КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Как противодействовать сетевым атакам в новых реалиях

26.05.2022

Знакомство

Обо мне

- В 2012 году окончил Балтийский федеральный университет им. И. Канта по специальности: «Организация и технология защиты информации»
- С 2012 года работал в государственных учреждениях на различных должностях, отвечал за обеспечение информационной безопасности
- С 2013 года осуществляю преподавательскую и научную деятельность в сфере защиты информации, член государственной аттестационной комиссии.
- Руководитель и Владелец компании, занимающейся информационной безопасностью.

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

.01

Основные проблемы

в обеспечении информационной

безопасности организации

.02

Особенности соответствия

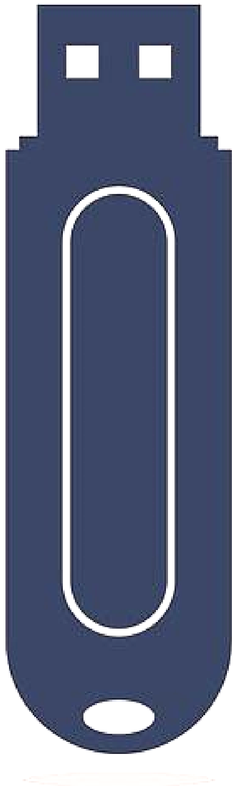
требованиям по защите информации (187-

ФЗ КИИ, 152-ФЗ ПДн, Приказ ФСТЭК № 17,

ГИС и т.д.)

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Бесконтрольное использование съемных носителей в организации.



.01

Утеря

съемных носителей, содержащих конфиденциальную информацию.

.02

Копирование

конфиденциальной информации преднамеренно

.03

Заражение

Вредоносным ПО.

.04

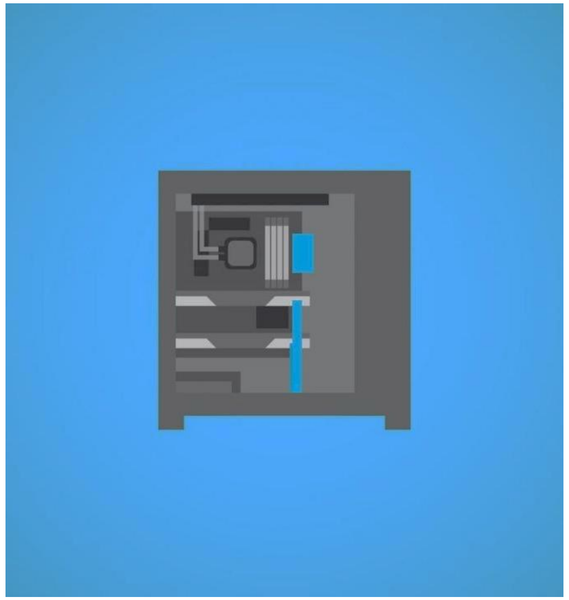
Выход в Интернет

в обход установленных правил.

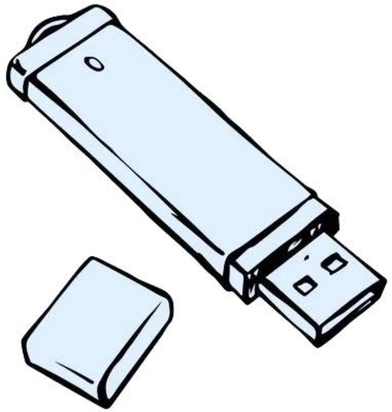
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бесконтрольное использование съемных носителей в организации.

Решения.



Использование «Буферного компьютера».



Использование только служебных съёмных носителей.

Применение DLP систем

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Решения

Незащищённый удаленный доступ в информационную систему организации

- Использование VPN соединений.
- Двухфакторная аутентификация (одноразовый пароль, устройство).

