Бюллетень по актуальным схемам мошенничества

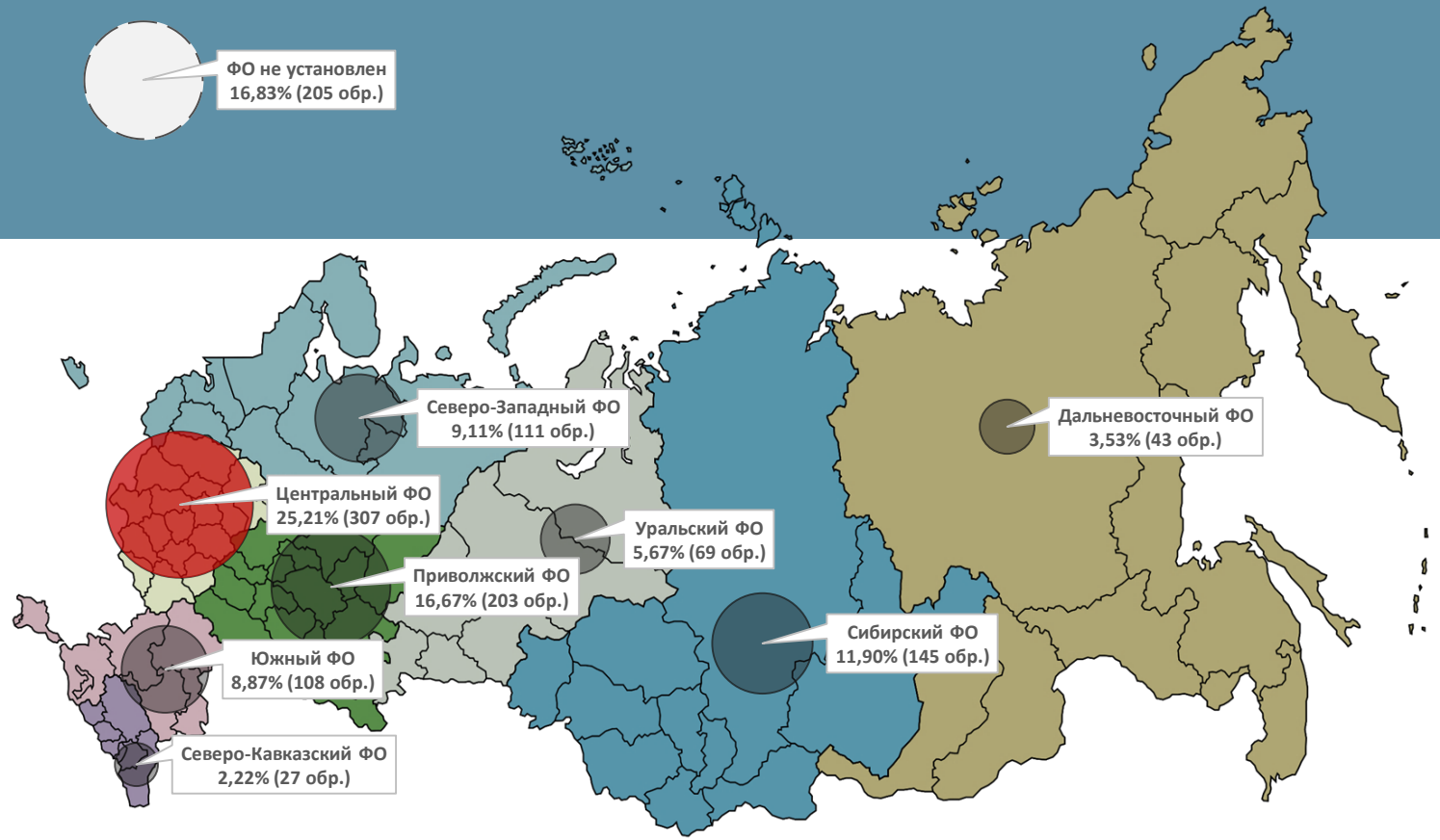
Департамент информационной безопасности

февраль 2023

Сведения о поступивших в Банк России обращениях граждан по вопросам мошенничества.

