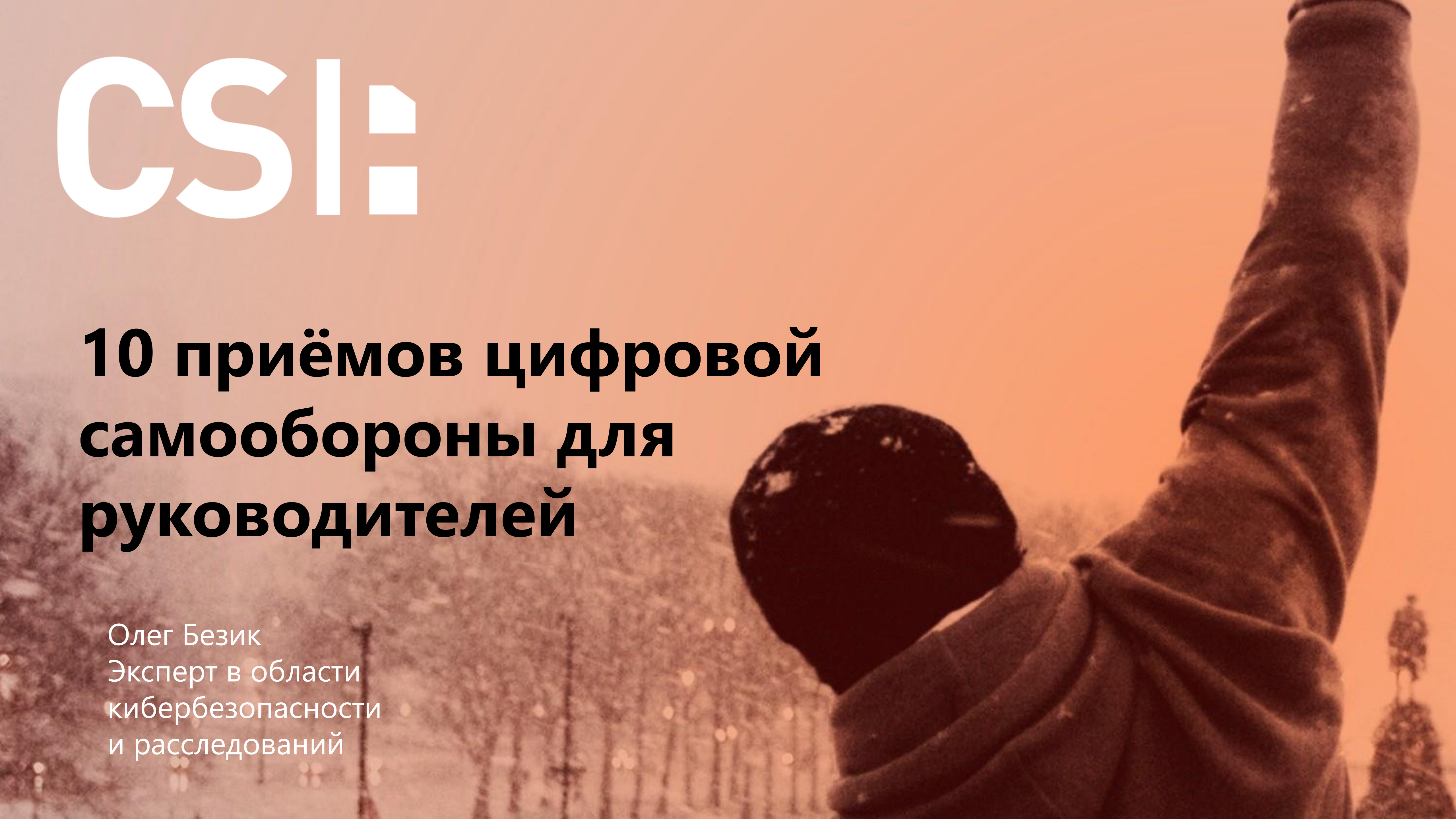




CSI:

10 приёмов цифровой самообороны для руководителей

Олег Безик
Эксперт в области
кибербезопасности
и расследований



Давайте знакомиться

Олег Безик

Руководжу проведением компьютерных исследований в рамках внутренних корпоративных расследований и судебных споров

- Certified ISACA CISM
- Associated ISACA member
- Access Data Certified Examiner
- Certified Ringtail User





Два слова о CSI Group

CSI Group была основана в 2013 году группой профессионалов в области внутренних корпоративных расследований, и объединила профессионалов в области права, финансов, бухгалтерского аудита, компьютерной криминалистики и информационной безопасности

Что мы делаем?

