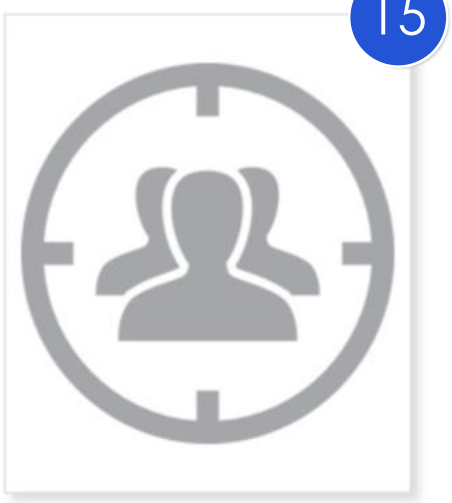
ГАЗПРОМБАНК

Практические подходы к построению отказоустойчивых ИБ-решений в финтехе

2025

itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

ПЛЕШКОВ АЛЕКСЕЙ



Groteck Business Media

АИС АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Коммерсантъ

CNews

Habr

КОМСОМОЛЬСКАЯ ПРАВДА

Смещение фокуса кибератак на финтех

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

от 2 ноября 2024 года

БАНК РОССИИ УТВЕРДИЛ ПЕРЕЧЕНЬ

СИСТЕМНО ЗНАЧИМЫХ КРЕДИТНЫХ ОРГАНИЗАЦИЙ

Банк России в соответствии с Указанием от 13.04.2021 N 5778-У "О методике определения системно значимых кредитных организаций" утвердил перечень системно значимых кредитных организаций. На их долю приходится около 79% совокупных активов российского банковского сектора:

N п/п	Наименование кредитной организации	Рег. N
1	АО ЮниКредит Банк	1
2	Банк ГПБ (АО)	354
3	ПАО "Совкомбанк"	963
4	Банк ВТБ (ПАО)	1000
5	АО "АЛЬФА-БАНК"	1326

13

Банков


UniCredit Bank
ВТБ
МОСКОВСКИЙ КРЕДИТНЫЙ БАНК
Т БАНК
ГАЗПРОМБАНК
Альфа-Банк
открытие
БАНК
ПСБ
Райффайзен БАНК
СОВКОМБАНК
СБЕР БАНК
РОСБАНК
РСХБ
РоссельхозБанк

Основные виды кибератак на банки в 2024 году

ГАЗПРОМБАНК

- Реализация атаки типа «отказ в обслуживании»
- Компрометация аутентификационных/учетных данных
- Использование вредоносного программного обеспечения
- Фишинг и социальная инженерия
- Поиск и эксплуатация уязвимостей в инфраструктуре

75+%

ВАЖНО: эффективно реализовывать в 2025 году в банках РФ комплекс мероприятий по минимизации угрозы успешной реализации кибератак с учетом переходящих тенденций

Тенденции 2025 года

- рост кибератак на цепочки поставок (supply chain)
- смещение фокуса при выборе цели с крупных компаний на малый и средний бизнес (MSB)
- рост кибератак с долгосрочным присутствием в инфраструктуре
- маскирование кибератак, использование в сценариях легитимного ПО (antiAV)
- акцент на деструктивное воздействие на инфраструктуру и бизнес-процессы в банках

DDOS атаки на банки H1.2025

1 ТБит/с

ГАЗПРОМБАНК

Цели DDOS в РФ:

- 22,3% - финтех
- 21,0% - IT и телеком
- 20,9% - e-com

Длительность:

