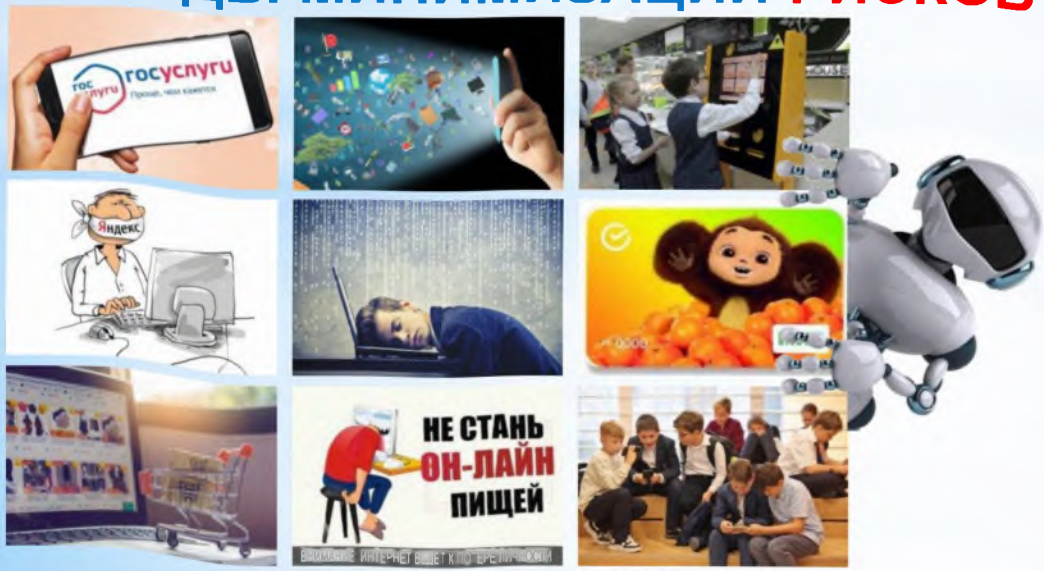
ИНСТИТУТ
СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ
ПРОБЛЕМ НАРОДОНАСЕЛЕНИЯ
им. Н.М. Римашевской
ФЕДЕРАЛЬНОГО НАУЧНОГО
ИССЛЕДОВАТЕЛЬСКОГО
СОЦИОЛОГИЧЕСКОГО ЦЕНТРА
РОССИЙСКОЙ АКАДЕМИИ НАУК

III МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ВОПРОСЫ
ПУБЛИЧНОГО УПРАВЛЕНИЯ, ЭКОНОМИКИ, ПРАВА
В СОВРЕМЕННЫХ ГЕОПОЛИТИЧЕСКИХ УСЛОВИЯХ»
28 марта 2026 г., Россия, г. Калининград

СОВРЕМЕННОЕ НАСЕЛЕНИЕ и КИБЕР-ОПАСНОСТИ – ТРЕНДЫ МИНИМИЗАЦИИ РИСКОВ



КРОШИЛИН
Сергей Викторович

Кандидат технических наук,
доцент,
Ведущий научный сотрудник
Лаборатории исследования
поведенческой экономики
ИНСТИТУТА
СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ
ПРОБЛЕМ НАРОДОНАСЕЛЕНИЯ
им. Н.М. Римашевской
ФНИСЦ РАН

СОВРЕМЕННЫЕ ТРЕНДЫ в ЦИФРАХ

- Всегда быть на связи — девиз современного человека, который задает ритм **жизни**.
  - Жизнь на «повышенных скоростях» предъявляет повышенные требования к организму: прежде всего к восприятию, реагированию, скорости принятия решений и процессу обработки информации.
- Исследование: средняя продолжительность концентрации внимания у **молодых людей** сократилась с 12 секунд в 2000 году до 8 секунд сегодня.
  - Если продолжительность роликов превышала **2–3 секунды**, мозг не в состоянии интерпретировать полученную информацию.

ФАКТЫ:

- Электронные устройства действуют со скоростями, которые человеку трудно осмыслить.
- Смена технологий идет такими темпами, за которыми человеку сложно успеть, а мобильных устройств, подключенных к интернету, уже больше, чем людей на планете.
- Современный контекст все более стимулирует активность и многозадачность человека, стремление «все успеть».
- Но «обратная сторона медали» — все большее давления, отсутствие времени даже на физиологически важные процессы, например, на сон.

Источник: Маербеков, А. Е. Влияние цифровых технологий на формирование привычек здорового образа жизни: возможности и риски / А. Е. Маербеков. — Текст : непосредственный // Молодой ученый. — 2025. — № 13 (564). — С. 19-21. — URL: https://moluch.ru/archive/564/123367. (дата обращения 10.10.2025)

НАСЕЛЕНИЕ и ИКТ

- **4,5 часа ежедневно** — среднее время, которое россияне проводят онлайн
  - **83%** заходят в сеть, чтобы скроллить ленты;
  - **70%** пользуются интернетом перед сном;
  - **50%** совершают покупки в вечерние часы.
- При этом россияне отмечают, что устают от объёма информации в интернете, а некоторые испытывают раздражение, когда долго не могут найти нужный контент или товар.
- Кроме того, современные ИКТ могут таить в себе множество опасностей и угроз, о которых пользователь может даже не подозревать.

НАИБОЛЕЕ ПОПУЛЯРНЫЕ ДЕЙСТВИЯ В ИНТЕРНЕТЕ:

- отправка личных сообщений (**63%**);
- просмотр страниц интернет-магазинов (**59%**).

