КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

Единый день информирования населения

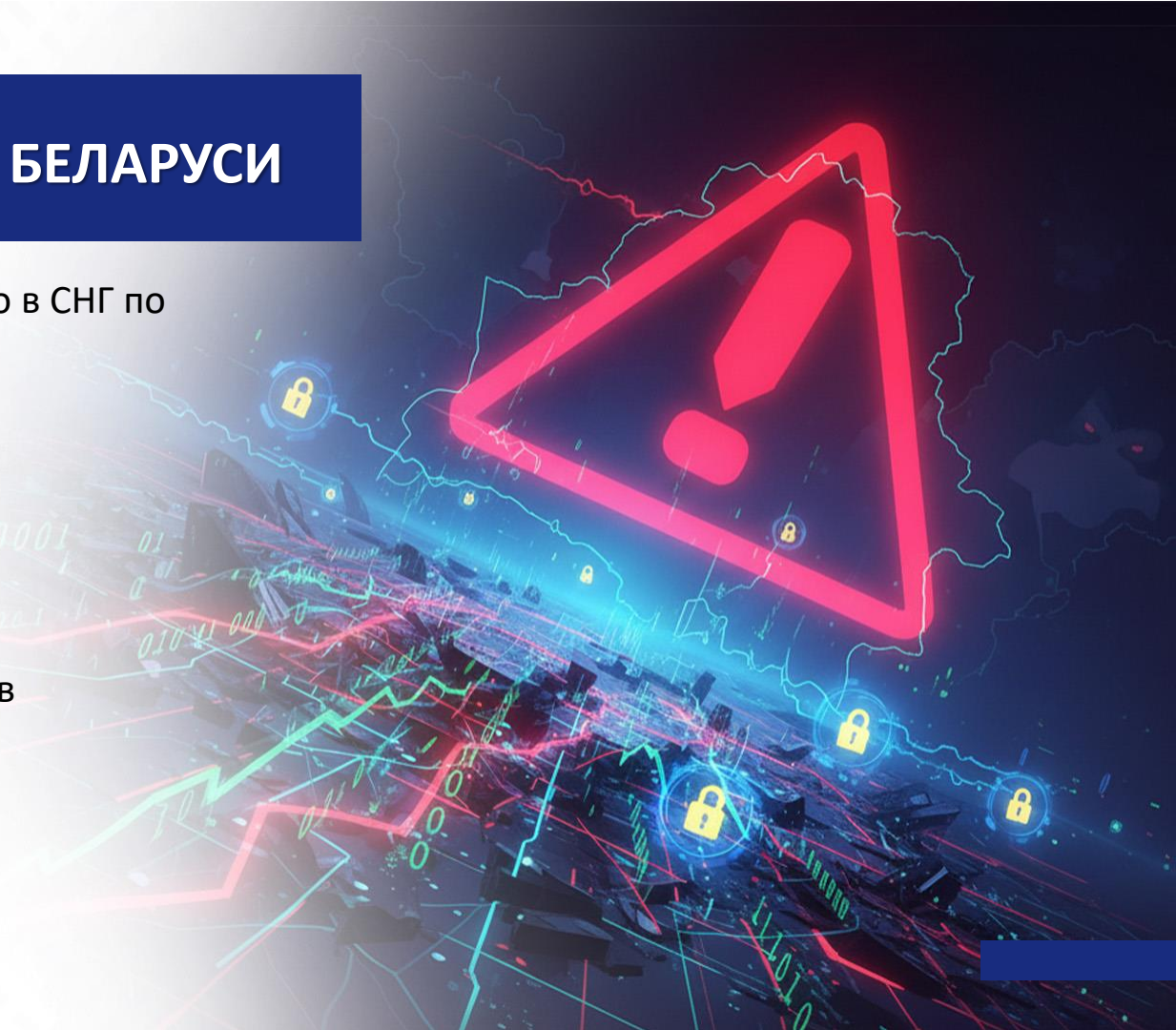
ноябрь 2025 г.