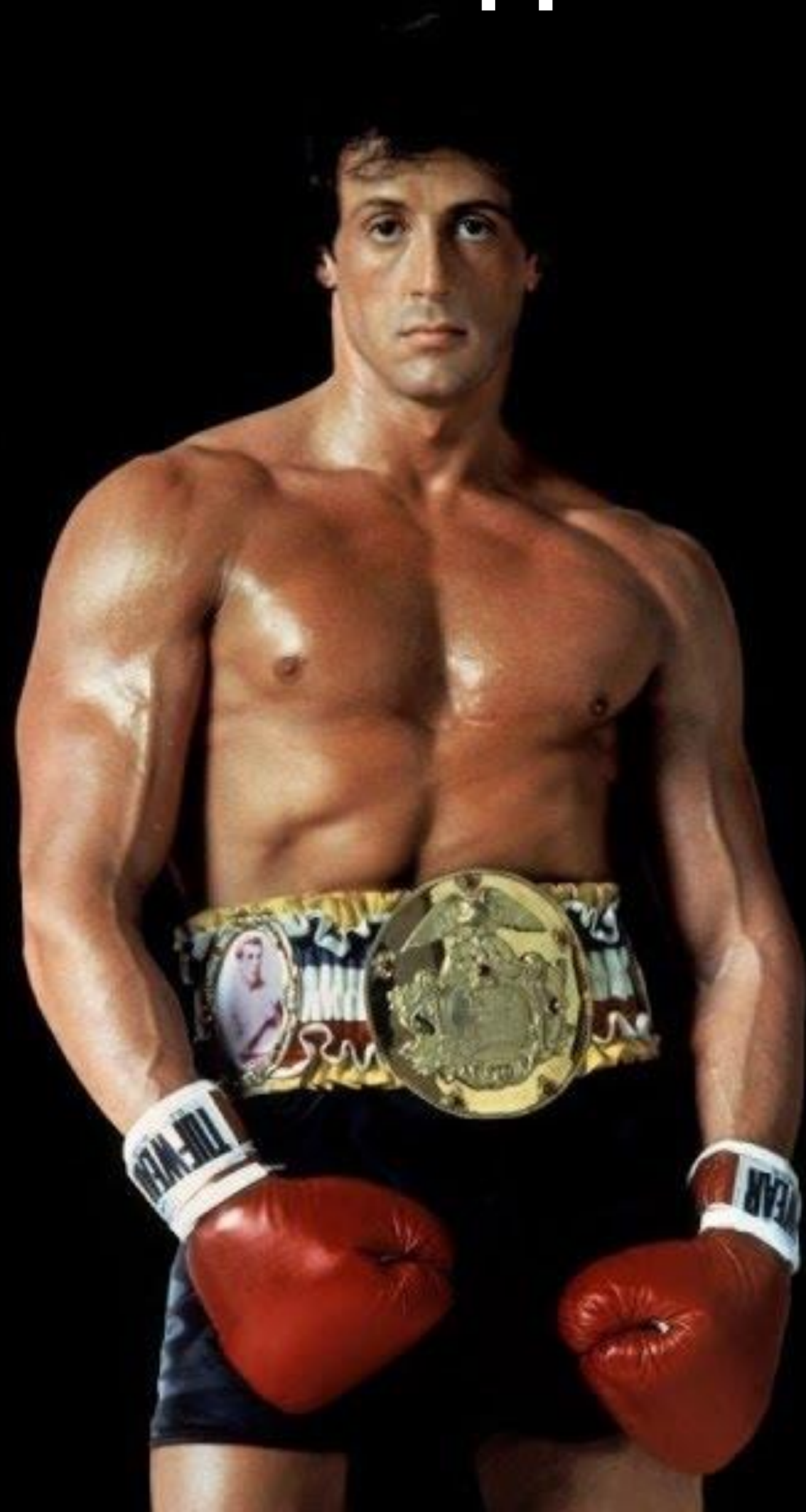
- Компьютерно-криминалистические исследования
- Судебная компьютерно-техническая экспертиза
- eDiscovery проекты
- Проведение внутренних аудитов
- Корпоративная разведка
- Географическая и микроэкономическая аналитика
- Отслеживание активов
- Управление корпоративными рисками
- Поддержка в суде
- Профайлинг

Подробнее: www.csi.group

РУКОВОДИТЕЛЬ

+

- принимает решения
- имеет авторитет
- чемпион по жизни
- пример для подражания
- силен духом



-

- принимает решения
- имеет доступ к ЭЦП
- часто бывает в командировках
- общается с большим количеством людей

CSI:

1. Освойте защитную стойку: Разработайте свой парольный рецепт

Золотое правило:

Для каждого сервиса используйте уникальные **ХОРОШИЕ** пароли!

ХОРОШИЙ пароль должен быть таким:

- Сложным: буквы, цифры, символы;
- Никак не ассоциироваться с Вами: ФИО, дата рождения, родной город, кличка собаки и т.д.;
- Не относится к ПЛОХИМ ПАРОЛЯМ!!!

123456
password
123456789
12345678
12345
111111
1234567
sunshine
qwerty
iloveyou

**ПЛОХИЕ
ПАРОЛИ!!!**



Privet kak dela?

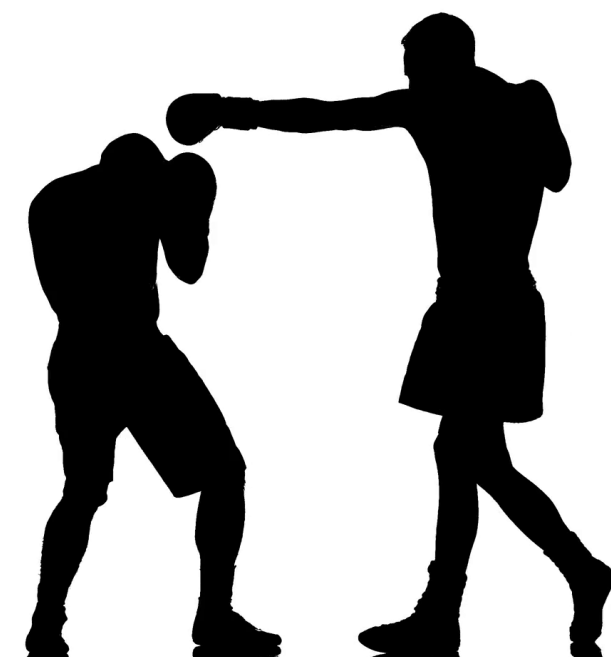
72Pr1vEt_K@k-DEla?=)



2. Научитесь работать корпусом: Грамотно управляйте паролями

Соблюдайте простые правила:

- Стикер, приклеенный на монитор – это не место для паролей!
- Офисная тумбочка – не место для паролей!
- Не пересылайте пароли в почте или мессенджерах.
- Не позволяйте кому-то видеть, какой пароль Вы вводите.
- **Храните пароли в менеджерах паролей: 1Password, iCloud Keychain, LastPass, Dashlane**



16:35

Отменить

Новый логин

Сохранить

СЕЙФ PERSONAL

Aebrus

Имя пользователя

oleg.bezik@csi-group.org

Пароль

Пароль

пароль

[Создать новый пароль](#)

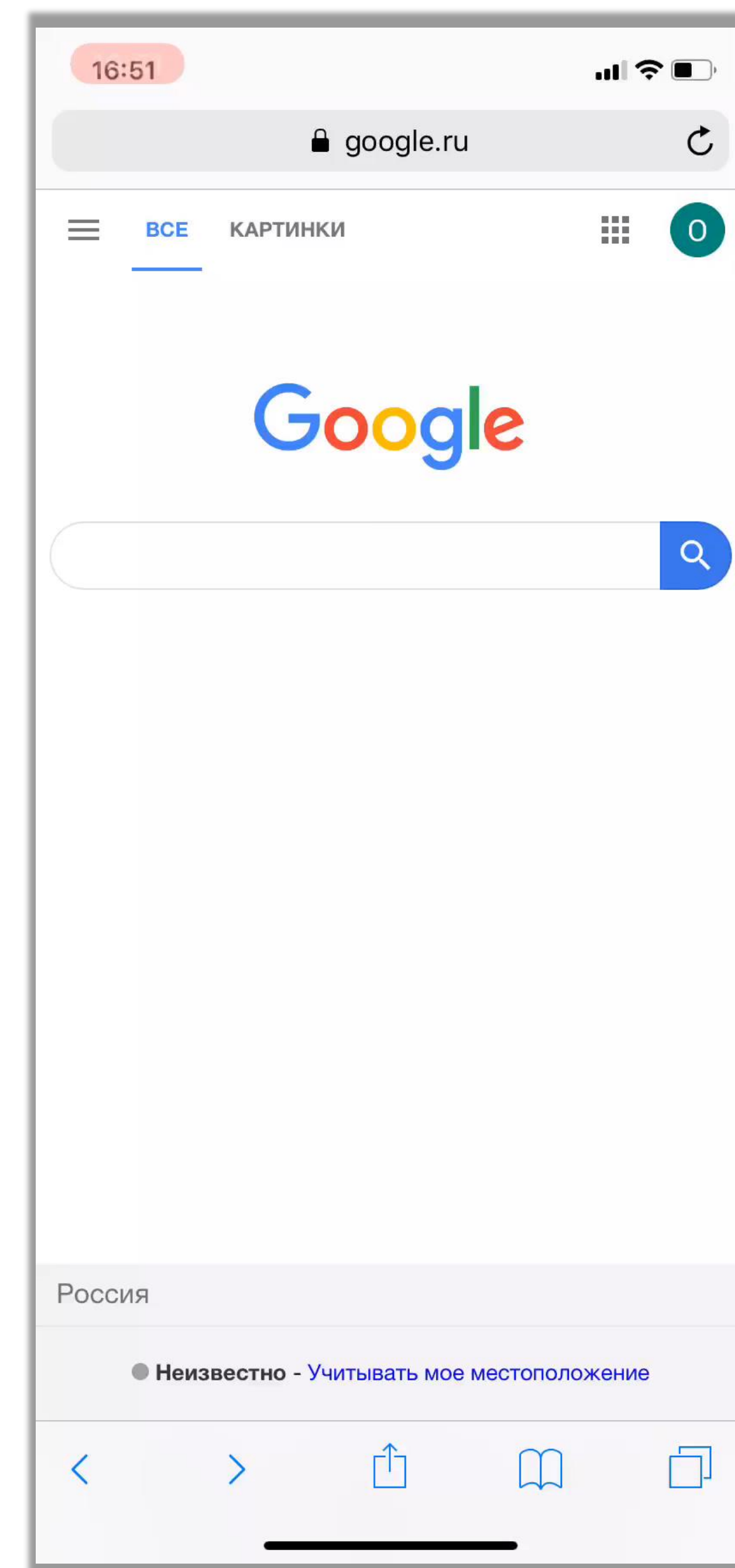


3. Используйте защиту уходом: Освойте двухфакторную аутентификацию

Двухфакторная аутентификация – это дополнительная защита, когда для входа в аккаунт кроме пароля нужно ввести ещё один короткий пароль, который приходит на почту или телефон.

Включите второй фактор везде:

- банк-клиенты;
- почта и облачные хранилища: Google, Yandex, Mail.Ru, Yahoo, и т.д.;
- социальные сети: Facebook, LinkedIn, Instagram, Twitter, ВКонтакте;
- другие сайты и сервисы.



CSI:

4. Научитесь защищаться уклоном: Работайте с ЭЦП безопасно

Электронно-цифровая подпись (ЭЦП) – аналог обычной подписи в цифровом мире. Позволяет подтвердить подлинность цифрового документа/файла.



Советы по безопасной работе с токенами ЭЦП:

- Используйте **ХОРОШИЙ** пароль.
- Извлекайте ЭЦП после завершения операций.
- Храните ЭЦП в защищенном месте (сейф – идеально!).
- По возможности **не передавайте ЭЦП другим сотрудникам.**
- Если всё таки необходимо передать ЭЦП другому сотруднику, сперва убедитесь, что сотрудник понимает, как безопасно работать с ЭЦП.