- **32%** пользователей **совершают покупки** через социальные сети, что демонстрирует растущую интеграцию коммерции и контентных платформ в повседневные привычки российских пользователей.

Источник: Исследования сервиса «Яндекс Ритм».
Каждый третий россиянин проводит в интернете более шести часов в день / Портал Прайм. URL: https://1prime.ru/20251020/rossijanin-863705611.html (дата обращения 10.10.2025)

КИБЕР-ОПАСНОСТИ

- **«Жизнь» в цифровом мире** дает новые широкие возможности, но и провоцирует серьезные опасности.
- Несоблюдение **«элементарных правил»** может привести к краже конфиденциальных данных, финансовой информации, денежных средств.
- **Безопасность в сети** зависит не только от тех кто предоставляет цифровые услуги и государства, но и от **самого человека**.

НЕКОТОРЫЕ ЦИФРЫ

- **91%**
  россиян сталкивались с попытками мошенничества
- **123456**
  самый популярный пароль среди пользователей Рунета
- **меньше 2 сек.**
  требуется для взлома любого пароля до 6 символов
- **59%**
  пользователей используют один и тот же пароль для всех аккаунтов
- **от 80% угроз**
  защищает соблюдение простых правил кибербезопасности

Источник: 1) Как защитить себя и близких от киберугроз? [Электронный ресурс] // Минцифры России. Портал «КиберЗОЖ». URL: https://киберзож.рф/ (дата обращения 10.11.2025)
2) Кибермошенничество: портрет пострадавшего [Электронный ресурс] // Портал «Банк России». Режим доступа: https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения 05.09.2025 г.)

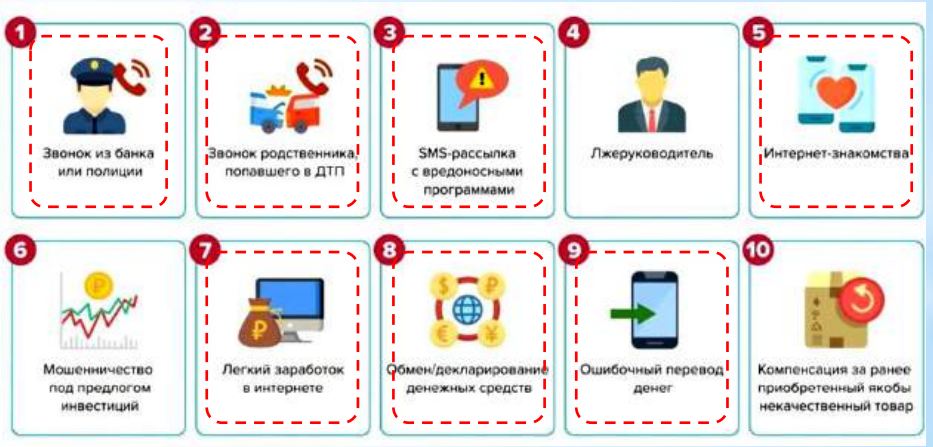
СХЕМЫ ОБМАНА МОШЕННИКОВ

- За первое полугодие 2025 года у россиян с помощью «телефонных мошенников» украдено почти **7 млрд руб.**, что на 2/3 выше, чем в 2024г.
- При этом само количество случаев совершения противоправных действий в России **сократилось почти на 1/5** по сравнению с предыдущим периодом прошлого года. Но действия мошенников стали ориентированы «на более прибыльные» схемы.

Как мошенники пытались получить доступ к деньгам

Источник: Кибермошенничество: портрет пострадавшего [Электронный ресурс] // Портал «Банк России». Режим доступа: https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения 05.09.2025 г.)

10 самых распространенных способов мошенничества (данные Прокуратуры Москвы)



- В первом полугодии 2025 г. **в семь раз** возросло использование мошенниками «**дропперов**» (незаконные переводы и/или обналичивание средств), **в четыре раза** увеличилось использование схем с **букмекерскими ставками** / «фейковыми» выигрышами в лотерею.

Банк России

Источник: Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс] // Портал «Банк России». Режим доступа: https://www.cbr.ru/statistics/ib/review_2q_2025/ (дата обращения 05.09.2025 г.).

«ДИПФЕЙКИ» С ИСПОЛЬЗОВАНИЕМ ИИ

- Начиная с 2025 года технологии «**дипфейков**» используется уже больше, чем в половине мошеннических схем. Они связаны, прежде всего, с **телефонными звонками в мессенджерах**.
- Согласно исследованиям компании RTM Group, **более 70% «дипфейков»** применяются против физических лиц с целью **кражи денежных средств**. Чаще всего используются популярные мессенджеры и социальные сети к которым уже привыкли.

RTM GROUP

ПОРТРЕТ ПОСТРАДАВШЕГО ОТ КИБЕРМОШЕННИКОВ

Источник: Кибермошенничество: портрет пострадавшего [Электронный ресурс] // Портал «Банк России». Режим доступа: https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения 05.09.2025 г.)