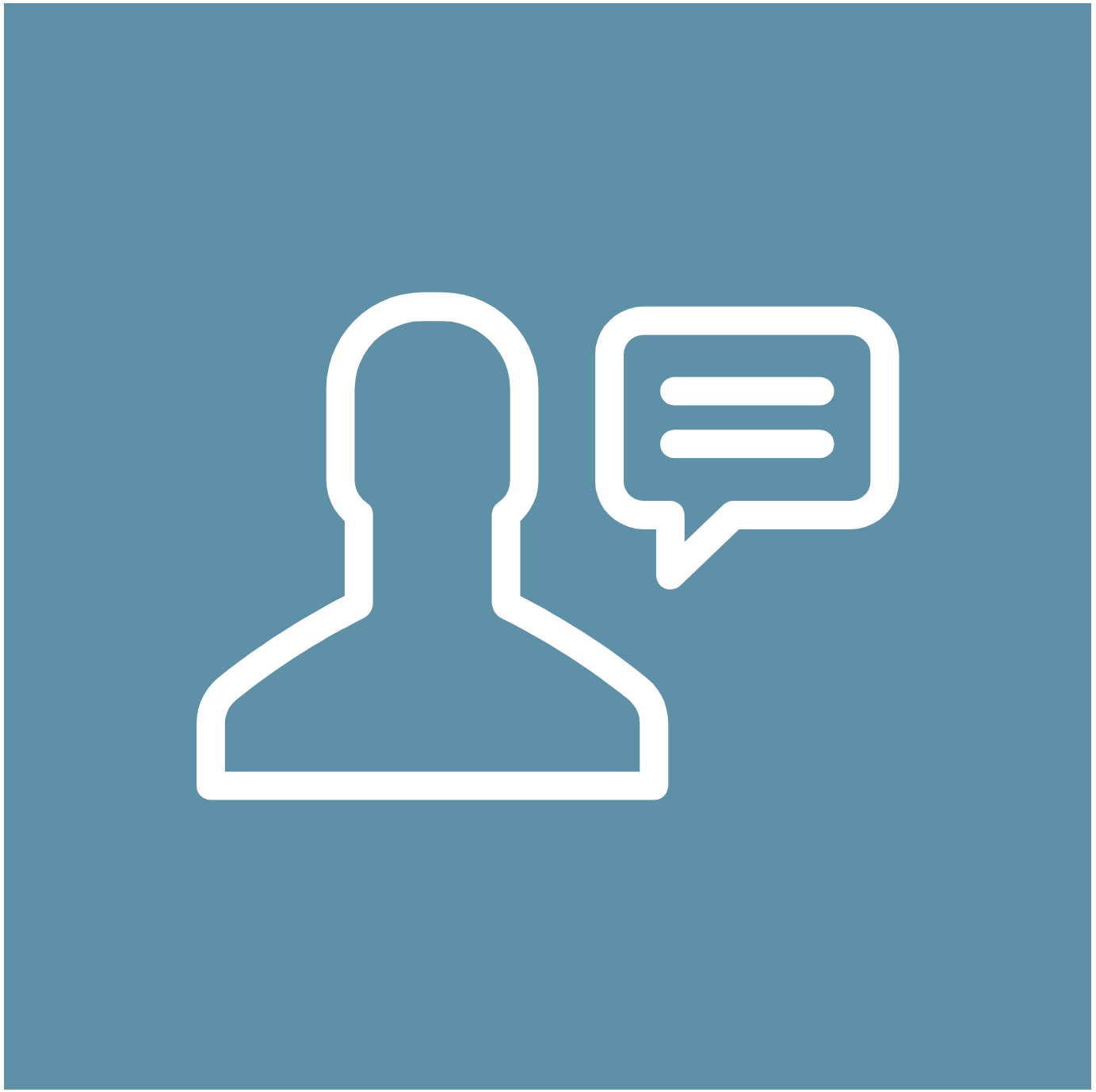
Департамент информационной безопасности Банка Росси на постоянной основе осуществляет анализ данных по операциям переводов денежных средств без согласия клиентов кредитных организаций. Для проведения анализа были использованы данные из обращений граждан. В пределах Российской Федерации наибольшее число обращений (307) зарегистрировано в Центральном федеральном округе, наименьшее – в Северо-Кавказском федеральном округе (27).

