
Информационные угрозы в цифровой среде. Способы противодействия.

Тарас Сергеевич Черевко
К.ф.н. доцент кафедры теории и экономики СМИ
cherevkot@gmail.com



К определению

- Безопасность как отсутствие опасностей;
- Безопасность – это определенная деятельность по обеспечению или по предупреждению каких-либо угроз, опасностей;
- Безопасность – это осознанная потребность, ценность.



«Информационная безопасность»

- Информационная безопасность – совокупность мер по защите информационной среды, общества и человека;
 - Информационная безопасность – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц;
 - Информационная безопасность – защита потребителей от информации, защита информации от потребителей.
-



Дробление проблемы

Информационная безопасность

- информационная безопасность - защита национальных интересов, обеспечение потребителя достоверной и полной информацией, защита потребителя при получении, распространении и использовании информации;
- безопасность информации – отсутствие в ней побуждения человека к негативным действиям, умышленно заложенных механизмов негативного воздействия на человеческую психику или негативного воздействия на иной блок информации (вирус);
- защита информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации (изменения смысла), либо уничтожения

Таким образом, выстраивается ряд из трех научных категорий: информационная безопасность, безопасность информации и защита информации. При этом каждая последующая категория является составной частью предыдущей.



Регулирование информационных угроз



Доктрина информационной безопасности

- *доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;*
- *противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;*
- *пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;*
- *достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;*
- *создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;*
- *проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;*
- *развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;*
- *обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.*
- *соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;*

Блок «нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей» в новой доктрине вынесен в самый конец. Изменились приоритеты.



Федеральный закон «О безопасности»

- В соответствии с Законом РФ «О безопасности» безопасность – это «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». «Жизненно важные интересы – это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства»;
 - Основными принципами обеспечения безопасности являются:
системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, *информационных*, правовых и иных мер обеспечения безопасности.
-



ФЗ «Об информации, информационных технологиях и о защите информации»

- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации.
- Государственное регулирование в сфере применения информационных технологий предусматривает:
 - обеспечение информационной *безопасности детей*;
 - контроль и надзор за выполнением организационных и технических мер по *обеспечению безопасности персональных данных*.
- Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.



Программа «Цифровая экономика»

Задачи:

- Увеличить долю граждан, повысивших грамотность в сфере информационной безопасности, медиапотребления и использования интернет-сервисов;
- Увеличить долю населения, использовавшего средства защиты информации по субъектам Российской Федерации.



Что происходит с информационными угрозами сейчас?



Угрозы информационной безопасности - эволюционирующая среда

- За последнее десятилетие вместо хакерских атак на арену вышли приемы социальной инженерии. Внешние угрозы никогда не потеряют актуальность. Но уже очевидно, что технологии простого взлома теряют популярность. Будущее за социальной инженерией, фишингом и другими комбинациями цифровых атак, которые нацелены не на бездушную машину, а на главную уязвимость любой системы защиты — **человека**.
- В настоящее время наблюдается устойчивая тенденция смещения акцентов в деятельности по обеспечению безопасности с парадигмы *защищенности* на парадигму *развития*.
Появилось понятие «безопасность через развитие».



Информационные угрозы



Виды угроз

- вредоносное ПО (вирусы);
- фишинговые проекты (сайты, приложения);
- DDos-атаки;
- Ботнеты;
- недостоверная/искаженная информация (fake news);
- информация, способная навредить незащищенным группам пользователей (дети);
- информационные войны.

Цели:

- Получение доступа к данным;
- Получение доступа к управлению устройством;
- Получение финансовой выгоды;
- Актуализация инфоповодов;
- Формирование стереотипных представлений;
- Влияние на принятие решений;
- Моральный ущерб;
- Хактивизм.



Источники угроз и обеспечение ИБ

Организации, обеспечивающие информационную защиту:

- государственные структуры
- коммерческие организации
- общественные организации
- медиа
- пользователи

Источники угроз:

- другие государства
- коммерческие организации
- организованные преступные группы
- медиа
- частные лица

«По неосторожности»

Отставание по урону информатизации, отставание по технологии,
недостаточный уровень цифровой грамотности



НОВЫЕ ТЕХНОЛОГИИ

ВОЗМОЖНОСТИ ИЛИ УГРОЗЫ



Факультет журналистики Московского государственного университета имени М.В. Ломоносова

Ничего личного

- В 2018 году более 98 000 почтовых аккаунтов граждан в самых популярных российских и международных почтовых сервисах были скомпрометированы;
- Более 13 000 учетных записей пользователей в популярных российских соцсетях были взломаны в 2018 году;
- Утечки Facebook, Gmail, UBER, MyFitnessPal или индийского госпортала Aadhar, когда данные миллиарда человек продавались по цене 500 рупий (примерно 470 рублей).