МНЕНИЕ ЭКСПЕРТА:

- *«…Особенно активно растет количество атак с применением технологий искусственного интеллекта (ИИ).*
- *В начале прошлого года число мошеннических схем с применением ИИ увеличилось на 1/3 по сравнению с предыдущим периодом …»*

Управляющий компанией RTM Group
(кибербезопасность и право в ИТ-индустрии)
Евгений ЦАРЕВ

Источник: Отдай мне свои данные! Россиян атакуют дипфейки. Раздел «Экспертиза» [Электронный ресурс] // Портал ВЦИОМ. Режим доступа: https://wciom.ru/expertise/otdai-mne-svoi-dannye-rossijan-atakujut-dipfeiki (дата обращения 05.09.2025 г.)

УЩЕРБ ОТ КИБЕРМОШЕННИКОВ

- Согласно официальным заявлениям МВД России в 2024 году кибермошенничество **составило 40%** от общего числа совершенных преступлений.
- В 2023 году их было меньше на 13%.
- Во втором квартале 2025 г. было совершено **273,1 тысячи** мошеннических операций.
  - Ущерб от действий злоумышленников составил **6,3 млрд руб**.
  - У частных (физических) лиц было похищено **более 6 млрд руб.**, но благодаря противодействиям со стороны соответствующих органов часть средств было возвращено.

Источник: Кибермошенничество: портрет пострадавшего [Электронный ресурс] // Портал «Банк России». Режим доступа: https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения 05.09.2025 г.)

Банк России

Похищенные денежные средства кибермошенниками у ФЛ (II квартал 2025 г.)

Вид хранения финансовых средств жертв	Сумма похищенных денежных средств, млрд руб.	Доля возвращенных денежных средств, %
Пластиковые карты клиентов	1,561	7,2
Счета клиентов (при осуществлении дистанционного банковского обслуживания)	2,225	6,8
Система быстрых платежей (СБП) (при переходе на фейковые QR-коды)	2,192	2,7
Электронные кошельки клиентов	0,021	6,1
Без открытия счёта в банке	0,016	0,0

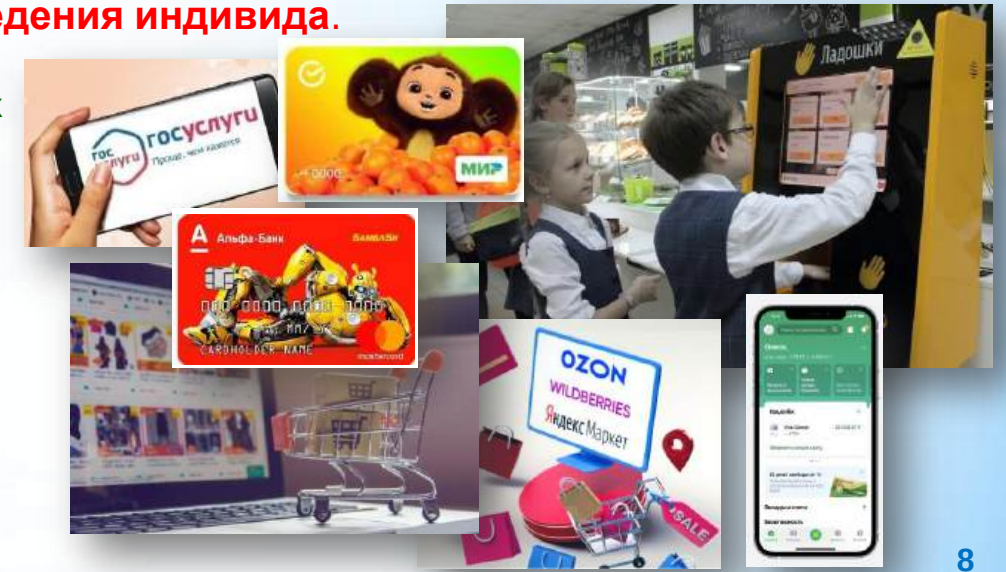
- Похищено при дистанционном банковском обслуживании / при переводах (2,225 млрд руб.). Удалось вернуть 6,8%.
- СБП, как правило при переходе «жертвы» по фейковым QR-кодам (2,192 млрд руб.). Удалось вернуть лишь 2,7%.
- С пластиковых банковских карт украдено около 1,6 млрд руб. Удалось вернуть 7,2% украденных средств.

Банк России

Источник: Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс] // Портал «Банк России». Режим доступа: https://www.cbr.ru/statistics/ib/review_2q_2025/ (дата обращения 05.09.2025 г.).

КИБЕРМОШЕННИЧЕСТВО и ФИНАНСОВАЯ ГРАМОТНОСТЬ

- **Проблема финансовой грамотности** при массовом распространении и доступности ИКТ через которые сегодня совершается большинство транзакций с финансовыми организациями – становится все актуальнее. Все чаще применяется «цифровой-расчет» при покупке в магазинах и на маркетплейсах в Сети.
- Меняется сама **форма финансового поведения индивида**.
- Финансовые услуги предлагаются даже детям (банковские карты для детей, списание денежных средств со счета телефона при оплате «школьного» питания – проект «Ладошки» и т.п.).
- Молодое российское поколение «**не видит препятствий**» для совершения финансовых операций посредством современных гаджетов и устройств, которые позволяют это сделать **в любом месте и в любое время**.
- Все больше информационных услуг, в т.ч. и государственных, оказываются с **помощью ИКТ**, которые используют конфиденциальную информацию и финансовые данные человека.



