А Н А Л И З

динамики основных показателей, характеризующих преступность, связанную с использованием (применением) информационно – коммуникационных технологий (далее IT - преступления)

(по данным Департамента региональной безопасности ХМАО-Югры и

УМВД России по ХМАО-Югре)

Удельная доля IT – преступлений в Ханты-Мансийском автономном округе–Югре (далее – автономный округ) на протяжении последних нескольких лет превышает одну треть в общем массиве зарегистрированных преступлений (в 2020 году – 41,2%, в 2021 году – 38,4%, в 2022 году – 35,5%, за 7 месяцев 2023 года – 43,7%). По итогам 9 месяцев 2024 года прирост числа совершенных IT–хищений составил 22,4% (увеличение с 4530 до 5546 фактов). Число потерпевших от IT–хищений увеличилось на 25,8% (4799 человек).

Удельный вес IT–хищений в общем количестве всех совершенных преступлений в автономном округе достиг 32,8% (каждое третье преступление). Общий материальный ущерб от дистанционных хищений превысил 2 миллиарда рублей.

В среднем за одни сутки в автономном округе совершается 20 IT–хищений (600 фактов за месяц), ущерб от которых составляет более 7 миллионов рублей (более 220 миллионов рублей в месяц).

Результаты опроса правоохранительными органами потерпевших граждан свидетельствуют о том, что более90% пострадавших были осведомлены о потенциальной угрозе преступных посягательств и основных схемах, применяемых преступниками для обмана граждан.

Мошенники совершенствуют методы и схемы обмана граждан, в том числе используя технологии социальной инженерии. При этом жертвами мошенников становятся все категории граждан независимо от возраста, образования, социального статуса и имущественного положения.

Из дистанционных краж и мошенничеств каждое третье преступление совершено по схеме – «звонок сотрудника банка, правоохранительных органов или государственных структур».

При совершении сделок на торговых площадках (Авито, Юла, ВКонтакте и др.) совершено 27% дистанционных краж и мошенничеств; в сфере микрокредитования – 13%; по схеме «инвестирование или торги на фондовых площадках, биржах» – 12%; по схеме «просьбы о финансовой помощи или родственник в беде» – 5%.

Значительная часть переданных мошенникам денежных средств являются заемными средствами, полученными потерпевшими при заключении кредитного договора лично в офисе банка.

В значительном случае жертвами преступлений становятся наиболее законопослушные граждане, которые готовы «оказать содействие правоохранительным органам в выявлении и изобличении преступников».

Мошенники применяют методы психологического давления на потерпевших, подчеркивая угрозу потери накопительных денежных средств, необходимости из «защиты» путем перевода на «безопасные» счета.

Представляясь сотрудниками правоохранительных органов и банковских учреждений, мошенники обращаются к чувствам гражданской ответственности граждан, необходимости оказания содействия правоохранительным органам. При выражении сомнений со стороны граждан прибегают к угрозам привлечения к ответственности за соучастие в совершении преступления.

В общении с гражданами злоумышленники подчеркивают необходимость неразглашения содержания телефонного разговора под угрозой привлечения к ответственности.

Значительные финансовые потери граждан в результате совершения дистанционных краж и мошенничеств потенциально содержат социальный риск негативной оценки населением способности правоохранительных органов и органов власти противодействовать и пресекать данные преступления.

В настоящее время основной рекомендацией безопасного поведения является безоговорочное и безусловное прекращение дистанционного общения (по телефону, в мессенджерах, социальных сетях) если разговор с незнакомым собеседником переходит к необходимости передачи персональных данных, сохранению, преумножению или передаче денежных средств, угрозам привлечения к ответственности за невыполнение требований.

Управлением по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России информация о применяемых новых схемах мошенничества размещается в телеграмм-канале «Вестник Киберполиции России»: https://t.me/cyberpolice\_rus/