GIS ГАЗИНФОРМ СЕРВИС

Защита информации от несанкционированного доступа в информационных системах от внутренних нарушителей

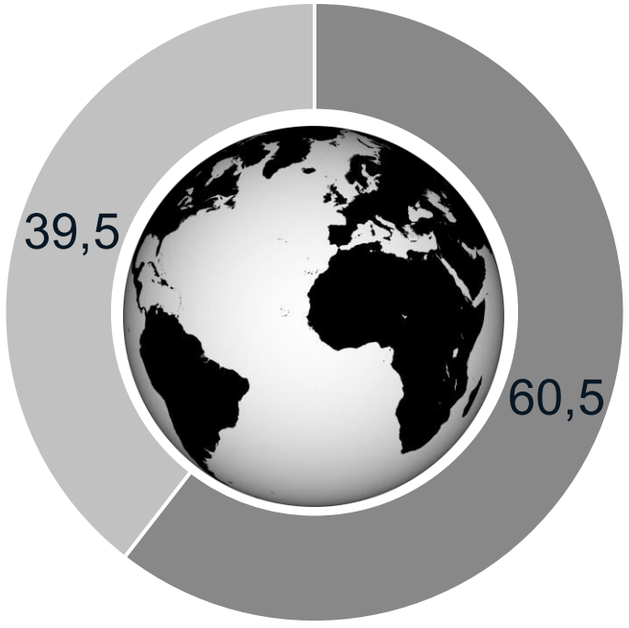
+7 (812) 677-20-53
sales@gaz-is.ru

13 февраля 2019 года
ТБ Форум, г. Москва

www.gaz-is.ru

Источники утечки информации

Мир



■ Внутренние ■ Внешние

Россия

■ Внутренние ■ Внешние

INFOWATCH

Глобальное исследование утечек конфиденциальной информации в 2017 году

Утечки и попытки кражи информации

31% ОРГАНИЗАЦИЙ НЕ СТАЛКИВАЛИСЬ С ПОДОБНЫМИ ИНЦИДЕНТАМИ

3% ОПРОШЕННЫХ НЕ ВЛАДЕЮТ ДАННЫМИ ОБ УТЕЧКАХ

ИБ-инциденты происходили

54% Случайно

46% Намеренно

38%

столкнулись с утечкой конфиденциальной информации

28%

из них смогли пресечь попытки кражи

SEARCHINFORM
INFORMATION SECURITY

Исследование утечек конфиденциальной информации в 2017 году

Типы данных, подвергающиеся утечке

Данные о клиентах и сделках
21%

Техническая информация
20%

Коммерческая тайна
17%

Информация о партнерах
11%

Персональные данные
9%

Внутренняя бухгалтерия
7%

Руководящие документы ФСТЭК России, регламентирующие требования безопасности к сертифицируемым СЗИ

- **Требования к операционным системам**

утверждены приказом ФСТЭК России от 19 августа 2016 г. №119

- **Требования к средствам доверенной загрузки**

утверждены приказом ФСТЭК России от 27 сентября 2013 г. №119

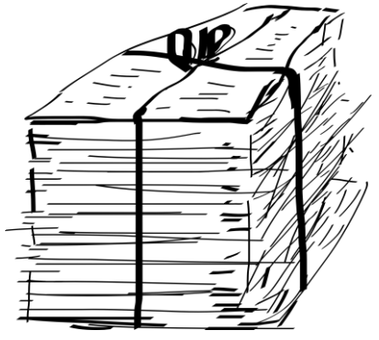
- **Требования к средствам контроля съемных машинных носителей информации**

утверждены приказом ФСТЭК России от 28 июля 2014 г. №87

- **Требования к средствам антивирусной защиты**

утверждены приказом ФСТЭК России от 20 марта 2012 г. №28

- **Требования к межсетевым экранам**



утверждены приказом ФСТЭК России от 09 февраля 2016 года №9

- **Требования к системам обнаружения вторжений**

утверждены приказом ФСТЭК России от 06 декабря 2011 г. №638

Угрозы безопасности до загрузки ОС

- Загрузка не целевой ОС или ОС с неразрешенными модификациями;
- Загрузка целевой ОС нарушителем;
- Нарушение целостности аппаратной части компьютера;
- Угроза нарушения целостности UEFI прошивки.