CSI:

5. Защита отбивом: Зашифруйте себя полностью

- Шифруйте свои устройства: рабочий и личный компьютер, смартфон, носители.
- Шифруйте свои файлы: почтовые архивы, мессенджеры, бэкапы.
- Используйте шифрованные носители для хранения конфиденциальных данных.

WINDOWS



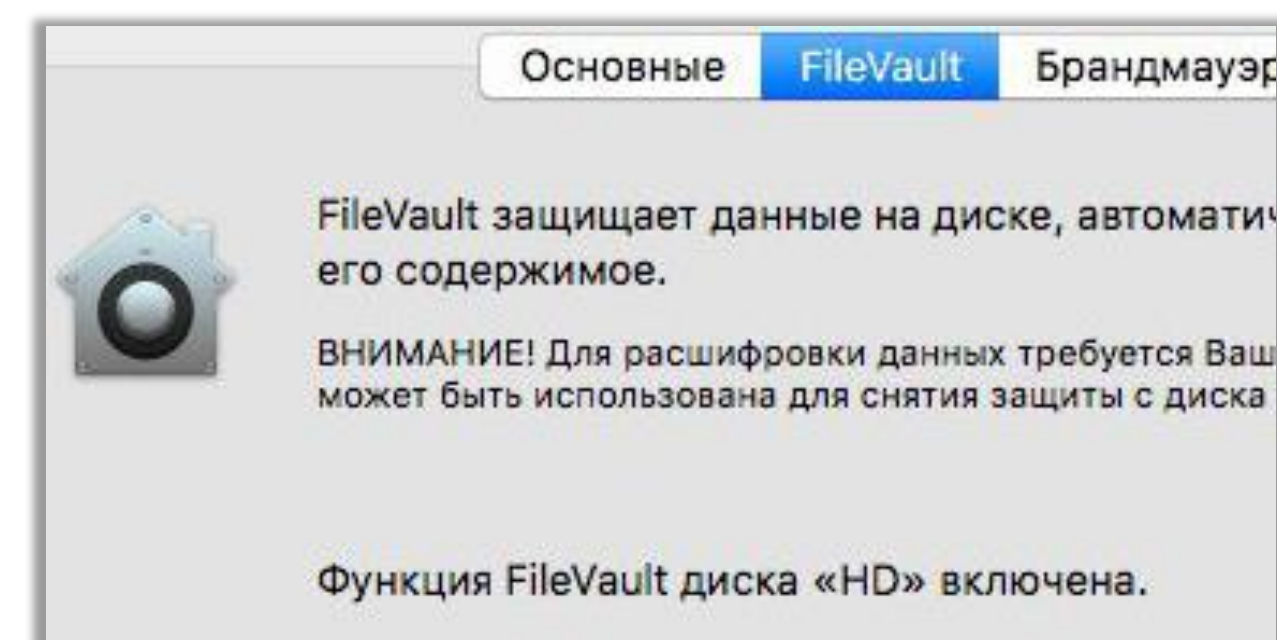
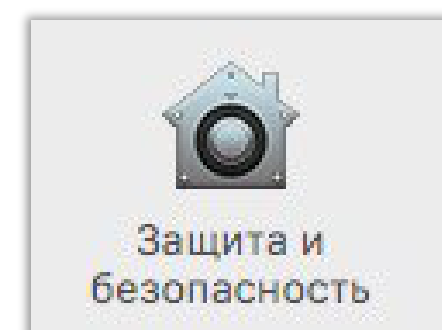
Operating system drive

C: BitLocker on



- Suspend protection
- Back up your recovery key
- Change password
- Remove password
- Turn off BitLocker

Mac OS



CSI:

6. Защита подставкой: Всегда обновляйте программы

- Обновления для программ часто устраняют известные уязвимости.
- Устанавливайте все появляющиеся обновления для всех программ: Windows, MacOS, iOS, Android, Mozilla Firefox, Google Chrome и т.д.



Обновление безопасности

Установите это обновление как можно раньше.

Security Update 2017-001 is recommended for all users and improves the security of macOS.

For more information on the security content of this update see <http://support.apple.com/kb/HT201222>.

7. Тренируйте реакцию:

Будьте внимательны к подозрительным письмам

А) Обращайте внимание на различные нестандартные ситуации:

- письмо попало в спам;
- вас просят перевести деньги;
- вас просят перейти по ссылке;
- вас просят скачать какой-либо файл.

Б) Обращайте внимание на адрес почтового ящика отправителя:

- вместо somebody@**yandex.ru** указано somebody@**yandeks.ru**;
- имя пользователя и доменное могут быть полностью подделано.

Фишинг:

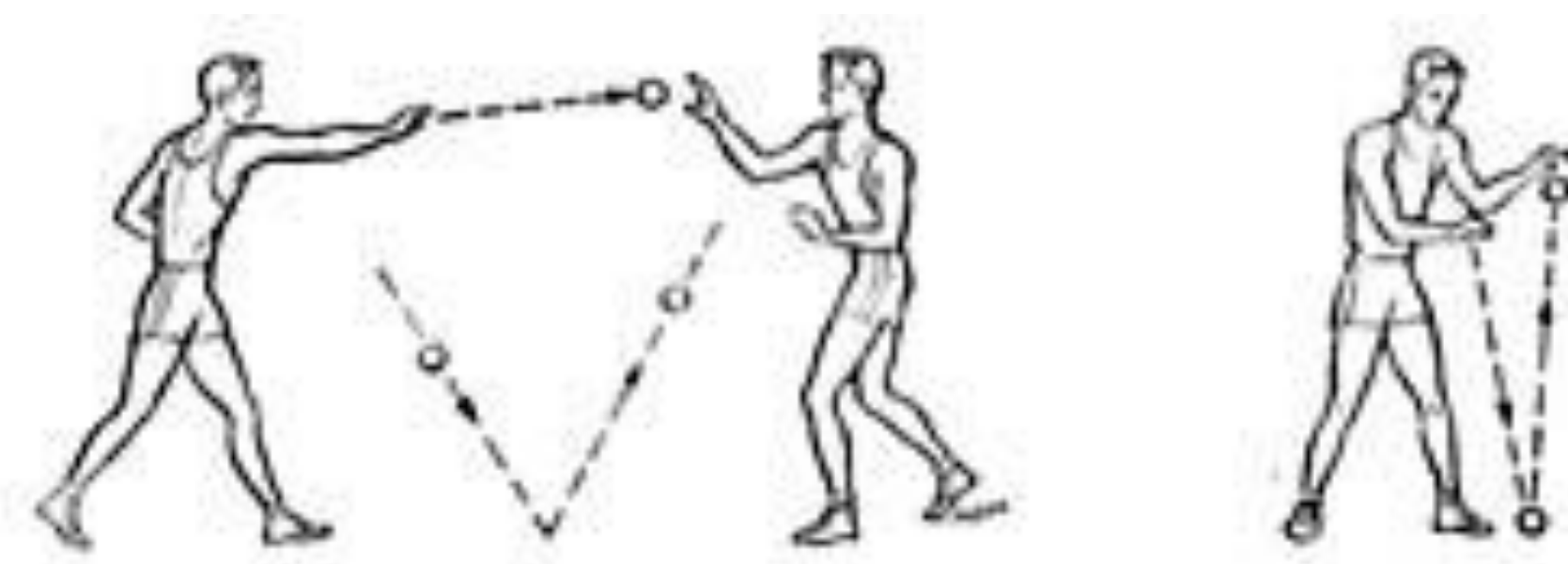
вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям

Е-mail-спуфинг:

подмена адреса e-mail отправителя

В) Обращайте внимание на манеру речи в письме:

- Есть речевые обороты, которые никогда бы не использовал ваш собеседник;
- используется «нестандартная» подпись;
- присутствуют нехарактерные грамматические и пунктуационные ошибки.



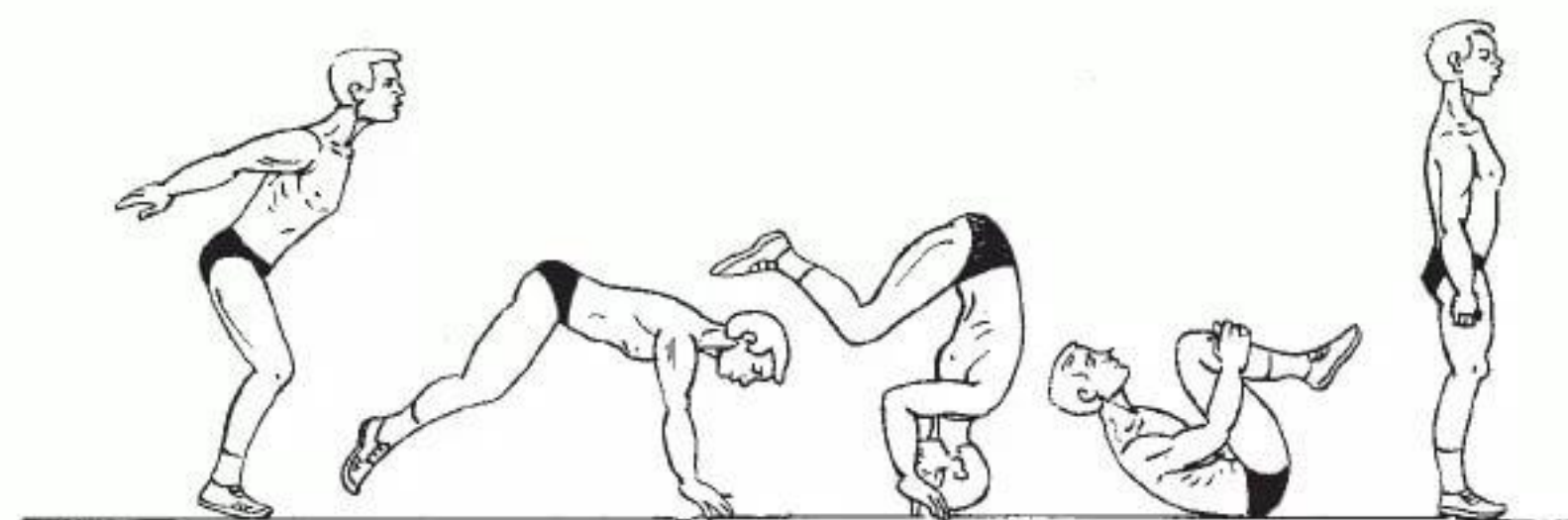


8. Тренируйте ловкость:

Правильно используйте устройства для личных и рабочих целей

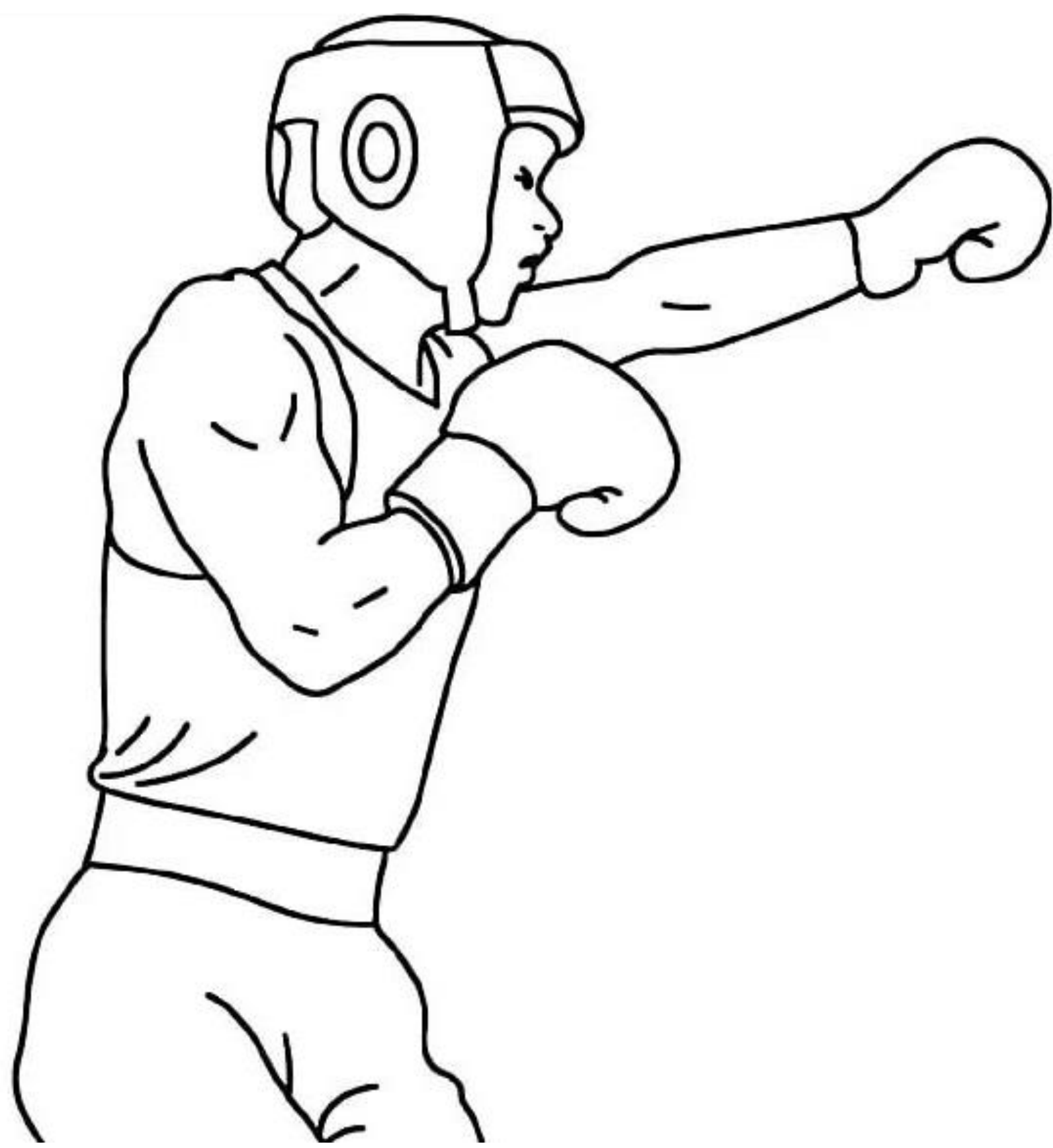
Правила просты, но эффективны:

- Не храните ваши личные файлы на корпоративных устройствах: фото, видео, персональные данные;
- Не входите на рабочем компьютере в свой личный банк-клиент, социальные сети или личную почту;
- Не сохраняйте в браузерах на рабочем компьютере пароли для автоматического входа в систему;
- Не осуществляйте через корпоративный компьютер покупки в Интернете с вводом данных личной банковской карты.



CSI:

9. Постоянно тренируйтесь: Повышайте свою кибер-грамотность



Оставайтесь в курсе всех новинок в сфере IT и ИБ:

- 1) Читайте блоги по информационным технологиям и ИБ;
- 2) Посещайте тематические конференции;
- 3) Перед приобретением новой версии гаджета убедитесь в том, что он надежно защищен;
- 3) Узнавайте мнение экспертов по сложным вопросам ИБ.

CSI:

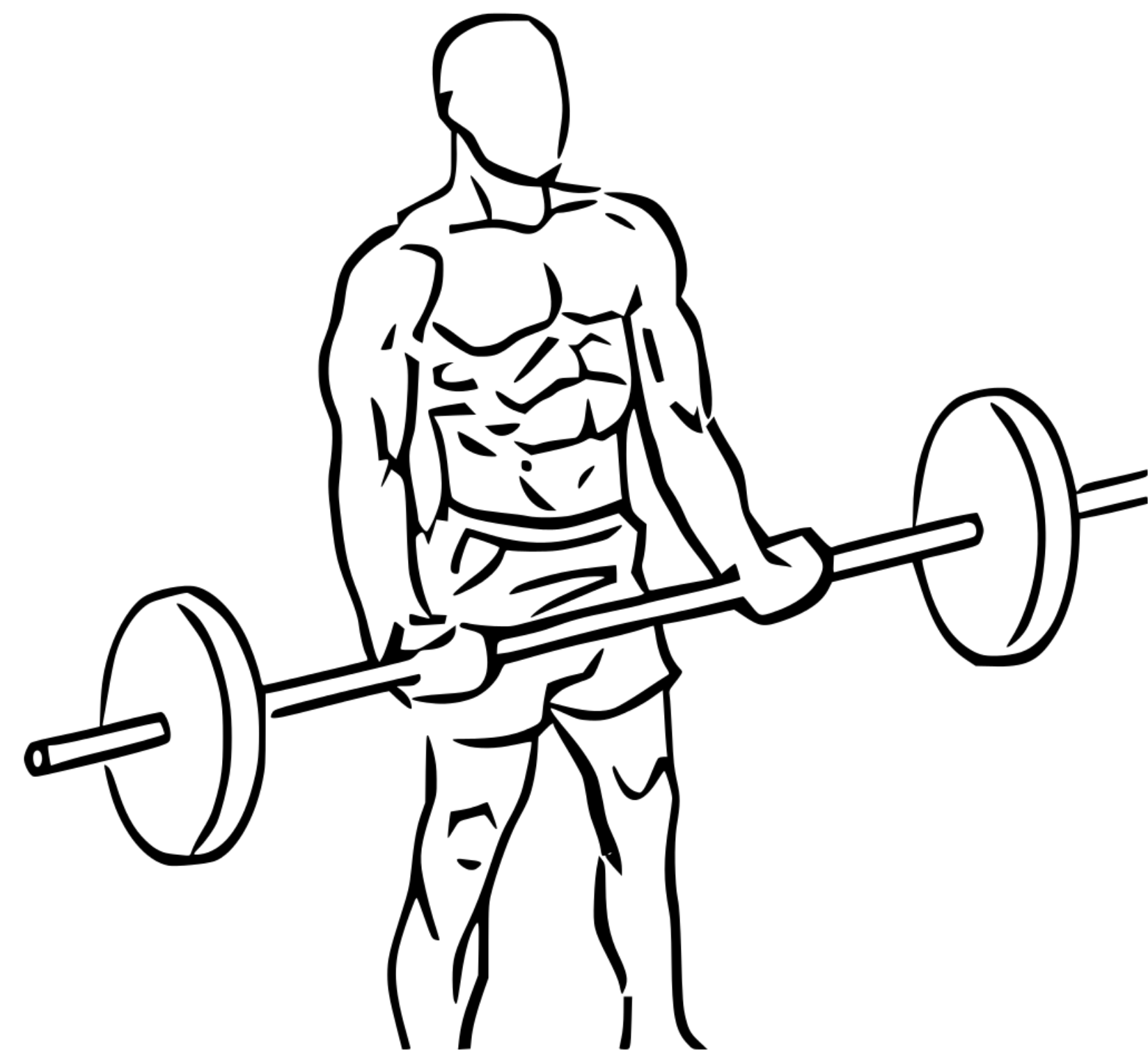
10. Наращивайте мышцы:

Повышайте кибер-грамотность и осведомленность ваших коллег

Организируйте в компании/отделе обучение по основам информационной безопасности и кибер-грамотности.

Используйте комплексный подход:

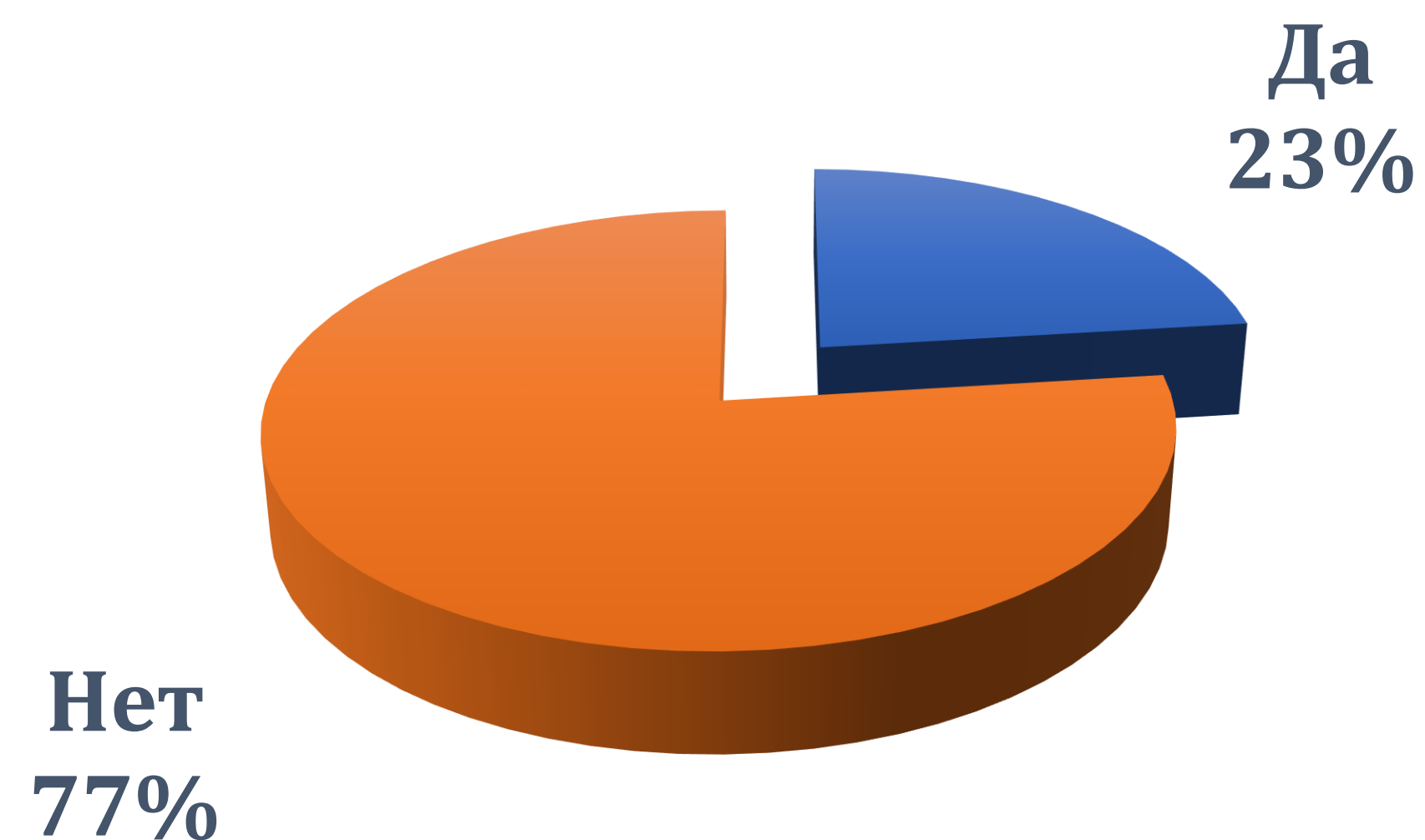
- ✓ Очные тренинги и семинары;
- ✓ Видеоролики;
- ✓ Вебинары;
- ✓ Тестирования и игры;
- ✓ Учения: имитация атаки, учебные фишинговые рассылки и др.;
- ✓ Брошюры и карточки;
- ✓ Мотивирующие плакаты и стикеры с напоминаниями.