Киберугрозы: вирусы-шифровальщики

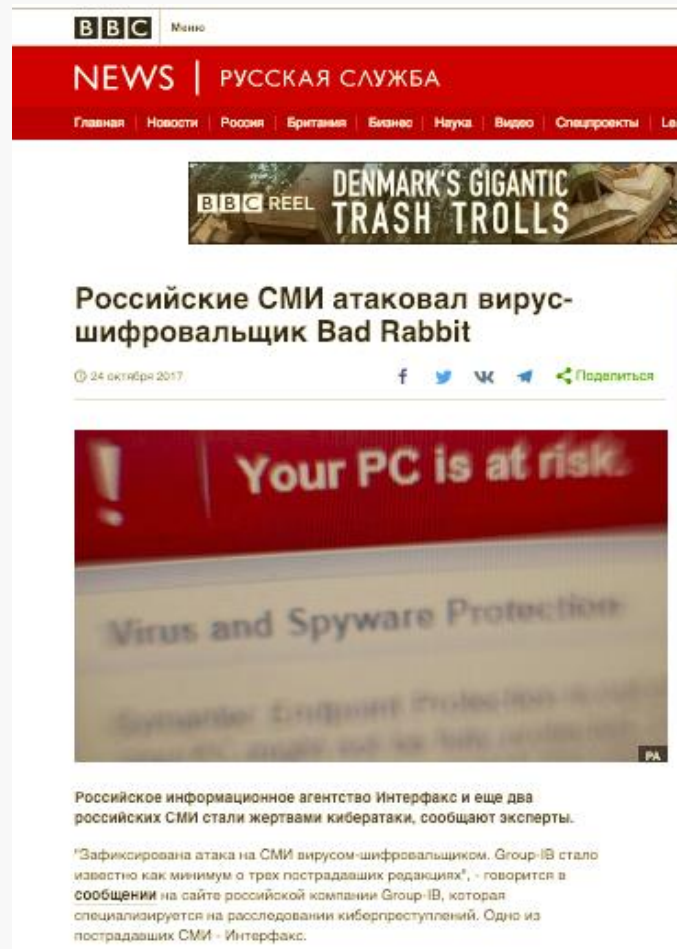
24 октября 2017.

BadRabbit атаковал серверы Киевского метрополитена, Министерства инфраструктуры, Международного аэропорта «Одесса».

Жертвы в России:

- ИА«Интерфакс»
- Фонтанка
- Новая газета (СПБ)
- Аргументы недели

Подозреваемый: АPT Black Energy.



Киберугрозы для СМИ: банковские трояны

Темы поиск по сайту... <АКТИОН> МЦФЭР <В> Вход и регистрация

Главбух **Акция!** **Новости** **Статьи** **Вопрос-ответ** **Учетная политика** **Формы** **Школа**

Главное в феврале Ваши контрагенты Сервисы Проверка отчетности Ещё... (7) **ПОДПИСАТЬСЯ**

Новости / 1 февраля 2019

Работникам хотят добавить 10 дней оплачиваемого отпуска

Работникам нужно предоставлять дополнительный отпуск при недомогании, если они не хотят обращаться ... 42417

Календарь бухгалтера на февраль 2019 года

В феврале бухгалтеру надо отправить 9 платежей и сдать 11 отчетов. 3354

Тема недели

Минтруд запретил отпуск в выходные дни

В свежем «Главбухе» /

- Выполняйте три условия, чтобы не платить штраф за НДФЛ
- Налоговики взялись за малый бизнес
- На сайте прокуратуры появились списки, к кому придет проверка

Июнь 2017 года

03:16 сотрудник фирмы в браузере Internet Explorer ввел запрос — "НДФЛ с доходов получаемых с иностранных компаний когда платить", нашел ссылку и зашел на сайт glavbukh.ru, в 03:29, уже сработал вредоносный скрипт, загрузка на компьютер банковского трояна Vuhtrap. Преступники получили удаленный доступ к счету и вывели деньги.



Киберугрозы для СМИ: фишинг и мошенничество

← → ↻ Ненадежный | lenta.run ☆

Приложения | Твиттер | (1) Facebook | Мой диск – Googl... | Входящие (1 914)... | Group-IB | Блог Group-IB | Tilda | HideNote - Пиши,... | Корпоративный п...

Главное
Россия
Мир
Бывший СССР
Экономика
Силовые структуры
Наука и техника
Культура
Спорт
Интернет и СМИ
Ценности
Путешествия
Из жизни
Дом

Войти в Мою Ленту


Мотор
Статьи
Галереи
Видео
Спецпроекты

Поиск

Лента добра

LENТА.RU

14 ЯНВАРЯ 2019, ПОНЕДЕЛЬНИК, 17:13



21:03 Раскрыты детали крушения самолета с российским экипажем в Африке

Добавить в «Мую Ленту»