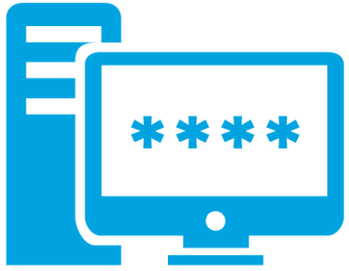
Основные функции безопасности средства доверенной загрузки

- Идентификация и аутентификация пользователей с использованием персональных идентификаторов и уникальных PIN-кодов к ним;
- Блокировка загрузки пользователями нештатных копий ОС с различных устройств ввода информации (DVD-ROM, HDD, USB) и с помощью внешних органов управления;
- Обеспечение защищенности паролей пользователей и PIN-кодов при выполнении операций их ввода-вывода;
- Контроль целостности: файлов, завершенности журналов транзакций файловых систем, объектов реестра для ОС семейства Microsoft Windows, параметров среды UEFI, загрузочных секторов устройств хранения данных, аппаратного обеспечения в процессе загрузки ОС.

Требования к функциям безопасности ОС согласно методическому документу «Профиль защиты ОС»

- Идентификация и аутентификация;
- Управление доступом;
- Регистрация событий безопасности;
- Ограничение программной среды;
- Изоляция процессов;
- Защита памяти;
- Контроль целостности;
- Обеспечение надежного функционирования;
- Фильтрация сетевого потока.