Распределение по федеральным округам



Актуальные схемы мошенничества

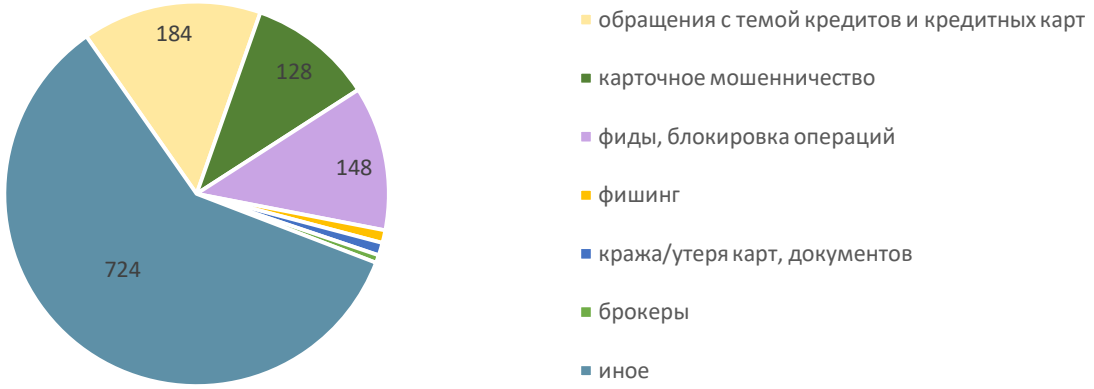
(анализ данных из обращений граждан в Банк России)



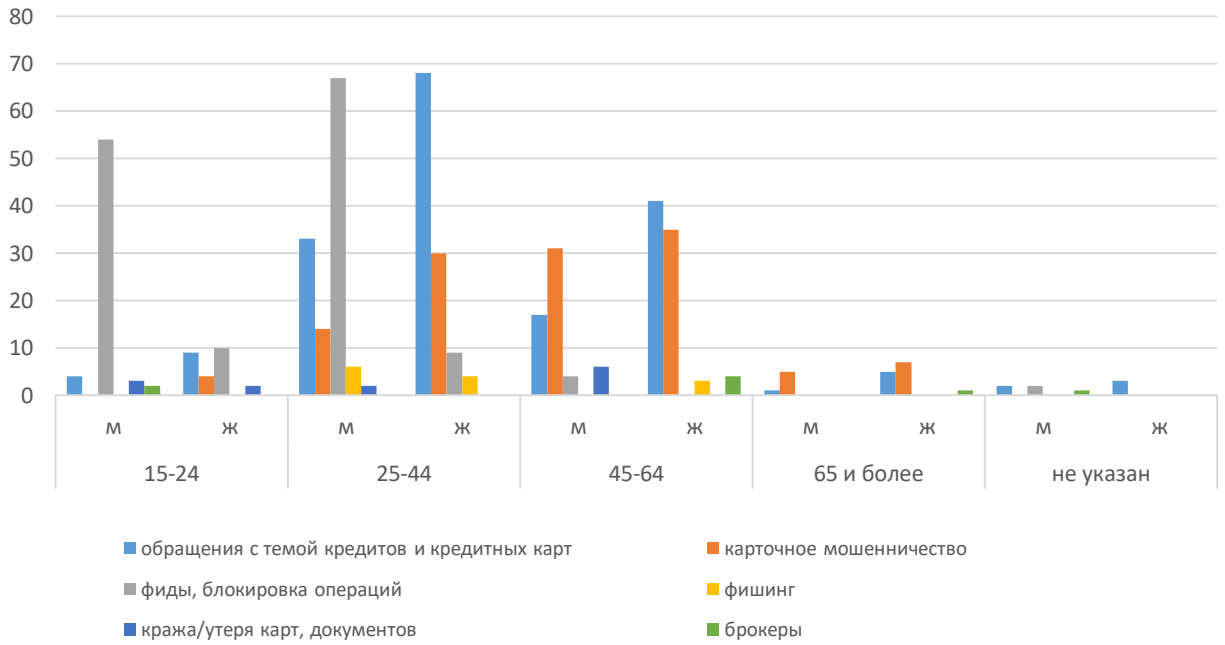
Согласно анализу данных из обращений граждан в Банк России за период с 01.02.2023 по 28.02.2023, преобладающей является схема мошенничества, направленная на хищение денежных средств граждан путем мошенничества с кредитами и кредитными картами:

- Злоумышленники посредством телефонного звонка жертве представляются уполномоченными лицами МВД, Банка России и службы безопасности банка.
- Убеждают жертву в том, что необходимо сообщить код для входа в приложение банка с целью улучшения безопасности/проведения технических работ.
- Получив доступ к личному кабинету жертвы, мошенник переводит средства с карт жертвы.
- Вывод средств мошенниками.