со 120 до 23 минут

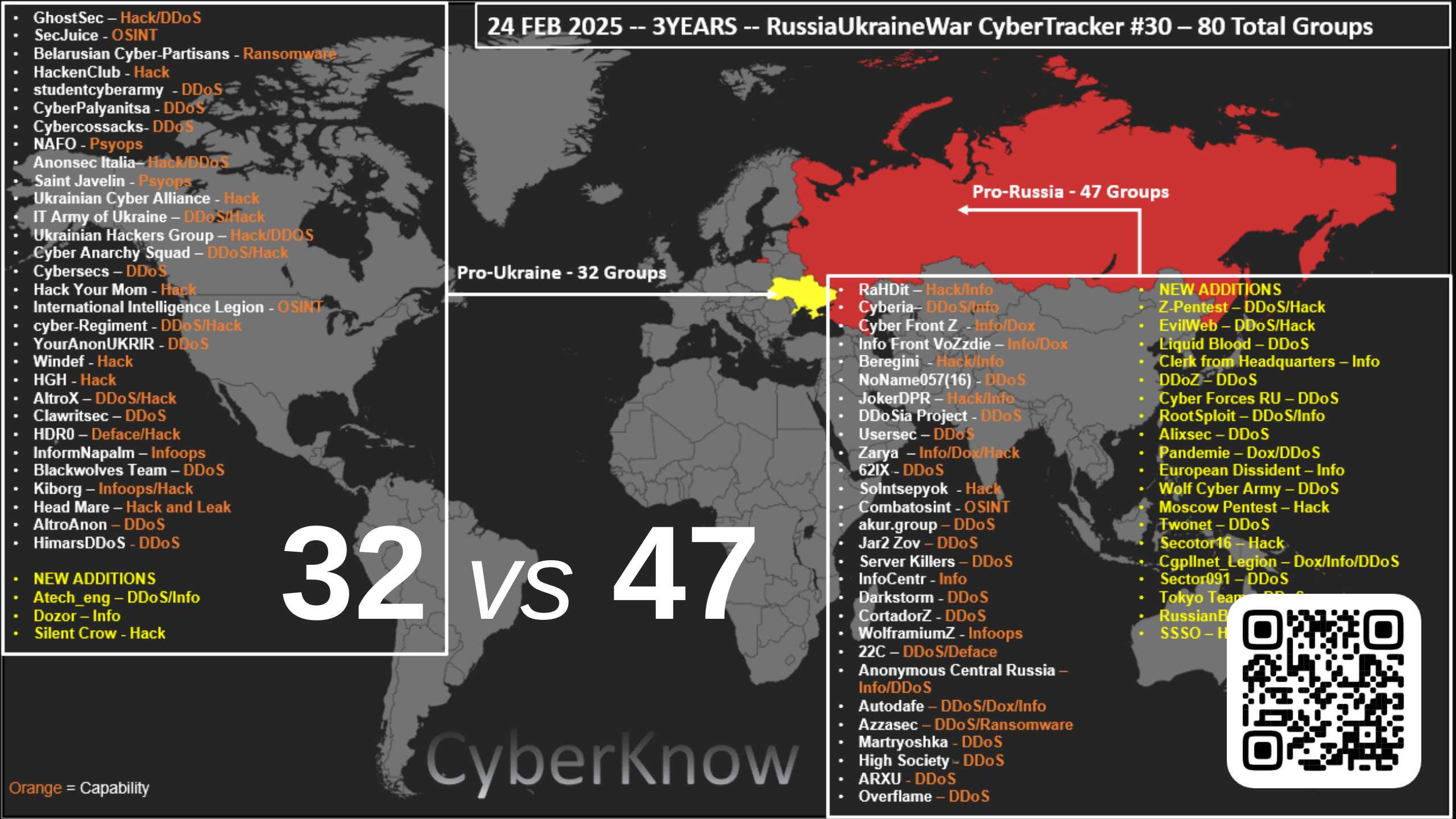
Вектор DDOS:

+58% – L3/L4

+62,6% – L7

+43% – MultyL

24 FEB 2025 -- 3YEARS -- RussiaUkraineWar CyberTracker #30 – 80 Total Groups



- GhostSec – Hack/DDoS
- SecJuice - OSINT
- Belarusian Cyber-Partisans - Ransomware
- HackenClub - Hack
- studentcyberarmy - DDoS
- CyberPalyanitsa - DDoS
- Cybercossacks- DDoS
- NAFO - Psyops
- Anonsec Italia– Hack/DDoS
- Saint Javelin - Psyops
- Ukrainian Cyber Alliance - Hack
- IT Army of Ukraine – DDoS/Hack
- Ukrainian Hackers Group – Hack/DDOS
- Cyber Anarchy Squad – DDoS/Hack
- Cybersecs – DDoS
- Hack Your Mom - Hack
- International Intelligence Legion - OSINT
- cyber-Regiment - DDoS/Hack
- YourAnonUKRIR - DDoS
- Windef - Hack
- HGH - Hack
- AltroX – DDoS/Hack
- Clawritsec – DDoS
- HDR0 – Deface/Hack
- InformNapalm – Infoops
- Blackwolves Team – DDoS
- Kiborg – Infoops/Hack
- Head Mare – Hack and Leak
- AltroAnon – DDoS
- HimarsDDoS - DDoS

- NEW ADDITIONS
- Atech_eng – DDoS/Info
- Dozor – Info
- Silent Crow - Hack

- RaHDit – Hack/Info
- Cyberia– DDoS/Info
- Cyber Front Z - Info/Dox
- Info Front VoZzdie – Info/Dox
- Beregini - Hack/Info
- NoName057(16) - DDoS
- JokerDPR – Hack/Info
- DDoSia Project - DDoS
- Usersec – DDoS
- Zarya – Info/Dox/Hack
- 62IX - DDoS
- SoIntsepyok - Hack
- Combatosint - OSINT
- akur.group – DDoS
- Jar2 Zov – DDoS
- Server Killers – DDoS
- InfoCentr - Info
- Darkstorm - DDoS
- CortadorZ - DDoS
- WolframiumZ - Infoops
- 22C – DDoS/Deface
- Anonymous Central Russia – Info/DDoS
- Autodafe – DDoS/Dox/Info
- Azzasec – DDoS/Ransomware
- Martryoshka - DDoS
- High Society - DDoS
- ARXU - DDoS
- Overflame – DDoS

