защитите данные таким образом, чтобы даже в случае их утечки – никто не смог с ними ничего сделать и главное – не смог получить их содержимое

Контакты

Игорь Лава
руководитель проектов
E-mail:
LavaIV@escltd.ru

Телефон: +7 (962) 222-99-77

Спасибо за внимание!