Информационно-справочные материалы по вопросам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Когда мы говорим о глобальном явлении киберпреступности, то такого понятия, как «рекордная сумма» не существует, потому что это не один случай, а миллионы инцидентов и ключевым аспектом является именно совокупный годовой ущерб и средние показатели, которые складываются из множества факторов.

Таким образом, анализируя киберпреступность в России, мы должны смотреть не на мифический «рекорд», а на динамику трех показателей:

- совокупный годовой ущерб;
- количество зарегистрированных преступлений;
- среднюю сумму ущерба на преступление.

Отвечая на поставленные вопросы можно отметить, что киберпреступления распространены во всех без исключения странах. И в каждой стране растет их количество и суммы причиненного ущерба.

Так, в 2024 году Международной группа исследований под руководством Оксфордского университета (Великобритания) определены страны, имеющие самый высокий индекс кибепреступности, такие как: Украина (36,4), Китай (27,86), США (25,01), Нигерия (21,8), Румыния (14,83), Северная Корея (10,61), Великобритания (9,01), Бразилия (8,03), Индия (6,13).

Из-за тотальной цифровизации во всех аспектах жизни, таких как финансы, бизнес, госуправление, по данным Group-IB, общий ущерб от киберпреступлений в мире исчисляется триллионами долларов ежегодно и продолжает расти двузначными процентами в год.

В России суммы похищенных денежных средств также растут. В **2022 году - 91 млрд**, в **2023 году – 156 млрд**, в **2024 году – более 192 млрд** рублей, за **10 месяцев 2025 года** – 158, 6 млрд рублей (в аналогичном периоде прошлого года - 150 млрд). То есть за **три года** население и государство лишилось **не менее 387 млрд** рублей.

Вместе с тем, принимаемые в текущем году правоохранительными органами и банковским сектором правовые и технологические меры позволили добиться определенной положительной динамики. **Прирост киберпреступлений в России сократился[1], что может позволить абсолютному ущербу расти более медленными темпами, чем ранее.**

При этом рост или падение в России «средней суммы» ущерба[2], ***сам по себе не говорит об успехе или провале борьбы с киберпреступностью.***

---

[1] По итогам 10 месяцев 2025 года зафиксировано снижение на 9,5% количества регистрируемых преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий.

[2] В случаях мошенничеств с помощью СМС или звонков от «служб безопасности банка», фиктивных выигрышей «средняя сумма» ущерба с жертвы составляет от 1 000 рублей до 100 000 рублей, при несанкционированных списаниях с банковского счета – несколько тысяч на операцию,

Нелепость и абсурдность сценариев это не признак глупости мошенников, а их тактическое оружие.

Не нужно искать в их методах сложной магии или гипноза. Вся их сила – в эксплуатации простых, примитивных, но безотказно работающих кнопок в нашей психике.

Поэтому сценарии, используемые мошенниками, позволяют вводить в заблуждение даже тех, кто по роду своей деятельности прекрасно осведомлен о происках аферистов. Это и молодежь, которая хорошо ориентируется в интернет-пространстве, и даже руководители, государственные служащие учреждений и организаций, работники банков и операторов связи, которые в свою очередь более осведомлены о способах мошенничества.

Значительную роль здесь играет низкая финансовая и цифровая грамотность населения. Кроме того в периоды кризисов и неопределенности люди становятся более тревожными и подверженными панике, чем активно пользуются злоумышленники.

Таким образом, самой современной и эффективной стратегией кибербезопасности в эпоху искусственного интеллекта и дипфейков является принцип нулевого доверия. Если говорить коротко, его суть можно выразить одной фразой «Никогда не доверяй, всегда проверяй».

Это полная противоположность устаревшему подходу «Доверяй, но проверяй», который и послужил причиной совершения злоумышленниками в 2024 и 2025 годах **2-х *крупных дистанционных хищений,*** *а именно:*

1. В 2025 году у жительницы одного из крупных областных центров России похищены денежные средства в особо крупном размере. Общая сумма ущерба составила свыше 400 млн рублей (в рублях, долларах и евро), что можно назвать «рекордной» суммой.

Злоумышленники, выдававшие себя за сотрудников силовых ведомств, тщательно готовились к преступлению: собирали о жертве информацию из открытых источников, убедили ее участвовать в спецоперации по поимке опасных преступников в качестве «приманки». Для правдоподобности они приобрели дорогие костюмы, арендовали автомобили и частный дом, привлекли курьеров и использовали документы, содержащие недостоверные сведения о личности.

По данному факту к уголовной ответственности ***в составе преступного сообщества*** привлекаются более 5 лиц, в отношении которых избраны меры пресечений в виде заключения под стражу. В ходе следствия у обвиняемых изъято более 7 млн рублей, 40 тыс. долларов и 35 тыс. евро, на указанные ценности наложены аресты.

2. В 2024 году телефонные злоумышленники обманом лишили квартиры известную народную артистку России, причинив имущественный ущерб в особо крупном размере более 200 млн рублей.

В обоих случаях, которые в настоящее время кажутся со стороны нелепыми, поскольку мошенники использовали примитивные сценарии, денежные средства жертвы передавали так называемым «курьерам» для их дальнейшего перевода на «безопасный счет».

Название более детальной информации и конкретных сумм ущерба в интересах потерпевших полагаем некорректным, поскольку это может нарушать их право на конфиденциальность и защиту личных данных.

Несмотря на многообразие мошеннических схем, базовые принципы финансовой самообороны неизменны.

Подводя итог, главные правила остаются все те же:

1. Получив неожиданную просьбу или указание перевести или передать незнакомому лицу деньги, тем более в ходе телефонного разговора, необходимо на 100% понимать, что это уловки мошенников, и положить трубку.

2. Настоящие сотрудники банков или государственных органов никогда не будут запрашивать по телефону или в смс данные ваших карт, пароли или коды подтверждения.

3. Для проверки информации перезвоните в банк или правоохранительные по официальным номерам с их сайтов.

В случае, если гражданин своевременно обращается с заявлением о совершении хищения дистанционным способом, сотрудники органов внутренних дел совместно с банками вовремя реагируют и становится гораздо больше шансов арестовать счета злоумышленников.

Кроме того, Президентом Российской Федерации подписан Федеральный закон, который ***наделил следователей и дознавателей правом без судебного решения приостанавливать расходные операции с денежными средствами, находящимися на счетах,*** использовавшихся в преступной деятельности. Указанная норма вступила в законную силу ***с 1 сентября текущего года.***

Следственный департамент МВД России