Среди основных угроз



Кража пароля

Неправомерный доступ

Неправомерный вывод информации

Запуск запрещенных процессов

Восстановление остаточной информации

Изменение ПО и реестра

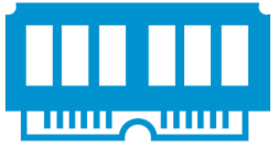
Основные защитные механизмы СЗИ от НСД

Двухфакторная аутентификация

Контроль вывод информации на носители

Межсетевой экран

Мандатный и дискреционный доступ



Очистка оперативной памяти

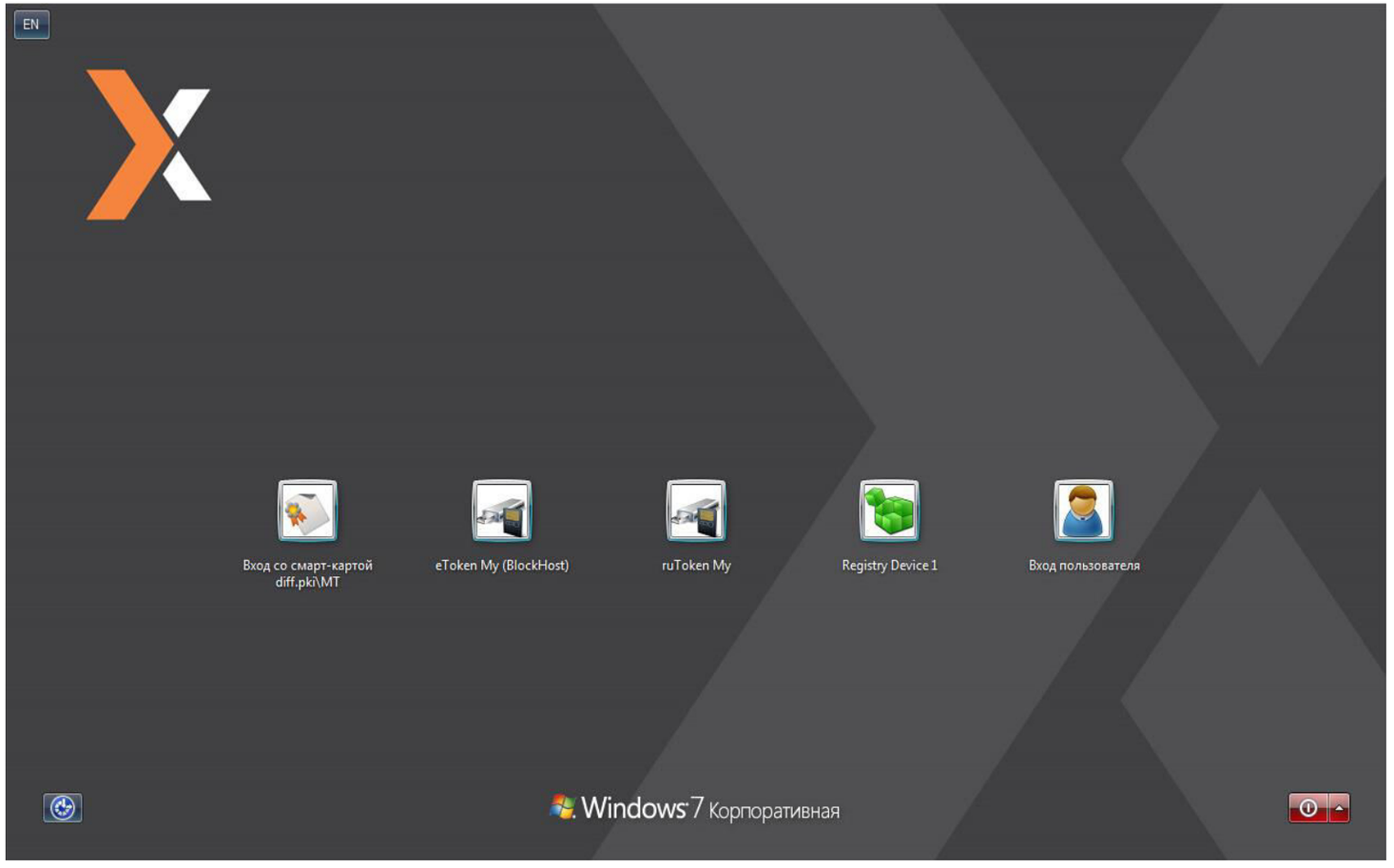
Контроль процессов, замкнутая среда

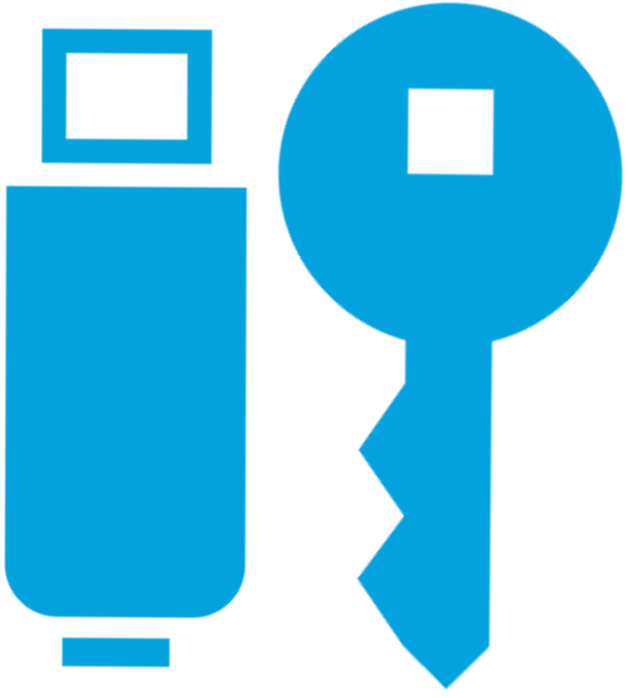
Контроль целостности

Гарантированное удаление

Самозащита СЗИ от НСД

Двухфакторная аутентификация

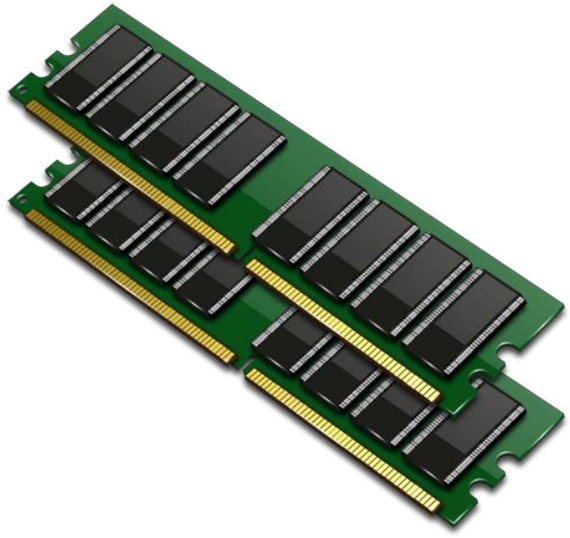




Гарантированное удаление

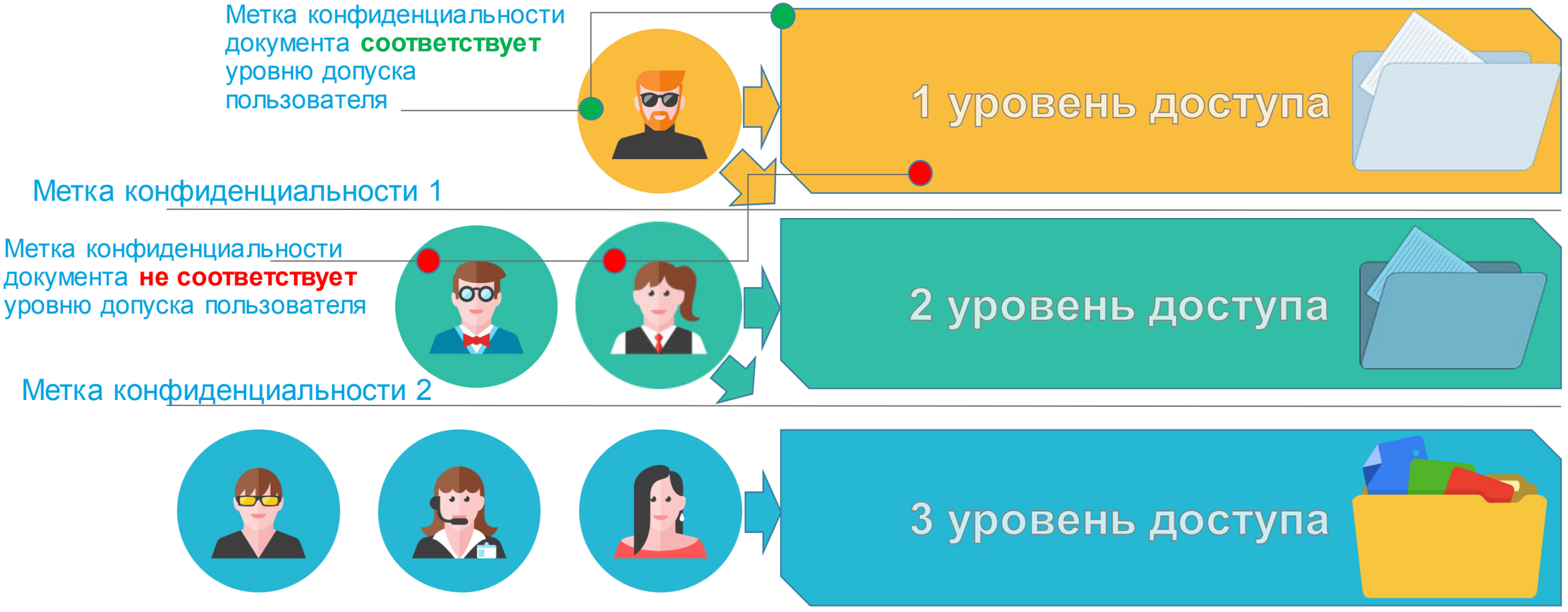
На место удаляемой информации записываются маскирующие данные в соответствии с ГОСТ Р 50739-95