00:13 В редакцию газеты принесли человеческую голову

23:03 Мексика отказалась договариваться с США насчет мигрантов

22:13 Тарасова оправдала провал Медведевой на чемпионате России

22:00 Взрывы салюта на складе пиротехники попали на видео

21:40 В Кремле объяснили правки в стенограмме пресс-конференции Путина

21:02 Германия покончила с углем

21:01 Рабочий выиграл сотни тысяч долларов и купил наркотики

КУРС ЦБ \$ 68,01 ↑ € 77,97 ↑

ГЛАВНЫЕ НОВОСТИ

США выдвинули России очередной ультиматум

Евросоюз продлил антироссийские санкции

В Москве подорожает проезд в общественном транспорте

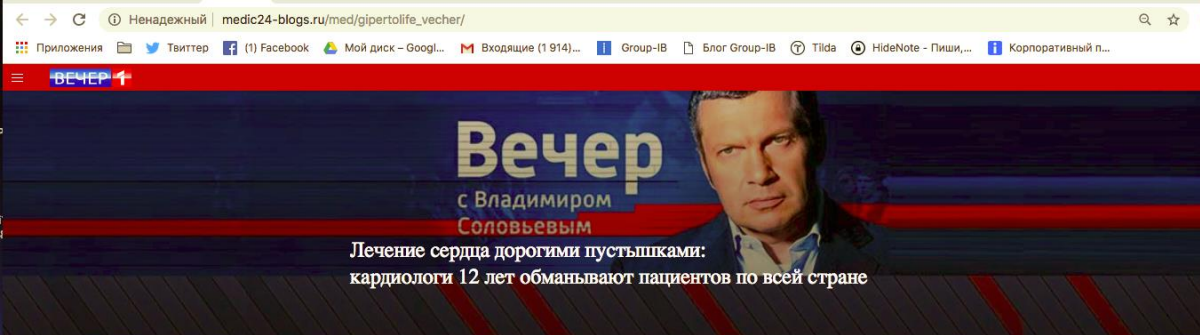
Кокорину и Мамаеву поменяли статью

Назван самый удобный для России кандидат в президенты Украины

Стало известно о гибели самолета с российским экипажем в Африке



Киберугрозы для СМИ: фишинг и мошенничество



От редакции:
Снижая давление - снижая 97% инфарктов и 87% инсультов! До 14.01.2019 (включительно) каждый гипертоник может получить уникальное средство для лечения давления (гипертонии), не уступающее аналогам в мире, по специальной программе **БЕСПЛАТНО**



Утечки в соцсетях и облачных сервисах



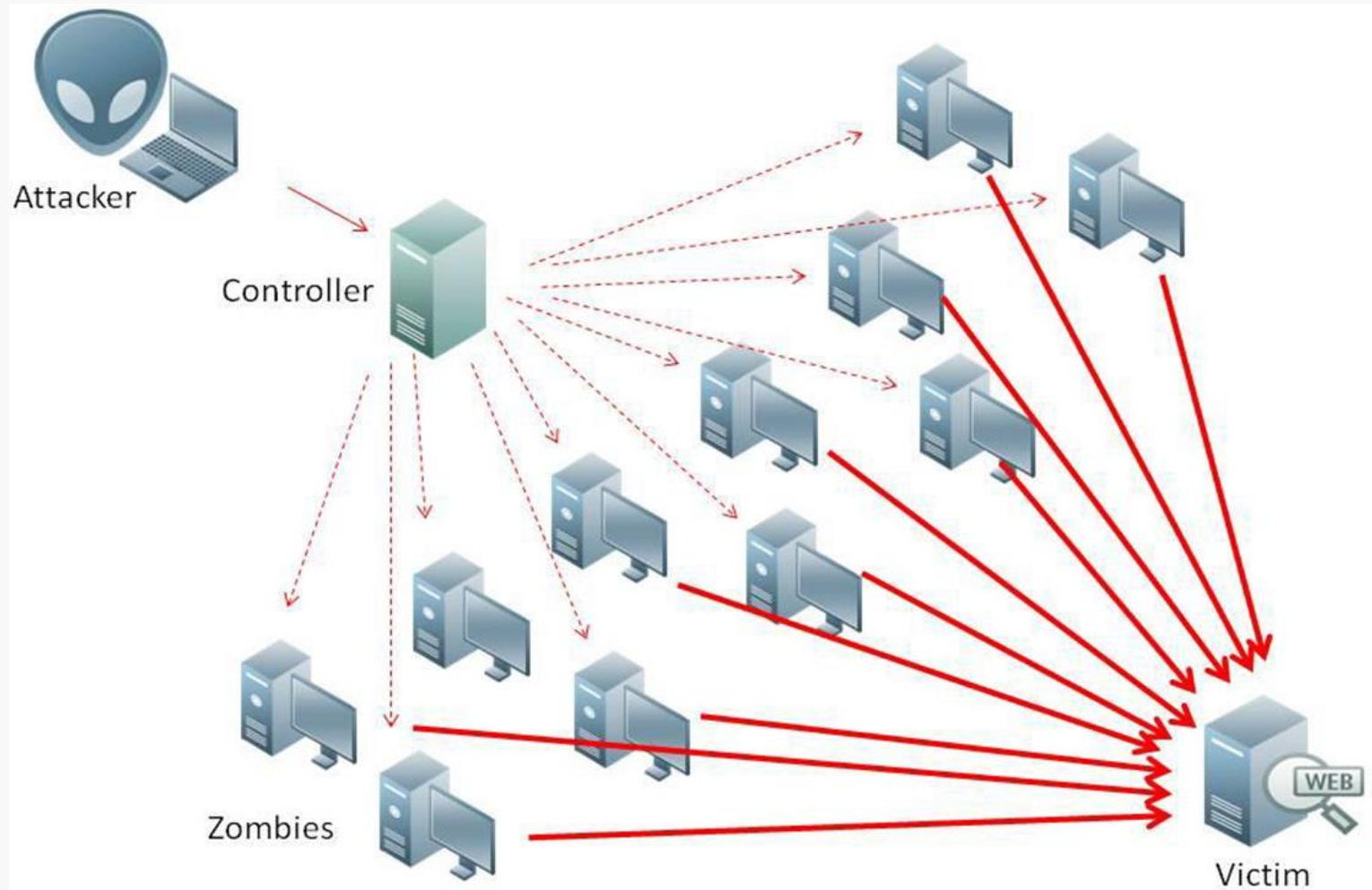
Евгений Никулин «гламурный хакер»
Его обвиняют во взломах LinkedIn,
Dropbox. Он якобы похитил и продавал
личные данные миллионов пользователей.