Простое

1

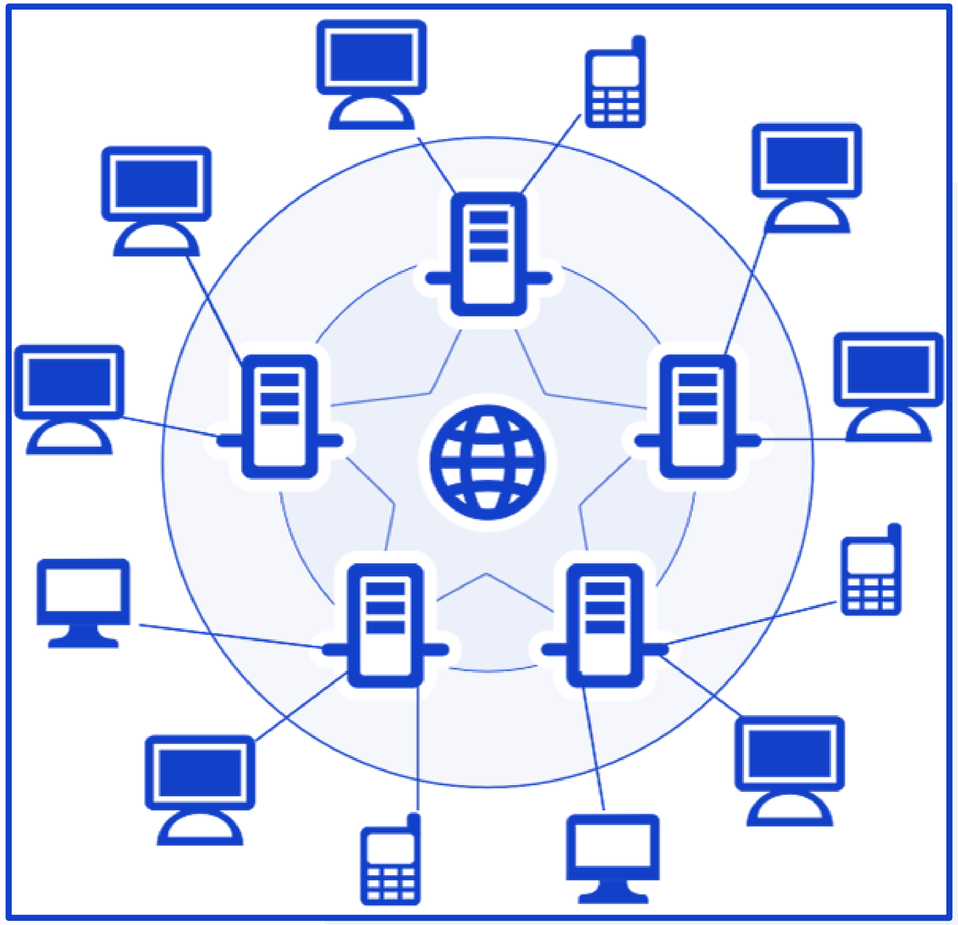
- Виртуальные машины на личном компьютере пользователя.
- Корпоративные ноутбуки.

Профессиональное

(включает первые два пункта), а также

2

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Решения

Отсутствие разграничения доступа к общим сетевым ресурсам.

.01

Назначение

минимальных прав (пользователю доступны только те файлы, с которыми он работает)

.02

Использование

меток конфиденциальности и соответствующих им уровней (степеней) допуска

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Неконтролируемый доступ в Интернет в организациях, где есть филиальная структура.

Отсутствуют документы, регламентирующие порядок защиты информации.

Доступ во внешние сети не ограничен.

Действия пользователей в информационной системе не регистрируются.

Каналы доступа в интернет не резервируются.

Доступ в админскую часть, корпоративный аккаунт без двухфакторной аутентификации.

Использование личных почт на рабочем месте.

Установка ПО, не связанного с исполнением своих должностных обязанностей.

Пользователи работают под учетными записями с правами администраторов.

Отсутствуют средства антивирусной зашиты.

Перед утилизацией техники гарантированное уничтожение информации не осуществляется.

Слабая парольная политика.

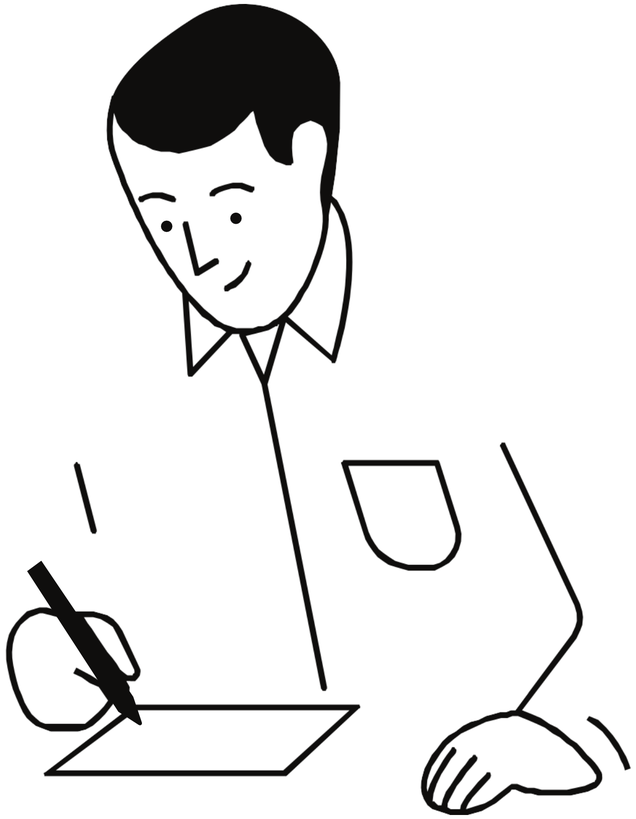
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Не используются двухфакторная аутентификация учетных записей с правами администратора.

Учетные записи не привязаны к конкретному пользователю (сложно идентифицировать пользователя).

Подключение СВТ в корпоративную сеть не ограничено.

Готов ответить на ваши вопросы



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