ФИНАНСОВАЯ ГРАМОТНОСТЬ НАСЕЛЕНИЯ

- Согласно результатам мониторинга **ВЦИОМ** по вопросу самооценки российского населения своей финансовой грамотности (проводится с 2010 года), люди стали более высоко оценивать свой показатель, который вырос до уровня **3,43** (из 5 возможных).
- Нынешнее поколение «Зумеров» входит в тройку лидеров по самооценке в вопросах финансовой грамотности (3,44 б.).
- Выше оценивают собственные знания «Старшие миллениалы», которые рождены в период реформ 90-х годов (3,62 б.).
- Более значимо оценили себя и те, кто старше 78 лет «Поколение оттепели» (3,42 б.).

Самооценка знаний и навыков в вопросах финансовой грамотности респондентами, балл

Примечание:
- Поколение цифры (зумеры) (рожденные в 2001 г. и позднее);
- Младшие миллениалы (рожденные в период с 1992 по 2000 гг.);
- Старшие миллениалы (рожденные в период с 1982 по 1991 гг.);
- Реформенное поколение (рожденные в период с 1968 по 1981 гг.);
- Поколение застоя (рожденные в период с 1948 по 1967 гг.);
- Поколение оттепели (рожденные до 1947 г.).

Источник: Финансовая (без)грамотность в России: мониторинг (22 апреля 2025) [Электронный ресурс] // Портал «ВЦИОМ». Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/finansovaja-bezgramotnost-v-rossii-monitoring (дата обращения 01.09.2025 г.)

МОЛОДОЕ ПОКОЛЕНИЕ – ОСНОВНАЯ ЦЕЛЬ

- На 2025 год можно констатировать, что практически **8 из 10 молодых людей** используют мобильный телефон для совершения различных финансовых операций.
- Выборка из массива данных ВЦИОМ «молодежи до 24 лет» (в т.ч. «Зумеров») показала, что они чаще остальных осуществляют управление своим финансами посредством телефона.
- Это безусловно предопределяет **рост интереса кибермошенников** к потребителям финансовых услуг **данного возраста**.

Использование мобильного телефона россиянами для решения финансовых задач, %

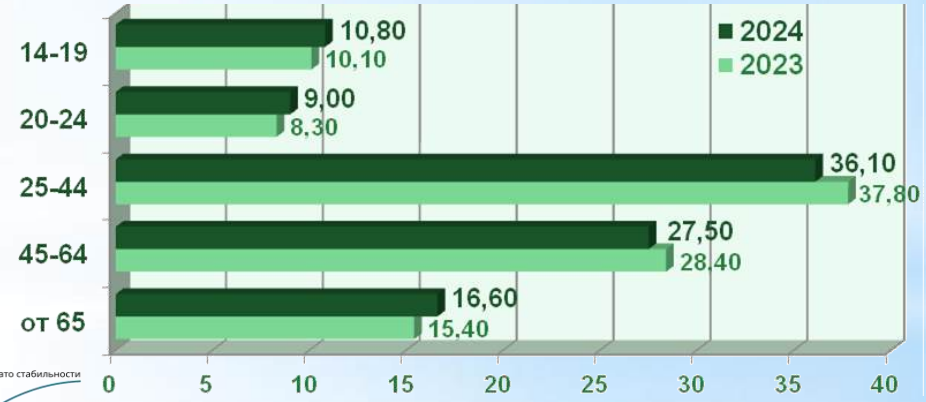
Примечание: МП – молодое поколение. Выборка сделана из базы SPSS обследования ВЦИОМ молодых опрошенных возрастных когорт (в т.ч. «Зумеров») до 24 лет включительно.

Источник: Финансовая (без)грамотность в России: мониторинг (22 апреля 2025) [Электронный ресурс] // Портал «ВЦИОМ». Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/finansovaja-bezgramotnost-v-rossii-monitoring (дата обращения 01.09.2025 г.)

ФИНАНСОВАЯ ГРАМОТНОСТЬ НАСЕЛЕНИЯ

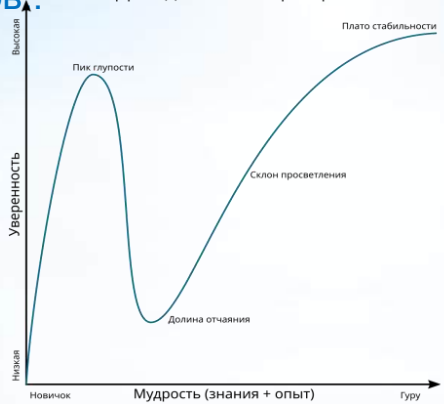
- Исследования, проведенным **Банком России**, показывают, что именно люди последних трех возрастных поколений (Зумеры, Младшие и Старшие миллениалы) чаще становятся **жертвами кибермошенников**.
- Они пользуются ИКТ интенсивнее в повседневной жизни для совершения банковских операций и являются наиболее **активными потребителями** различных цифровых сервисов.
- Разница в полученных результатах двух мониторингов может быть обусловлен так называемым **Эффектом Даннинга-Крюгера**.
- Люди, обладающие незначительными знаниями в определенной области, **значительно переоценивают** свои знания.

Доля возрастных когорт, среди граждан, ставшими жертвами кибермошенников (2023-2024 гг.), %



Примечание:
- Поколение цифры (зумеры) (рожденные в 2001 г. и позднее);
- Младшие миллениалы (рожденные в период с 1992 по 2000 гг.);
- Старшие миллениалы (рожденные в период с 1982 по 1991 гг.);
- Реформенное поколение (рожденные в период с 1968 по 1981 гг.);
- Поколение застоя (рожденные в период с 1948 по 1967 гг.);
- Поколение оттепели (рожденные до 1947 г.).