- NEW ADDITIONS
- Z-Pentest – DDoS/Hack
- EvilWeb – DDoS/Hack
- Liquid Blood – DDoS
- Clerk from Headquarters – Info
- DDoZ – DDoS
- Cyber Forces RU – DDoS
- RootSploit – DDoS/Info
- Alixsec – DDoS
- Pandemie – Dox/DDoS
- European Dissident – Info
- Wolf Cyber Army – DDoS
- Moscow Pentest – Hack
- Twonet – DDoS
- Secotor16 – Hack
- CgpIlnet_Legion – Dox/Info/DDoS
- Sector091 – DDoS
- Tokyo Team
- RussianB
- SSSO – H

Orange = Capability

Последствия DDOS для банка

- деградация производительности клиентских сервисов
- финансовые потери / недополученная прибыль
- реализация репутационных / имиджевых рисков
- доп. финансовые ресурсы на восстановление
- доп. финансовые ресурсы на резервирование
- финансовые претензии/штрафы от регуляторов
- …

2022

«Газпромбанк пожаловался на мощную DDoS-атаку»

ТОП-3

превентивные меры

- резервирование каналов и провайдеров
- регулярное резервное копирование и восстановление
- комплексный эшелонированный (провайдер + внутри) подход к защите

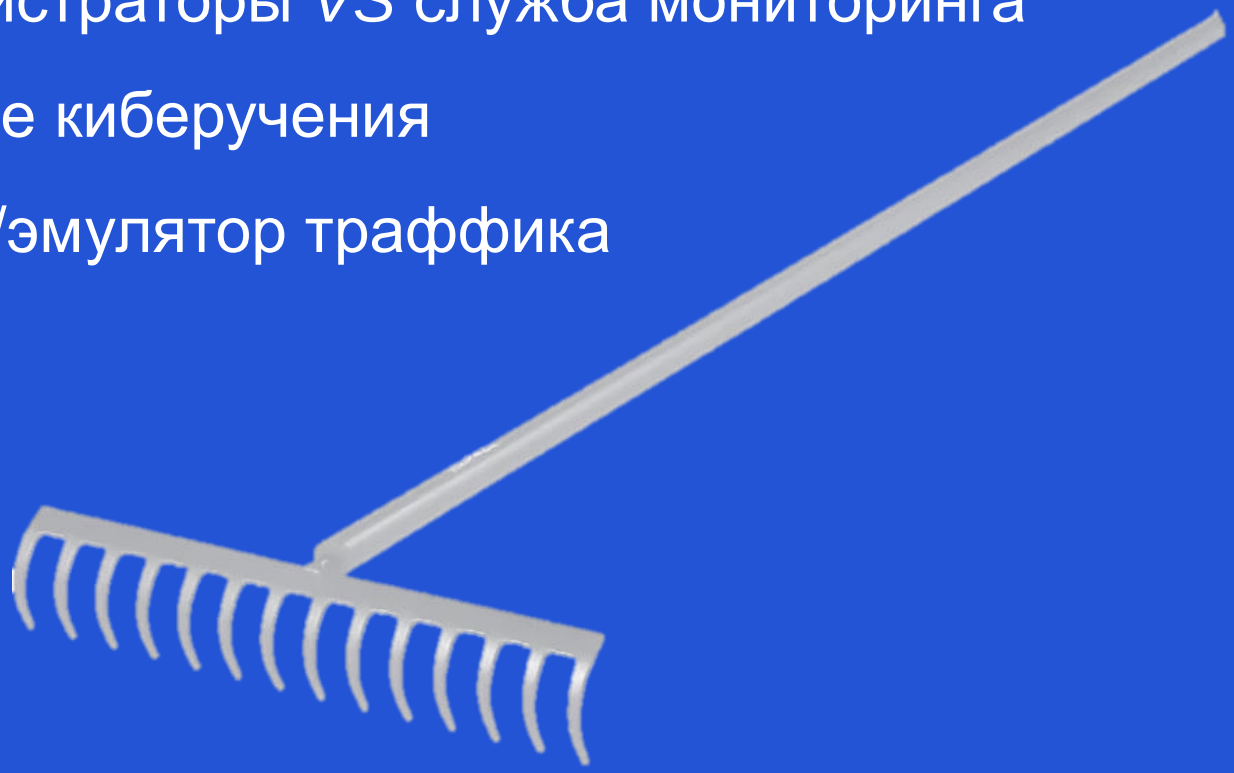
2025

Кто в зоне риска?

- клиенты
- работники
- провайдеры
- «соседи»

Опыт и рекомендации ИБ Газпромбанка

1. x2 | x3 для критических узлов в ИБ-инфраструктуре
2. Активный мониторинг и иерархия уведомлений
3. ИБ-администраторы *VS* служба мониторинга
4. Регулярные киберучения
5. Генератор/эмулятор траффика



2025

Алексей Плешков

заместитель начальника
Департамента защиты информации

pak@gazprombank.ru
+7(903)-613-84-85

#gpb.ru

Благодарю за приглашение, внимание и время !

Готов ответить на Ваши вопросы