РОСТ КИБЕРАТАК В БЕЛАРУСИ

- **Позиция Беларуси:** 3-е место в СНГ по количеству кибератак

- **ОСНОВНЫЕ ЦЕЛИ АТАК:**
  Госсектор – 22%
  Промышленность – 14%
  Финансы – 11%

- **ПОСЛЕДСТВИЯ:**
  Утечка данных – 57% случаев
  Нарушение работы – 16%
  Финансовые потери – 8%



ПОРТРЕТ ЖЕРТВЫ МОШЕННИЧЕСТВА

Женщины

Телефонные мошенники — 77,9%

Обман в сфере услуг — 65,6%

Мужчины

Мошенничество на сайтах знакомств — 84,8%

Возраст

50+: телефонное мошенничество, «помощь родственникам»

До 30 лет: псевдо-инвестиции (65,4%), дистанционные сделки с недвижимостью (56,3%)

30-49 лет: ИКТ-мошенничество с договорами (53,1%)

Социальный статус:

безработные чаще попадают в инвестиционные ловушки (46,2%)

ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫЕ В СТРАНЕ

- звонки от имени банка, сотрудника МВД, КГБ и иных государственных органов
- фишинговые SMS-сообщения и письма
- мошенничества в социальных сетях и мессенджерах
- мошенничества при онлайн-покупках на площадках по продаже товаров
- фейковые интернет-магазины
- мошенничества под видом государственных органов
- финансовые пирамиды и инвестиционные мошенничества
- вымогательство на интимной почве

АЗБУКА
ЦИФРОВОЙ
БЕЗОПАСНОСТИ

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

- **Целевой фишинг без ошибок:** персонализированные и грамматически безупречные рассылки, обходящие главный маркер угрозы.
- **Мошенничество через Deepfake:** генерация видео и голоса руководства для санкционирования незаконных финансовых операций.
- **ИИ-боты для социальной инженерии:** ведение осмысленных диалогов для выманивания конфиденциальной информации.

«Неуправляемая гонка в этой сфере превращает его** (прим. – искусственный интеллект) **из полезного ресурса в оружие. В перспективе – массового поражения.»

Президент Республики Беларусь А.Г. Лукашенко, III Минская международная конференция по евразийской безопасности, 28 октября 2025 г.

БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ — ЭТО НЕ ЗАПРЕТЫ, А ДОВЕРИЕ И ПРАВИЛА

Выстраивайте открытые отношения: ребенок должен знать, что может рассказать вам о любой проблеме без страха наказания.

Установите четкие границы: согласуйте время онлайн, разрешенные сайты и приложения.

Используйте технические средства: родительский контроль и общие аккаунты для младших детей.

РАСПРОСТРАНЕННЫЕ СХЕМЫ КИБЕРПРЕСТУПЛЕНИЙ ПРОТИВ ДЕТЕЙ

«Бесплатные» подарки

Цель: заманить на фишинговую страницу и украсть данные банковской карты.

Фейковые запросы от «друзей»

Цель: воспользоваться доверием и выманить деньги через взломанный аккаунт.

Груминг

Цель: выдавая себя за сверстника, войти в доверие, чтобы манипулировать и выпрашивать интимные фото/видео.

Сексторшен

Цель: шантажировать ребенка с помощью полученных интимных материалов.

Кибербуллинг

Цель: унизить и травмировать психологически через травлю в группах и личных сообщениях.

Деструктивный контент

Цель: вовлечь в опасные сообщества, пропагандирующие суицид, насилие и экстремизм.

4 КЛЮЧЕВЫХ ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ДЕТЕЙ И ПОДРОСТКОВ

1 **Храни личное в тайне**
Не публикуй адрес, школу, геометки, данные документов и карт, планы семьи.

2 **Помни алгоритм «СТОП-СПРОСИ-РАССКАЖИ»**
СТОП, если что-то настораживает. СПРОСИ у родителей, если непонятно. РАССКАЖИ взрослым о любой угрозе или дискомфорте.

3 **Контролируй круг общения**
Добавляй в друзья только тех, кого знаешь лично. Настрой приватность профиля.

4 **Включай критическое мышление**
Не переходи по сомнительным ссылкам. Не верь слишком «выгодным» предложениям.

Родители, научите детей пользоваться Интернетом правильно!

Правила безопасного поведения

Берегите аккаунты от аферистов!

АКАДЕМИЯ УПРАВЛЕНИЯ
ПРИ ПРЕЗИДЕНТЕ
РЕСПУБЛИКИ БЕЛАРУСЬ