ИНФОРМАЦИЯ О ПРОФИЛАКТИКЕ ПРАВОНАРУШЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, IT – ПРЕСТУПЛЕНИЙ И КИБЕРПРЕСТУПЛЕНИЙ

В 2025 году в России зафиксировано 675 тыс. IT-преступлений, что на 11,8% меньше, чем в 2024 году. При этом суммарный ущерб от дистанционных мошенничеств вырос на 16% и составил почти 120 млрд рублей за первое полугодие. В общем массиве преступности на IT-преступления приходится ~38% , а почти половина из них — кибермошенничество, зафиксированное в 350 тыс. случаев.

Тенденция такова, что при общем снижении числа зарегистрированных киберпреступлений, их раскрываемость улучшилась — количество нераскрытых дел сократилось на 13.5% до 494.3 тыс.

Основные виды и способы совершения преступлений

Киберпреступления можно условно разделить на три категории:

· Деятельность, направленная на ИТ-инфраструктуру (компьютеры, серверы, сети);

· Преступления, совершаемые с использованием ИТ (мошенничество, кражи);

· Преступления, связанные с содержанием данных (нарушение авторских прав, распространение запрещенной информации).

На практике в России наиболее распространены:

№ Категория Доля / Примеры

1. Хищения и мошенничество 63.4% всех преступлений (397.4 тыс. случаев)
2. Незаконный оборот наркотиков через интернет ~17.4%, рост на 28.5% за год
3. Неправомерный доступ к компьютерной информации ст. 272 УК РФ
4. Распространение вредоносного ПО вымогательство, шпионаж
5. Вовлечение несовершеннолетних склонение к диверсиям, дропперству.

Все чаще злоумышленники комбинируют технологии с методами социальной инженерии, когда жертва добровольно переводит сбережения под психологическим давлением. Например, аферисты звонят с номеров, похожих на официальные (+900 вместо 900 Сбера), представляются сотрудниками ФСБ или банков, убеждают перевести деньги на «безопасные счета». Главным инструментом также остаются мессенджеры — через них совершено 244.6 тыс. преступлений (+17.5%).

Индивидуальные меры профилактики для граждан

Главный принцип защиты — соблюдение базовой информационной гигиены и развитие критического мышления. Ниже представлены правила, которые помогут снизить риски:

1. Не сообщайте личные данные посторонним: реквизиты карт, паспортную информацию, коды из СМС, пароли от Госуслуг и банков.
2. Прерывайте подозрительный разговор: если звонят «из банка», «полиции» или «ФСБ» — положите трубку и сами перезвоните в организацию по официальному номеру.
3. Не переходите по подозрительным ссылкам: проверяйте адреса сайтов, не переводите предоплату незнакомым продавцам при покупках.
4. Используйте сложные пароли и двухфакторную аутентификацию, регулярно обновляйте антивирусное ПО.
5. Не доверяйте слишком выгодным предложениям: «легкий заработок», выигрыш в лотерею, звонки от «работодателя» с просьбой перевести деньги.
6. Сомневаетесь — посоветуйтесь с близкими: многие жертвы попадают под влияние из-за изоляции, когда мошенник требует говорить в одиночестве.

Будьте особенно бдительны в отношении звонков и сообщений от неизвестных номеров — ни один настоящий сотрудник банка или правоохранительных органов никогда не запрашивает по телефону конфиденциальные данные или переводы.

Государственные программы и законодательные меры

1) Концепция государственной системы противодействия киберпреступлениям (утверждена Правительством РФ 20 августа 2025 г.)

· Предусматривает комплексный план из 30 первоочередных мер до 2028 года.
· Включает создание единого реестра официальных сайтов интернет-магазинов для борьбы с фишинговыми двойниками.
· Обязует операторов связи и IT-компании информировать правоохранителей о признаках киберпреступлений.
· Планируется внедрение модулей обязательного оповещения о мошенничестве во все значимые мобильные приложения (госуслуги, банки, соцсети).
· Разрабатываются алгоритмы выявления использования искусственного интеллекта в киберпреступлениях.

2) Законопроект «Единой России» о профилактике киберпреступлений (март 2026 г.)

· Вносит мероприятия по кибербезопасности в перечень основных направлений профилактики правонарушений.

· Предусматривает комплексные программы в регионах с уроками в школах, колледжах, вузах, а также информирование через МФЦ, Госуслуги и национальные мессенджеры.

Если вы столкнулись с киберпреступлением, необходимо незамедлительно обратиться в отдел полиции (тел. **02** или **102**) и сохранить все возможные доказательства: переписку, логи звонков, скриншоты.