В США Никулину грозит 54 года
лишения свободы.



DDoS атаки



Из самого свежего (Troidesh)

- Только в июне Group-IB обнаружила более 1100 фишинговых писем.

ВНИМАНИЕ!

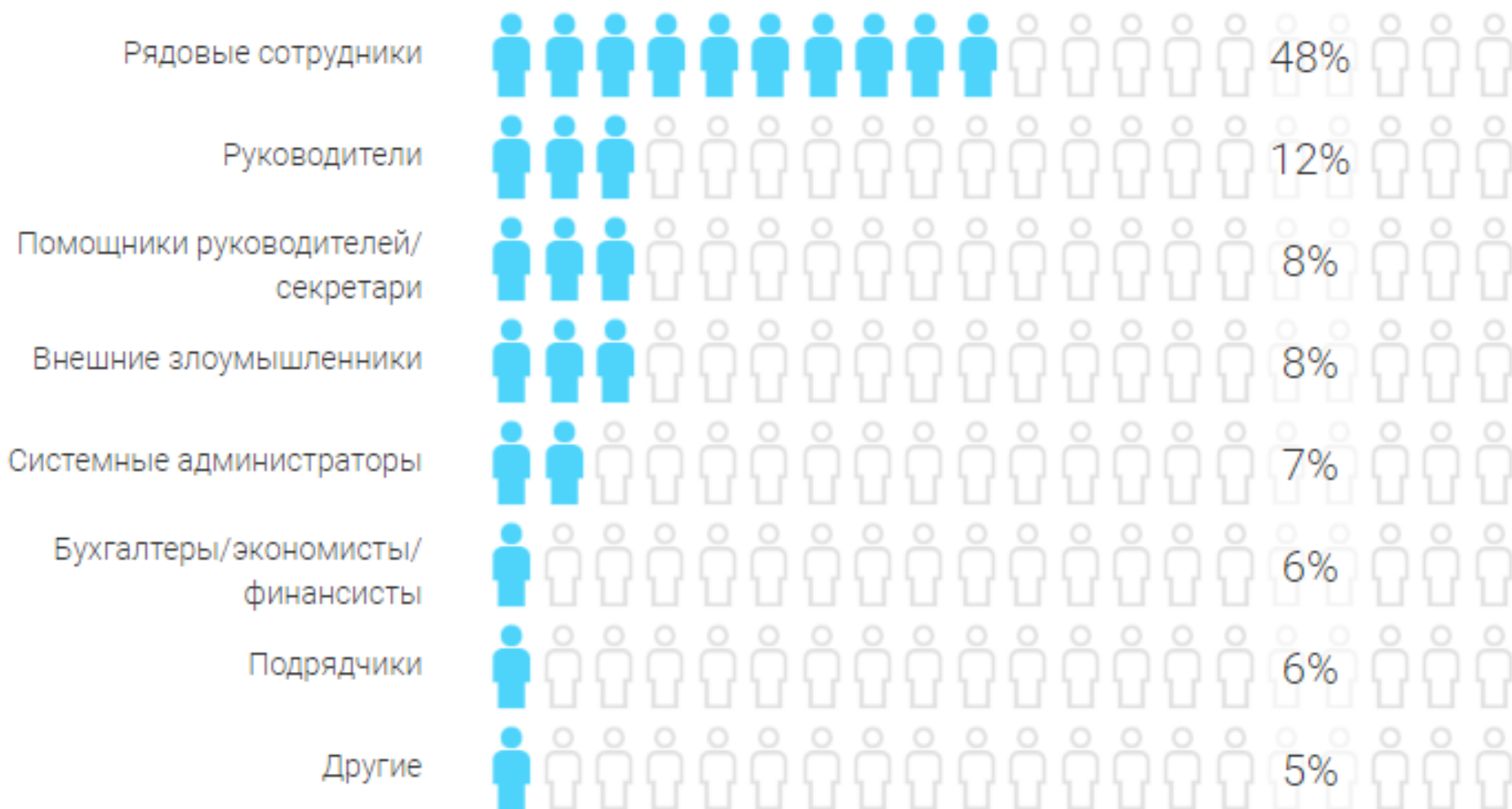
Все важные файлы на всех дисках вашего компьютера были зашифрованы. Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.