Немного занимательной статистики: пароли*

Дефолтные пароли



Пароли записаны на стикере



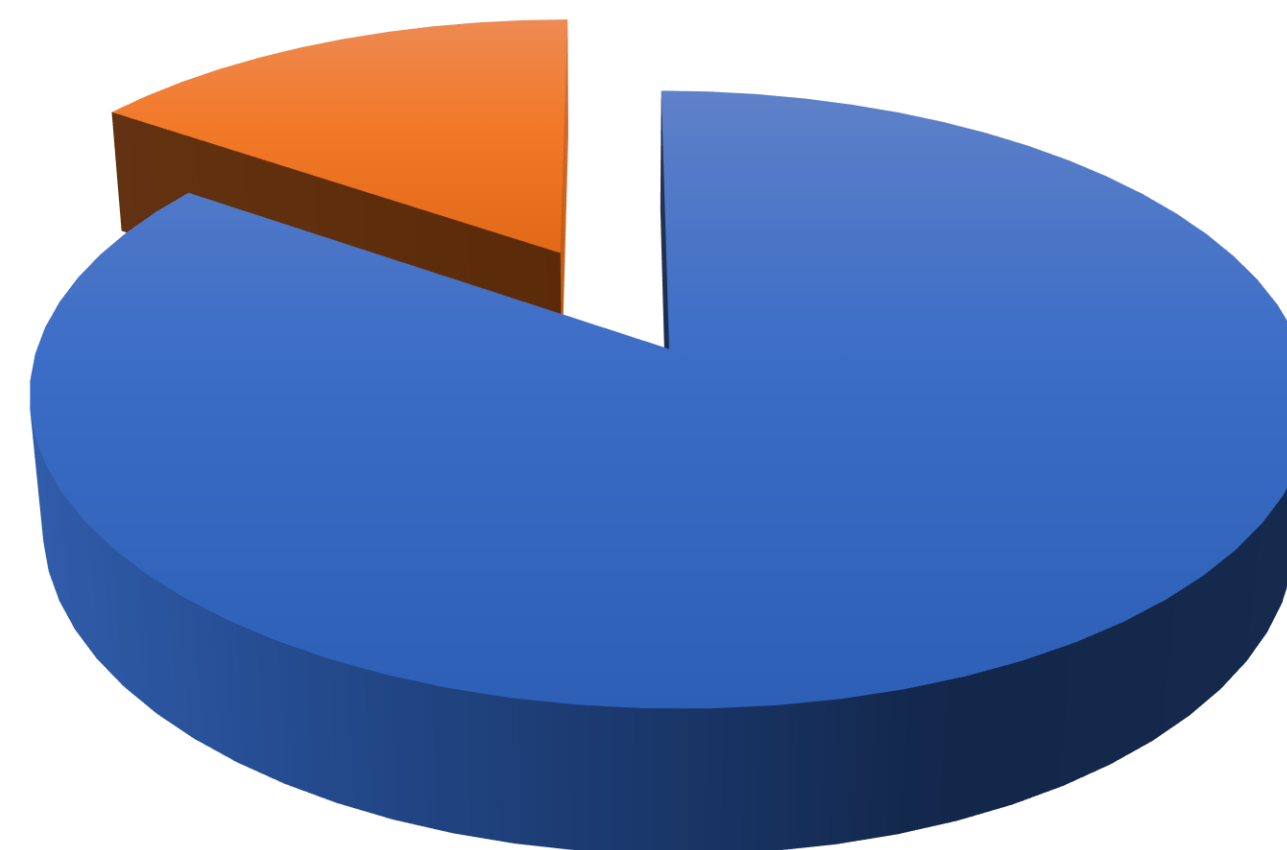
*Статистика собрана на основе анализа всех проектов CSI Group



Немного занимательной статистики: второй фактор*

Не настроен второй фактор

Нет
15%



Да
85%

*Статистика собрана на основе анализа всех проектов CSI Group



Немного занимательной статистики: ЭЦП*

ЭЦП была скомпрометирована



*Статистика собрана на основе анализа всех проектов CSI Group

Спасибо!

Вопросы?

Олег Безик
Эксперт в области
кибербезопасности и
расследований

+7 (926) 497-46-32, +7 (929) 629-81-62
oleg.bezik@csi.group