Распределение обращений по темам

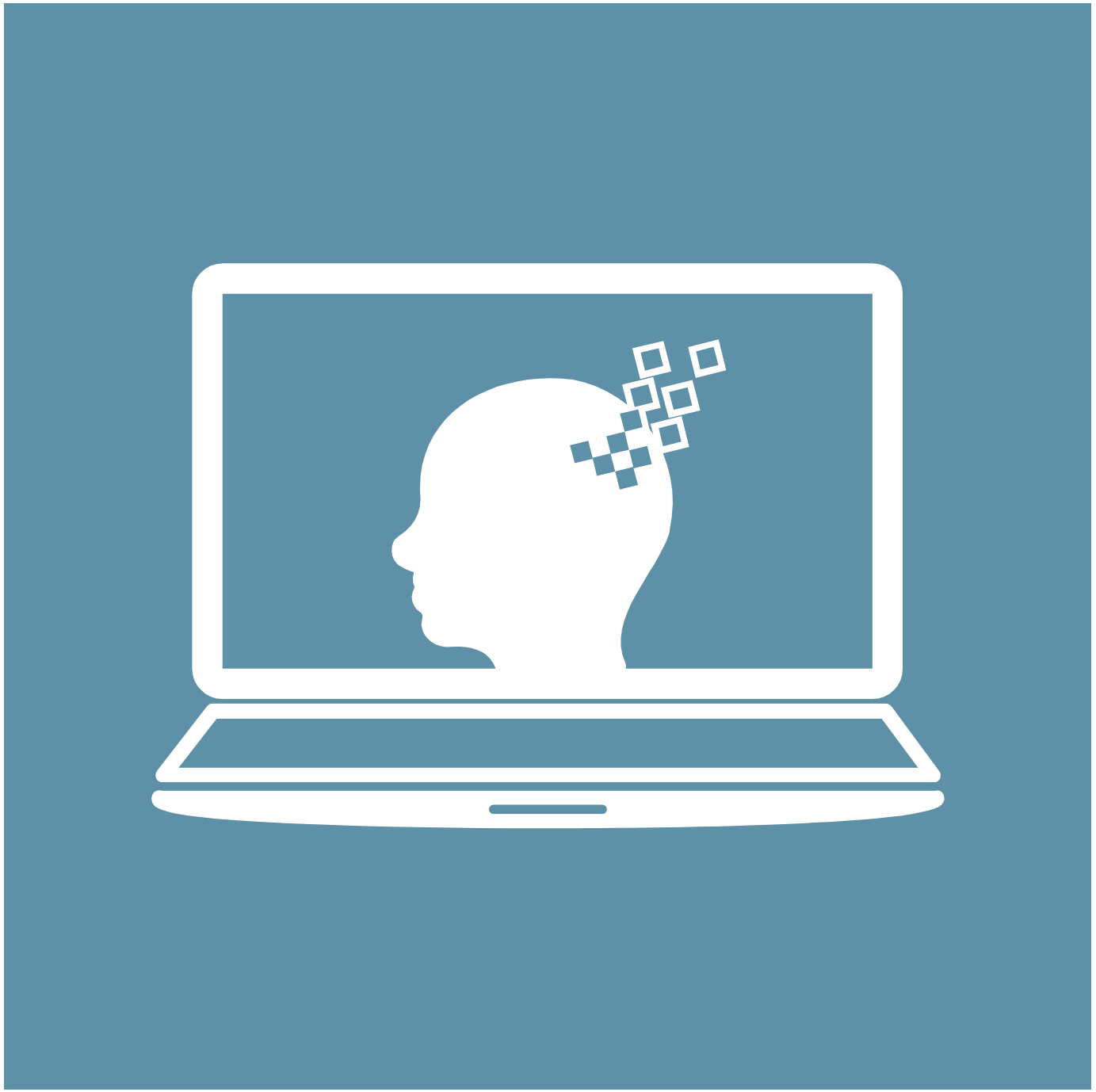


Данные по обращениям граждан в разрезе пола и возраста

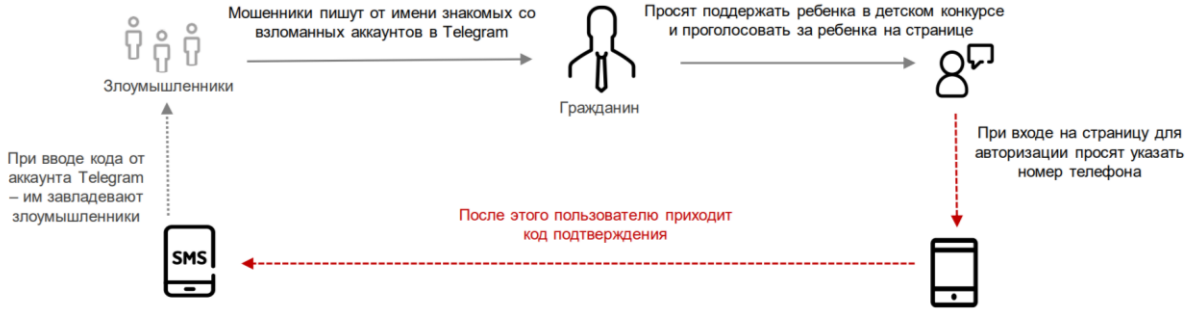


Актуальные схемы мошенничества

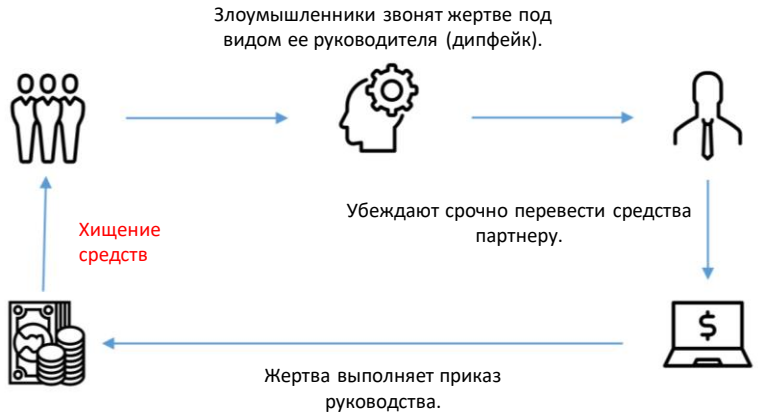
(анализ сети Интернет)



- Жертвы получают сообщение якобы от знакомого человека с просьбой поддержать ребенка (крестницу, племянника) в детском конкурсе рисунков и проголосовать за работу на странице "интернет-соревнования“;
- При входе на страницу фейкового конкурса для авторизации пользователя просят указать номер телефона;
- После этого пользователю приходит код подтверждения;
- Если ввести код авторизации от аккаунта Telegram на фишинговой странице конкурса, то им завладеют злоумышленники.



- Злоумышленники звонят жертве и убеждают сменить номер телефона, на который приходят уведомления от банка, или добавить для этой услуги дополнительный номер.
- После получения доступа к личному кабинету, мошенники списывают средства со счетов жертвы.