ATTENTION!

All the important files on your disks were encrypted. The details can be found in README.txt files which you can find on any of your disks.



Привели к нарушению ИБ



Уровень цифровой грамотности школьников 2018

64 617

ШКОЛЬНИКОВ ПРИНЯЛИ
УЧАСТИЕ В ТЕСТИРОВАНИИ

60%

ШКОЛЬНИКОВ ПОКАЗАЛИ **СРЕДНИЙ**
УРОВЕНЬ ЦИФРОВОЙ ГРАМОТНОСТИ

34%

ШКОЛЬНИКОВ ПОКАЗАЛИ **ВЫСОКИЙ**
УРОВЕНЬ ЦИФРОВОЙ ГРАМОТНОСТИ

6%

ШКОЛЬНИКОВ ПОКАЗАЛИ **НИЗКИЙ**
УРОВЕНЬ ЦИФРОВОЙ ГРАМОТНОСТИ

Москва
Санкт-Петербург
самые активные
города-участники

Чем школьники старше, тем
выше их уровень цифрового
потребления, цифровых компетенций
и цифровой безопасности

Цифровые компетенции
и цифровая безопасность
всех возрастных групп
нуждаются в повышении

Возрастные группы

- до 14 лет
- ▲ 14-16 лет
- 17-18 лет

■ ▲ ●
42 → 61 → 72

Высокий уровень **цифрового
потребления** в % школьников
по возрастным группам

■ ▲ ●
33 → 39 → 42

Высокий уровень **цифровой
безопасности** в % школьников
по возрастным группам

■ ▲ ●
18 → 28 → 36

Высокий уровень **цифровых
компетенций** в % школьников
по возрастным группам



Уровень цифровой грамотности взрослого населения (Москва)

52%

ОПРОШЕННЫХ МОСКВИЧЕЙ ПОКАЗАЛИ
СРЕДНИЙ УРОВЕНЬ ЦИФРОВОЙ ГРАМОТНОСТИ

47%

ОПРОШЕННЫХ МОСКВИЧЕЙ ПОКАЗАЛИ
ВЫСОКИЙ УРОВЕНЬ ЦИФРОВОЙ ГРАМОТНОСТИ

1%

ОПРОШЕННЫХ МОСКВИЧЕЙ ПОКАЗАЛИ
НИЗКИЙ УРОВЕНЬ ЦИФРОВОЙ ГРАМОТНОСТИ

Цифровое потребление
взрослых москвичей
нуждается в повышении

Лишь 5% взрослых
обладают высоким уровнем
цифрового потребления

Среди московских школьников
высокий уровень цифрового
потребления показали **63%**

Высокий уровень
цифровой
безопасности
показали

87% **40%**

взрослых

школьников

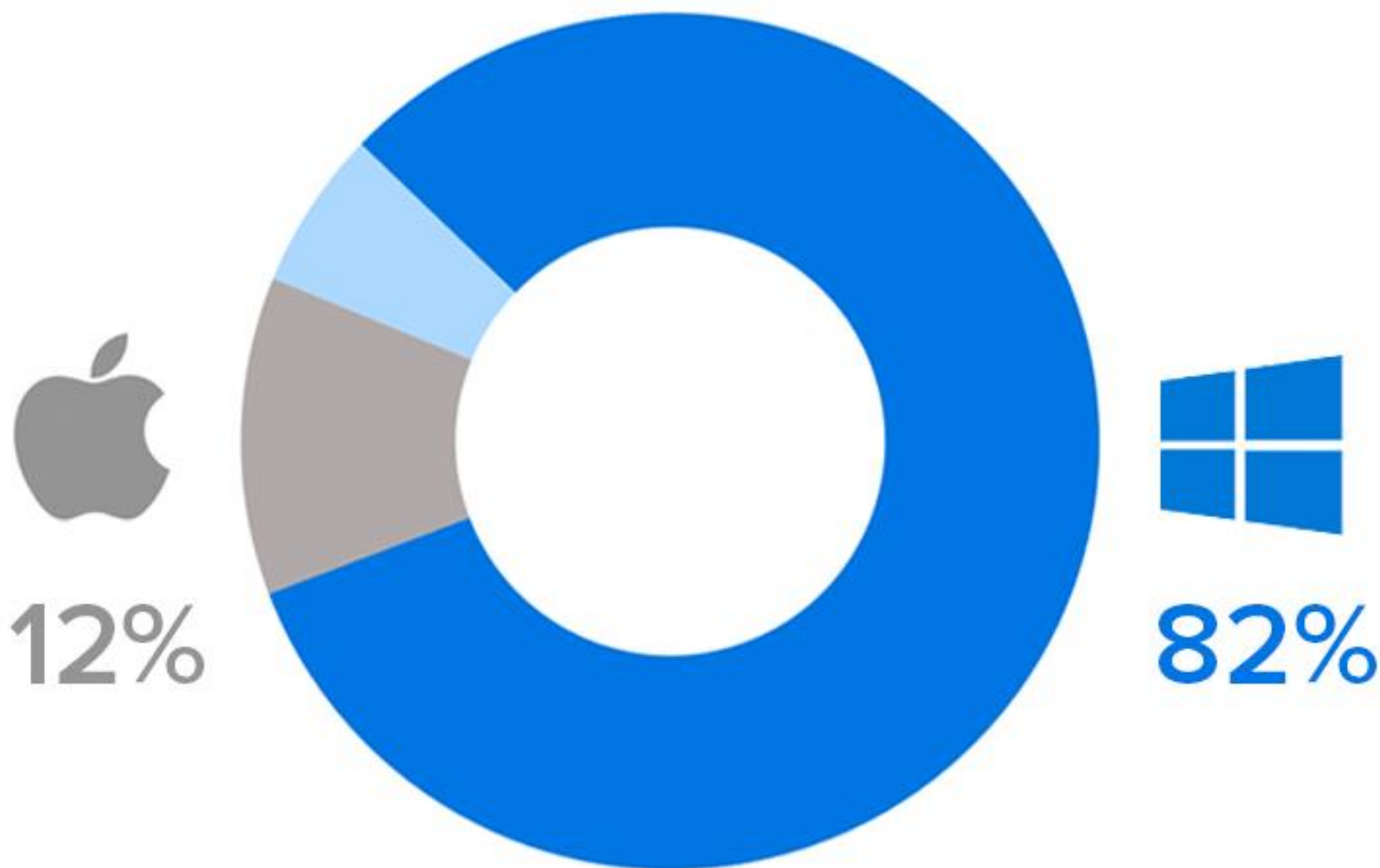
У взрослого населения Москвы наблюдается
дефицит компетенций транслирования
своих знаний младшему поколению