Эффект Даннинга — Крюгера



Банк России

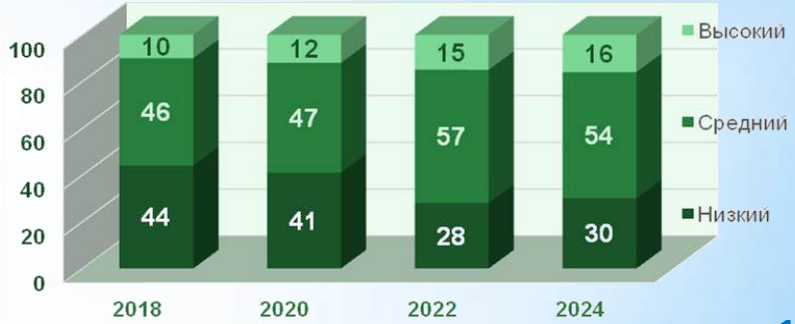
Источник: Кибермошенничество: портрет пострадавшего [Электронный ресурс] // Портал «Банк России». Режим доступа: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения 01.09.2025 г.).

ФИНАНСОВАЯ ГРАМОТНОСТЬ НАСЕЛЕНИЯ

- **НАФИ** уже более 10 лет рассчитывает «**Индекс финансовой грамотности россиян**».
  - В 2024 году **треть россиян** продемонстрировали «низкий» уровень, остальные – «высокий» или «средний».
- Индекс в 2024 год составил **12,77 баллов**.
  - С «низким» уровнем финансовой грамотности (диапазон 1-11 баллов) стало чуть меньше людей по сравнению с 2018 г..
  - Со «средним» уровнем в 2024 г. доля увеличилась до 54% (в 2018 г. значение было 46%).

Индекс финансовой грамотности россиян (2018-2024гг.), балл (из 21 возможных)

Диапазон и значения уровня финансовой грамотности россиян, %



Источник: Индекс финансовой грамотности россиян – 2024 [Электронный ресурс] // Аналитический центр «НАФИ». Режим доступа: https://nafi.ru/analytics/indeks-finansovoy-gramotnosti-rossiyan-2024/ (дата обращения 08.02.2026 г.).

КАК МИНИМИЗИРОВАТЬ РИСКИ

- **Цифровой ЗОЖ** — использование цифровых технологий для поддержания ЗОЖ (или **ЗОЖ в киберпространстве**).
  - Использование цифровых технологий для ЗОЖ имеет и риски, среди которых зависимость от устройств, неточность данных и утечка персональной информации.
- **Информационная гигиена** — это система правил и принципов, которые помогают эффективно обращаться с информацией и защищать себя от негативного влияния непроверенных или вредоносных данных.
  - Раздел медицинской науки, изучающий закономерности влияния информации на психическое, физическое и социальное благополучие человека.
- **КиберГигиена** — это совокупность правил и практик, направленных на обеспечение безопасного поведения в цифровом пространстве.

ПРАВИЛА КИБЕРГИГИЕНЫ:

- Создавайте надёжные пароли.
- Подключите двухфакторную аутентификацию.
- Будьте внимательны к письмам со ссылками и файлами.
- Будьте внимательны к именам сайтов или отправителям писем.
- Не скачивайте файлы из непроверенных источников.
- Минимизируйте использование открытого Wi-Fi.
- Регулярное обновление Антивирусов.
- Осуществляйте резервное копирование данных.

Источник: 1) Здоровый образ жизни: что это такое, главные правила и советы. Что дает ЗОЖ, как его придерживаться [Электронный ресурс] // Портал «RBC». URL: https://www.rbc.ru/life/news/62e253169a7947a362945b24 (дата обращения 10.10.2025);
2) Маербеков, А. Е. Влияние цифровых технологий на формирование привычек здорового образа жизни: возможности и риски / А. Е. Маербеков. — Текст : непосредственный // Молодой ученый. — 2025. — № 13 (564). — С. 19-21. — URL: https://moluch.ru/archive/564/123367. (дата обращения 10.10.2025).
3) Кибергигиена [Электронный ресурс] // Портал «Координационный центр по обеспечению кибербезопасности». URL: https://cert.gov.kg/ru/cyber_security/2/ (дата обращения 10.10.2025)

ЧЕМ НАМ ЭТО МОЖЕТ ГРОЗИТЬ ?

- **«Гуглизация сознания»** — понятие, которое описывает уверенность людей в том, что все **необходимые знания можно найти** с помощью **поисковой услуги** в интернете, не затрачивая особых усилий. **Сейчас это усугубилось использованием ИИ !**
- **«Смартфонизация населения» -** процесс активного роста числа пользователей смартфонов и их значимости в повседневной жизни.
  - Меняется **способ доступа** к интернету.
  - Происходит **трансформация социальных процессов.**
  - **Изменение восприятия** времени и пространства.
  - Влияние на **демографические процессы**.

ПРАВИЛА ИНФОРМАЦИОННОЙ ГИГИЕНЫ:

- Ограничение времени, проводимого в интернете, особенно в социальных сетях.
- Контроль входящей информации.
- Внимательное отношение к личным данным.
- Фильтрация информации.
- Использование сложных паролей.
- Защита от вирусов.
- Вежливое и корректное поведение в Сети.