Гарантированная очистка памяти

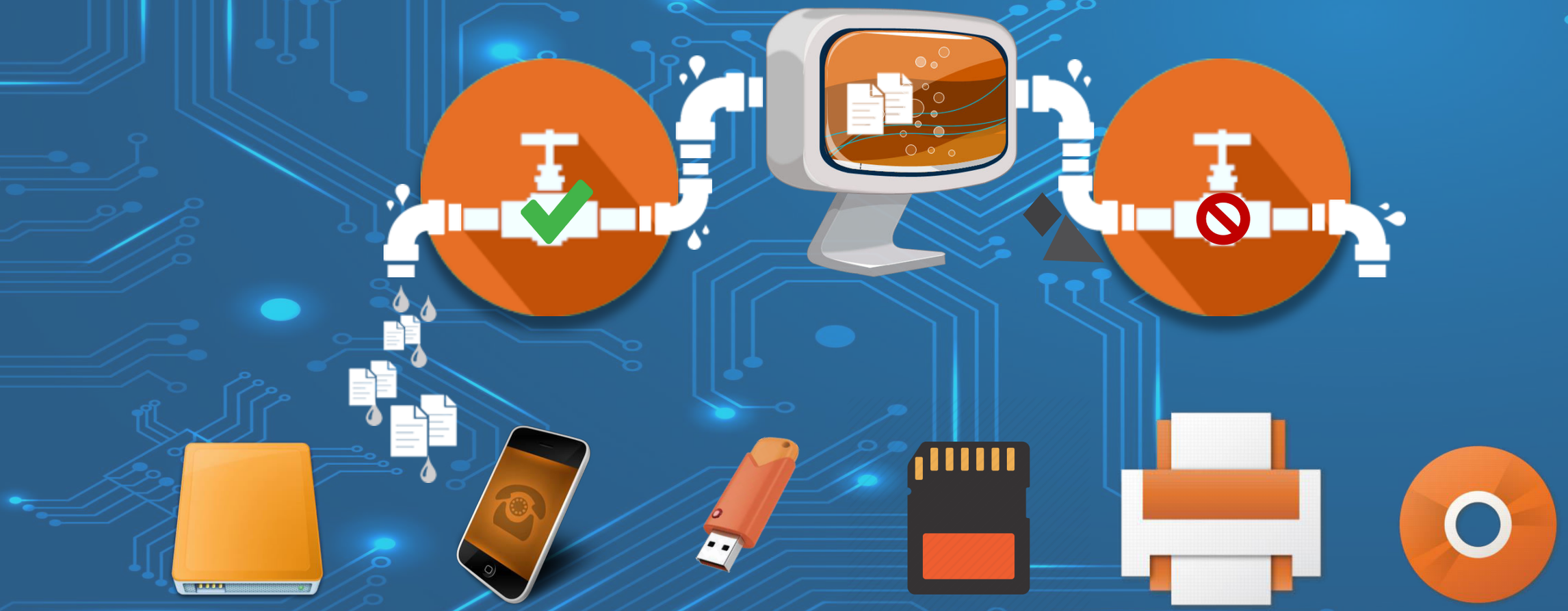


На место высвобождаемой памяти записывается маскирующая информация

Разграничение прав доступа

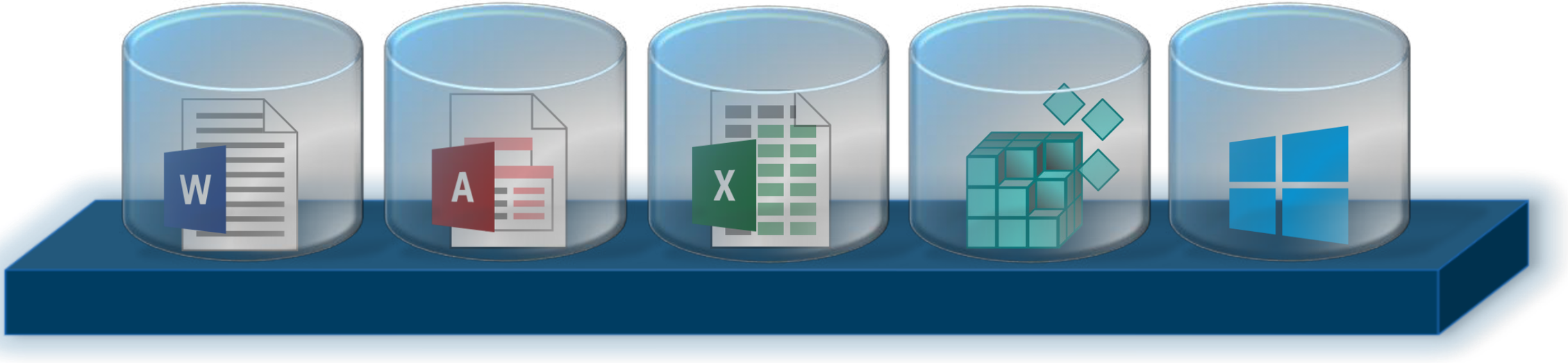


Контроль вывода информации на различные носители



Замкнутая программная среда

Контроль целостности



Проверка контрольной суммы файлов и их восстановление в случае изменения

Возможность украсть создает вора

Фрэнсис Бэкон (1564-1626)

GIS ГАЗИНФОРМ СЕРВИС

Спасибо за внимание!

+7 (812) 677-20-53

Hitrovo-K@gaz-is.ru

Константин Хитрово