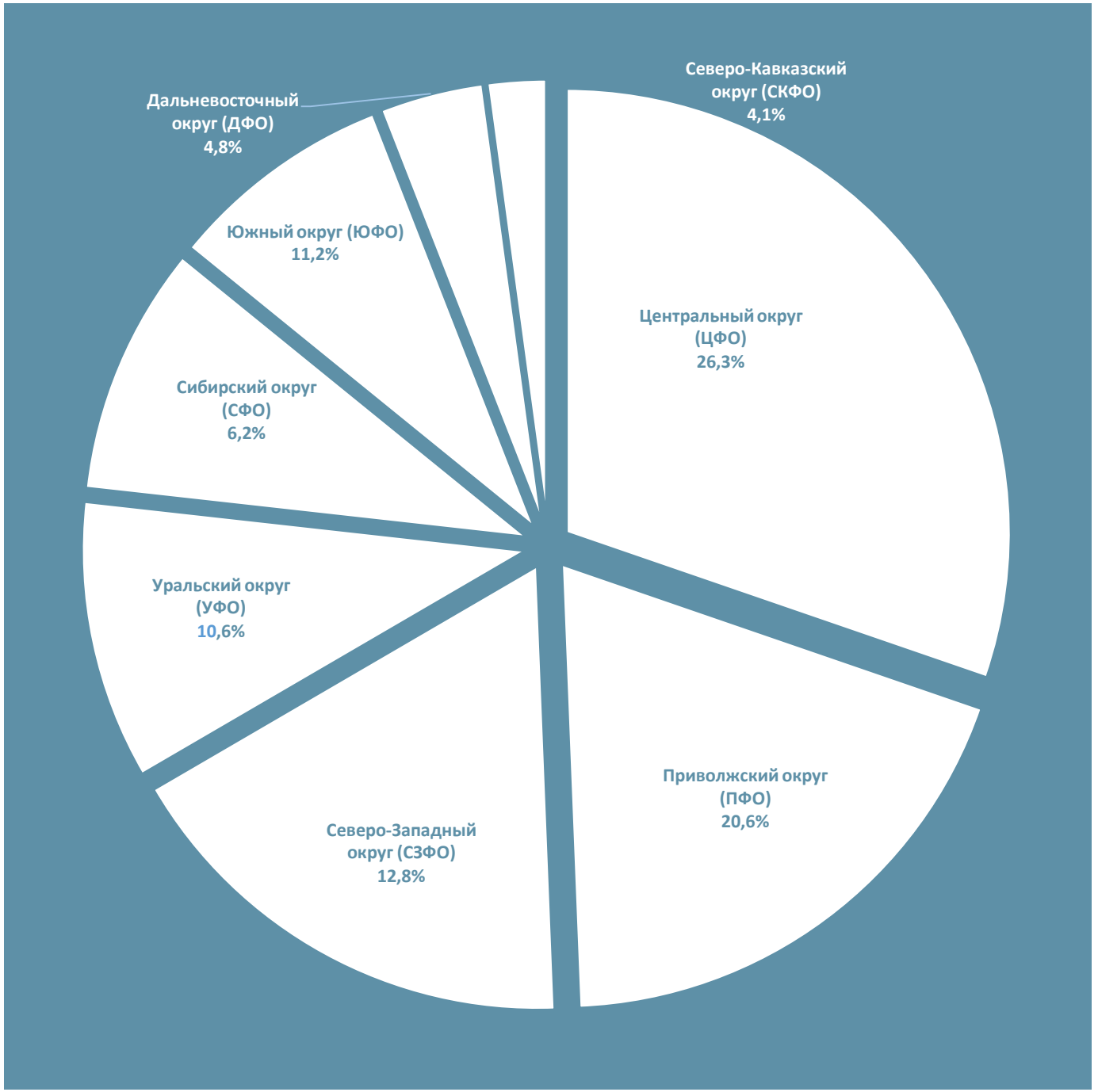
- Злоумышленники звонят жертве под видом ее руководителя (дипфейк).
- Убеждают срочно перевести средства партнеру.
- Жертва выполняет приказ руководства.

- Мошенники звонят от имени Управления Роспотребнадзора руководителям различных организаций;
- Мошенники сообщают, что собирают денежные средства на поддержку военнослужащих ЧВК «Вагнер»;
- Мошенники сообщают, что денежные средства необходимо перевести на «карту сбора помощи».

Статистические данные. Сообщения содержащие темы мошенничества.

(анализ сети Интернет)

Центральный округ (ЦФО)	1 954
Приволжский округ (ПФО)	1 548
Северо-Западный округ (СЗФО)	942
Уральский округ (УФО)	772
Сибирский округ (СФО)	464
Южный округ (ЮФО)	848
Дальневосточный округ (ДФО)	346
Северо-Кавказский округ (СКФО)	298



Советы

Телефонное мошенничество

• Будьте внимательны и не доверяйте неизвестным лицам, пусть даже говорят они при этом очень убедительно.
• Сотрудники банков никогда не запрашивают сведения по остаткам счетов граждан, личные и финансовые данные.
• Позвоните в банк, от имени которого Вам звонят, а также в банк, клиентом которого Вы являетесь (по номерам телефонов, указанным оборотной стороне карты или на официальных сайтах).
• Никогда и никому не сообщайте личные данные, а также полные реквизиты карты, пароли и коды от банка.

Фишинг

• Установите антивирус и регулярно обновляйте его.

• Не переходите по неизвестным ссылкам.

• Не заходите на подозрительные сайты.

• Никогда и никому не сообщайте личные данные, а также полные реквизиты карты, пароли и коды от банка.

• Сохраняйте в закладках нужные адреса сайтов. • Используйте для оплаты покупок в интернете отдельную карту, кладите на нее нужную сумму денег