Источник: Информационная гигиена [электронный ресурс] // Портал ФБУЗ «Центр гигиенического образования населения» Роспотребнадзора. URL: https://cgon.rospotrebnadzor.ru/naseleniyu/zdorovyy-obraz-zhizni/informatsionnaya-gigiena/ (дата обращения 10.10.2025)

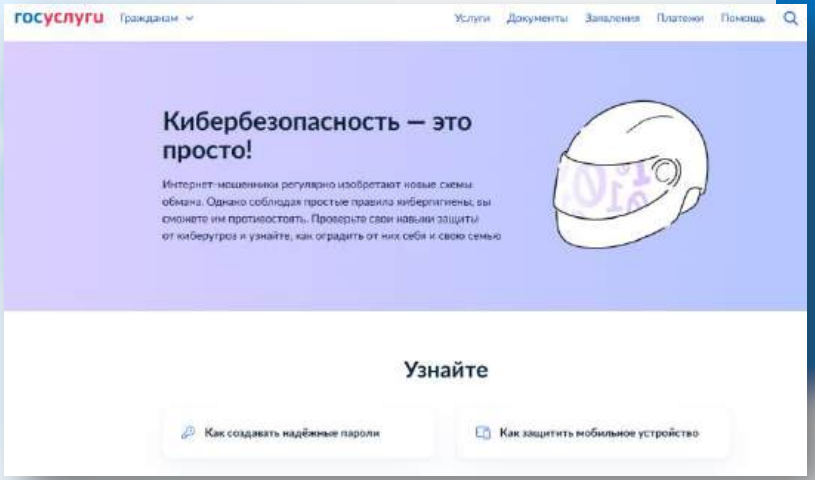
Распространение интернет-технологий в России и "гуглизация" сознания молодежи / Е. И. Медведева, С. В. Крошилин // Национальные интересы: приоритеты и безопасность. – **2014**. – Т. 10, № 3(240). – С. 9-19. – EDN RSMBUB.

КАК МИНИМИЗИРОВАТЬ РИСКИ:
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ и ГОСУСЛУГИ

- Осенью 2024 г. открылся специальный раздел на Госуслугах «**Кибербезопасность — это просто**».

РАЗДЕЛЫ РЕСУРСА

- Узнайте
- Часто задаваемые вопросы
- Новые схемы мошенничества
- Куда обратиться, если столкнулись с мошенничеством



https://www.gosuslugi.ru/cybersecurity

МНЕНИЕ ЭКСПЕРТА:

- *«Тема личной информационной безопасности раньше не была предметом системной разработки… Запланированная нами программа кибергигиены станет первым проектом такого масштаба.*
- *Она позволит пользователям узнать больше о том, как, например, защитить себя и свои данные, что, в свою очередь, будет способствовать снижению ущерба от кибератак.»*

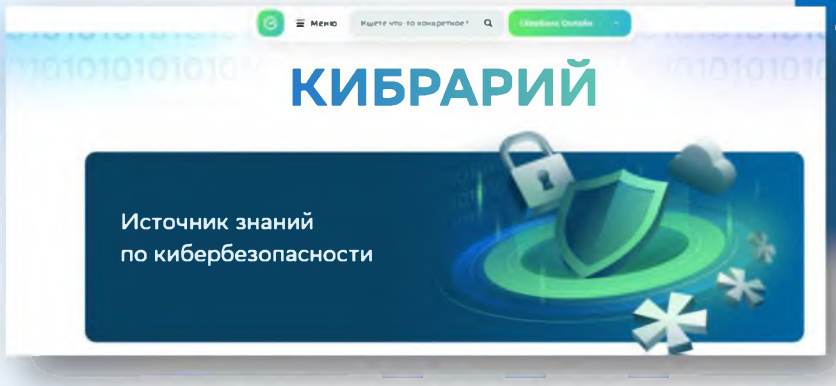
Директор Департамента обеспечения кибербезопасности Минцифры России
Владимир БЕНГИН

КАК МИНИМИЗИРОВАТЬ РИСКИ БЕЗОПАСНОСТЬ и КИБРАРИЙ (от СБЕРа)

- **«Кибрарий»** — библиотека знаний о кибербезопасности, запущенная в 2022 году.
- **Цель проекта** — повысить уровень киберграмотности граждан России, информировать о киберугрозах и распространённых схемах мошенничества.