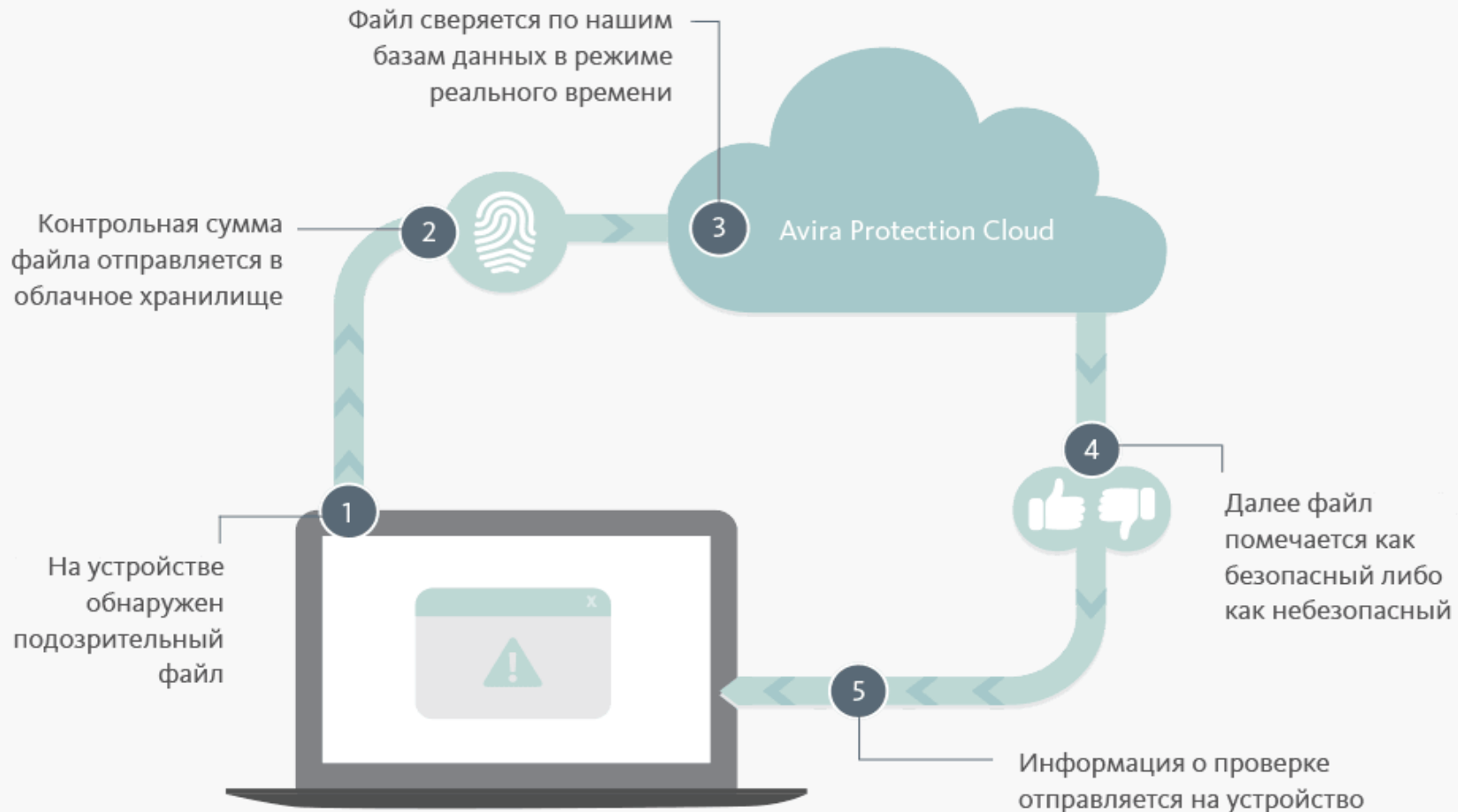
Пытаетесь ли вы противостоять информационным угрозам?