РАЗДЕЛЫ РЕСУРСА

- Что почитать
- Эксперты рекомендуют
- Киберсовет
- Защитите себя и близких



https://www.sberbank.ru/ru/person/kibrary

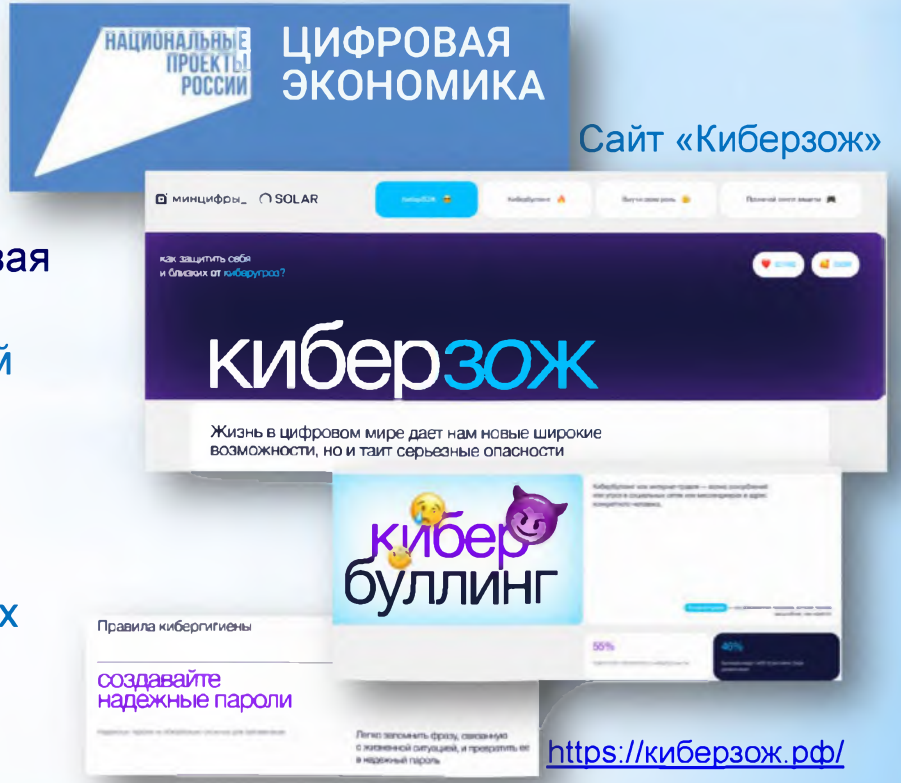
МНЕНИЕ ЭКСПЕРТА:

- *«Кибрарий» помогает людям и компаниям защищаться от мошенников, а экспертам в сфере кибербезопасности - быть ещё успешнее в борьбе с ними…*
- *России необходима национальная стратегия по кибербезопасности…*
- *Большинство киберпреступлений, в том числе все крупные современные кибератаки, совершаются с помощью технологий ИИ…»*

Президент и председатель правления ПАО «Сбербанк России»
Герман ГРЕФ

КАК МИНИМИЗИРОВАТЬ РИСКИ: КИБЕРЗОЖ от МИНЦИФРы

- Министерство цифрового развития, связи и массовых коммуникаций России (в рамках реализации Национального проекта «Цифровая экономика») запустило сайт «**Киберзож**».
  - Проект нацелен на повышение цифровой грамотности россиян.
  - Платформа рассказывает россиянам о правилах поведения при атаках мошенников.
  - Также россиянам напоминают о правилах «цифровой гигиены».



Сайт «Киберзож»

https://киберзож.рф/

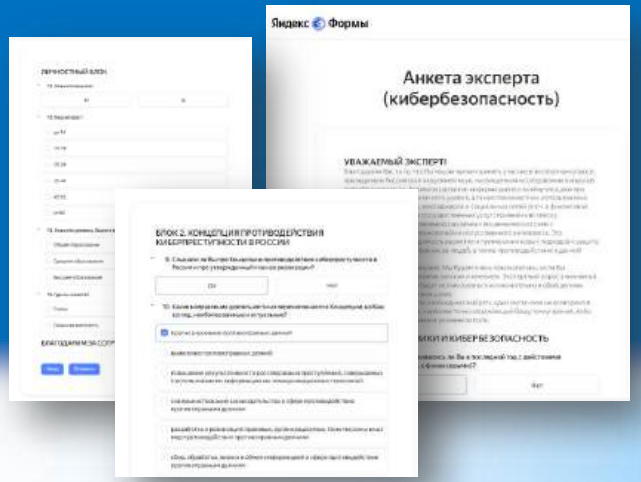
Источник: Бороться с мошенниками в России поможет «Киберзож» [Электронный ресурс] // Портал «ТВ.Санкт-Петербург». URL: https://tvspb.ru/news/2022/11/11/borotsya-s-moshennikami-v-rossii-pomozhet-kiberzozh (дата обращения 10.11.2025)

ИССЛЕДОВАНИЯ ИСЭПН ФНИСЦ РАН

- Учеными ИСЭПН ФНИСЦ РАН реализован **экспертный опрос**.
  - **Цель**: исследование вопросов кибербезопасности и кибермошенничества в российском обществе, защита от которых становится все более востребованной и актуальной, включая вопросы повсеместного использования мобильных приложений, мессенджеров и социальных сетей .
- **Эксперты**: молодые люди **в возрасте до 24 лет,** в т.ч. поколение «Зуммеров» (7 экспертов).
  - Все эксперты имели определенную профподготовку в сфере применения и использования ИКТ – 4 эксперта с высшим техническим образованием в сфере ИТ.
  - 3 эксперта являлись студентами старших курсов, которые обучаются по направлениям, связанным с информационной безопасностью и защитой данных.
  - Среди них - 5 специалистов уже работают на предприятиях, связанных с ИКТ и защитой данных, в т.ч. 2 эксперта из службы информационной безопасности в банковской сфере.

ИНСТРУМЕНТАРИЙ:

- Топ-гайд, реализованный на основе «Яндекс-формы», на основе технологии CAWI.
- Анализ результатов в ПО MS Excel («Анализ данных» и «Поиск решений»)



Источник: Авторские исследования. ИСЭПН ФНИСЦ РАН. 2024-2026 гг.

РЕЗУЛЬТАТЫ ЭКСПЕРТНОГО ОПРОСА

- **Эксперт №1** жертва кибермошенников по схеме «получение доступа к аккаунту на портале «ГосУслуги».
  - *«… Мне позвонили якобы сотрудники Социального фонда России (который объединили с Пенсионным фондом РФ) и очень мило попросили уточнить мое место работы и стаж. Для этого они готовы записать меня на удобное время через Портал «ГосУслуги». Мне достаточно только сообщить код подтверждения.*
    - *После того как мне действительно пришел «код подтверждения», который на самом деле оказался кодом на смену пароля на портале – я догадался, что разговаривал с мошенниками и повесил трубку. После этого уже «разворачивался знакомый сценарий».*
  - *Последовал звонок якобы из правоохранительных органов с вопросом: «Ваш аккаунт на «ГосУслугах» был подвержен атаке кибермошенников и т.д. и т.п.»… на что я просто не среагировал» - рассказал нам один из экспертов. На наш вопрос эксперту: «А что именно Вас натолкнуло на мысль, что это мошенники?» он ответил: «Это приписка в СМС сообщении от Портала «ГосУслуг» – что не сообщайте код другим лицам…».*

ЭКСПЕРТНОЕ МНЕНИЕ

- Все эксперты в том или ином варианте **сталкивались за последний год с действиями кибермошенников** в т.ч. в финансовой сфере как физические лица.
- В основном им поступали телефонные звонки и «дипфейковые» сообщения в мессенджерах (атаки через мессенджеры).
- В меньшей степени мошенники их беспокоили через сообщения в социальных сетях, а также письмами на электронную почту (все опрошенные имеют надежные программы защиты от СПАМа и вирусов как на компьютерах, так и на телефонах).

Источник: Авторские исследования. ИСЭПН ФНИСЦ РАН. 2024-2026 гг.

РЕЗУЛЬТАТЫ ЭКСПЕРТНОГО ОПРОСА

- **Эксперт №2** чуть не был обманут (по схеме мошенников) на одном из маркетплейсов.
  - *«… Я разместил сообщение на одном из популярных ресурсов… Покупатель нашелся достаточно быстро.*
  - *Однако вместо изучения особенностей предлагаемого товара его в большей степени интересовал процесс осуществления платежа.*
    - *На мое предложение осуществить его с помощью «перевода на карту по номеру телефона», потенциальный покупатель сослался на некие технические сложности и попросил сбросить реквизиты банковской карты и CVP-код.*
  - *После чего, по понятным причинам (поняв, что это мошенник) я отказался от сделки…».*

ЭКСПЕРТНОЕ МНЕНИЕ

- Экспертами была составлена иерархическая структура современных мошеннических схем.

1. **Предложение перейти по ссылке**
2. **«Дипфейки» в соцсетях от коллег или родственников**
3. **Звонки от сотрудников силовых структур или банков**
4. **Предложения о введении данных банковских карт**
5. **Получение «пуш»-уведомлений от «фейковых» банков**

Источник: Авторские исследования. ИСЭПН ФНИСЦ РАН. 2024-2026 гг.

РЕЗУЛЬТАТЫ ЭКСПЕРТНОГО ОПРОСА

- **Эксперт №3.** Мнение по вопросу, кто должен нести ответственность и защищать граждан от мошенников.
  - *«… Сейчас много создано различных Министерств и ведомств, которые так или иначе занимаются данными вопросами.*
  - *Я думаю все кто работает с личными конфиденциальными данными должны быть включены в данный процесс. Те, кто обладает информационными ресурсами (государственными) и тем более оказывает финансовые услуги...*
  - *Все должны быть озадачены данными вопросами. Сейчас без этого невозможно …».*
- Только 2 эксперта «что-то слышали» про **Концепцию противодействия киберпреступности в России**, но не изучали подробно.

ЭКСПЕРТНОЕ МНЕНИЕ

- В **меньшей степени** злоумышленники стали использовать электронную почту, так как большинство людей имеют хорошо защищенные электронные почтовые ящики.
- В **большей степени** стали использоваться различные мессенджеры и соцсети, так как при работе с ними пользователь в большей степени доверяет представленному контенту.
- **Чаще** используют схемы на маркетплейсах, где, как правило, у пользователя уже имеется «привязка банковской карты».

Источник: Авторские исследования. ИСЭПН ФНИСЦ РАН. 2024-2026 гг.

ИСЭПН
© КРОШИЛИН С.В.
ИНСТИТУТ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ ПРОБЛЕМ НАРОДОНАСЕЛЕНИЯ им. Н.М. Римашевской ФЕДЕРАЛЬНОГО НАУЧНОГО ИССЛЕДОВАТЕЛЬСКОГО СОЦИОЛОГИЧЕСКОГО ЦЕНТРА РОССИЙСКОЙ АКАДЕМИИ НАУК

III МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ВОПРОСЫ ПУБЛИЧНОГО УПРАВЛЕНИЯ, ЭКОНОМИКИ, ПРАВА В СОВРЕМЕННЫХ ГЕОПОЛИТИЧЕСКИХ УСЛОВИЯХ»
28 марта 2026 г., Россия, г. Калининград
КИУ

СОВРЕМЕННОЕ НАСЕЛЕНИЕ и КИБЕР-ОПАСНОСТИ – ТРЕНДЫ МИНИМИЗАЦИИ РИСКОВ

СПАСИБО ЗА ВНИМАНИЕ !!!

ВОПРОСЫ ???

КРОШИЛИН
Сергей Викторович

Кандидат технических наук, доцент,
Ведущий научный сотрудник Лаборатории исследования поведенческой экономики
ИНСТИТУТА СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ ПРОБЛЕМ НАРОДОНАСЕЛЕНИЯ им. Н.М. Римашевской ФНИСЦ РАН

Центр РАН
ИСЭПН