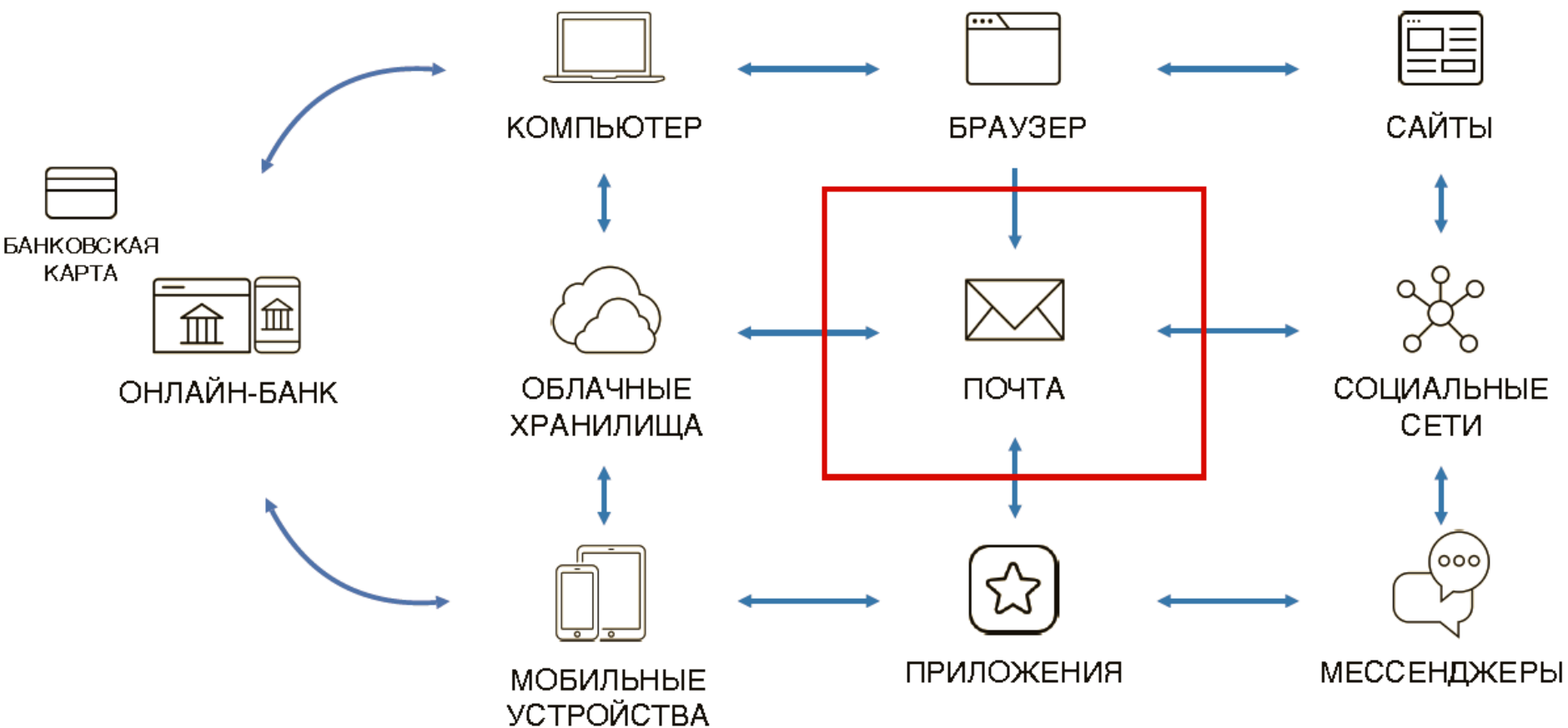
Пользователи операционных систем



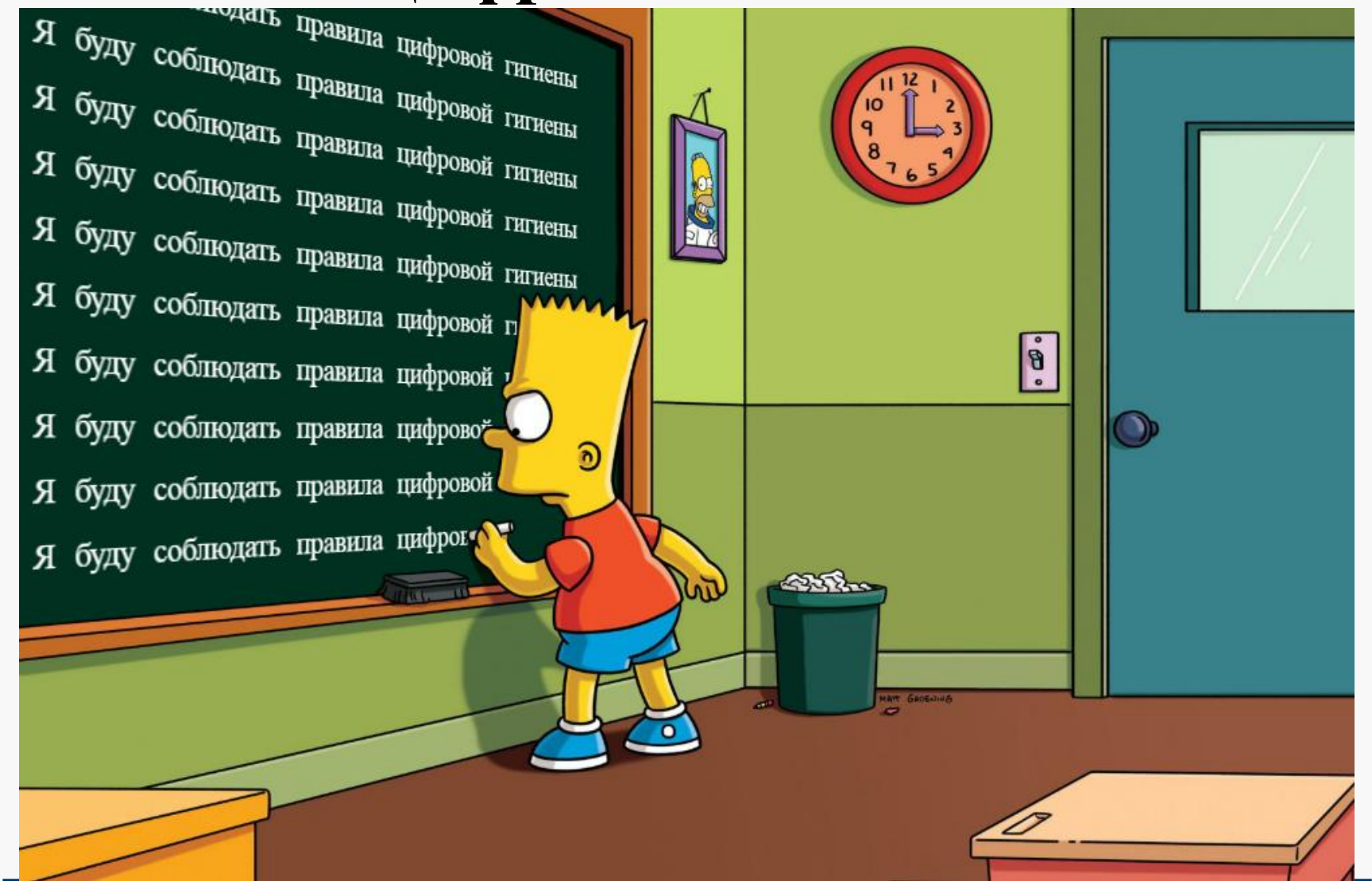
Как работают антивирусы



Ваша цифровая инфраструктура



Цифровая гигиена



Защита паролями

Топ 20 паролей

Gmail

123456
password
123456789
qwerty
12345678
111111
abc123
123123
1234567
1234567890
iloveyou
password1
000000
zaq12wsx
tinkle
qwerty123
monkey
target123
dragon
1q2w3e4r

Yandex

123456
123456789
111111
qwerty
1234567890
1234567
7777777
123321
000000
123123
666666
12345678
555555
654321
gfhjkm
777777
112233
121212
987654321
159753

Mail.ru

qwerty
123456
qwertyuiop
qwe123
qweqwe
klaster
1qaz2wsx
1q2w3e4r
qazwsx
1q2w3e
123qwe
1q2w3e4r5t
123456789
111111
zxcvbnm
1234qwer
qwer1234
asdfgh
marina
q1w2e3r4t5



gildartsev



Фишинг

Одноклассники (i)

odnoklasniki-vesna.ru/?check=e994c&subid=49#

Адрес не тот

одноклассники ⓘ

Зарегистрироваться

Регистрация моментальная

Вход на сайт

логин

пароль

запомнить

Войти Забыли пароль или логин?

Одноклассники Ж — универсальное средство - помощник для поиска людей, в системе которой ежедневно пользуются десятки миллионов человек

С помощью Одноклассники ЖВы можете:

- Обучиться, как Найти людей, с которыми Вы когда-либо учились, работали или отдыхали.
- Обучиться, как Узнать больше о людях, которые Вас окружают, и найти новых друзей.
- Обучиться, как Всегда оставаться в контакте с теми, кто Вам дорог.

что здесь делает эта полоса прокрутки? видимо это не конец страницы



Фишинг



Культура пользования антивирусом



KASPERSKY lab
ANTIVIRUS



Серьезное отношение к содержанию



Проверим наше умение противостоять цифровым угрозам

<https://meduza.io/games/postavte-sebya-na-mesto-rukovoditelya-i-zaschitite-kompaniyu-ot-kiberugroz>



СПАСИБО ЗА ВНИМАНИЕ

Будьте в безопасности

Тарас Сергеевич Черевко
К.ф.н. доцент кафедры теории и экономики СМИ
cherevkot@gmail.com

