kaspersky

Конструктивная информационная безопасность

Андрей Ярных

Директор стратегических проектов

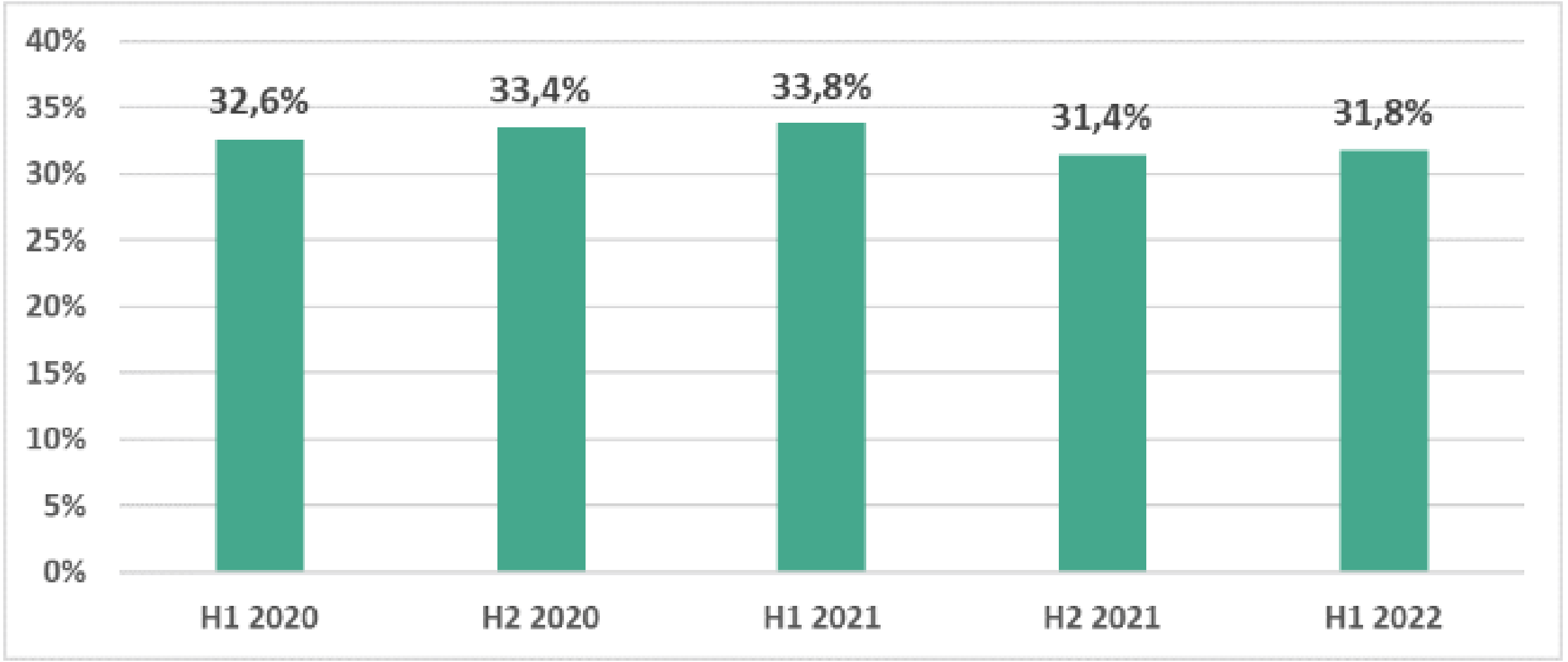
Future Technologies

Цифры квартала

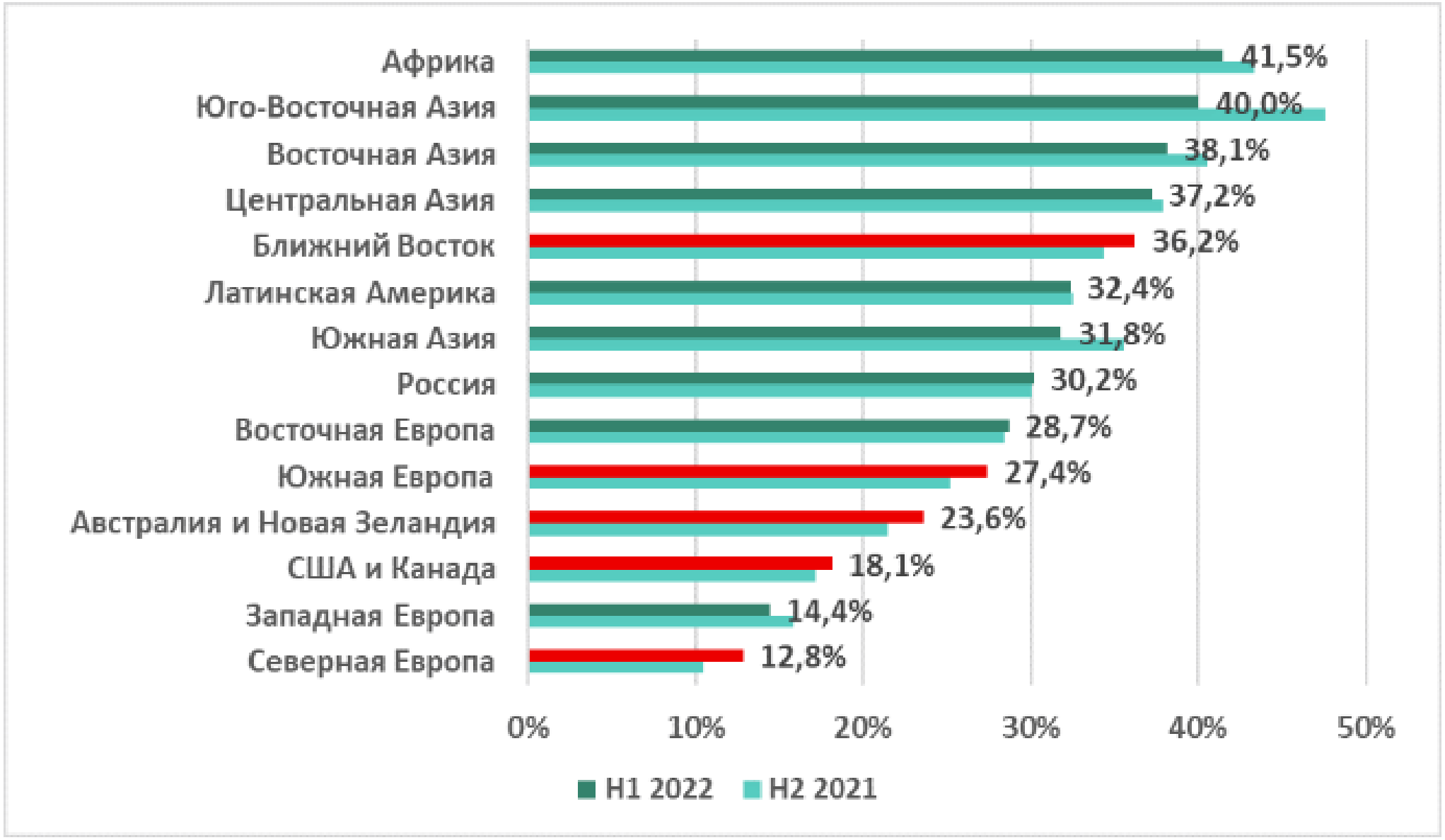
По данным Kaspersky Security Network, во втором квартале 2022 года:

- Решения «Лаборатории Касперского» отразили 1 164 544 060 атак с интернет-ресурсов, размещенных по всему миру.
- Зафиксировано 273 033 368 уникальных ссылок, на которых происходило срабатывание веб-антивируса.
- Запуск вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам предотвращен на компьютерах 100 829 уникальных пользователей.
- Атаки шифровальщиков отражены на компьютерах 74 377 уникальных пользователей.
- Наш файловый антивирус обнаружил 55 314 176 уникальных вредоносных и потенциально нежелательных объектов.

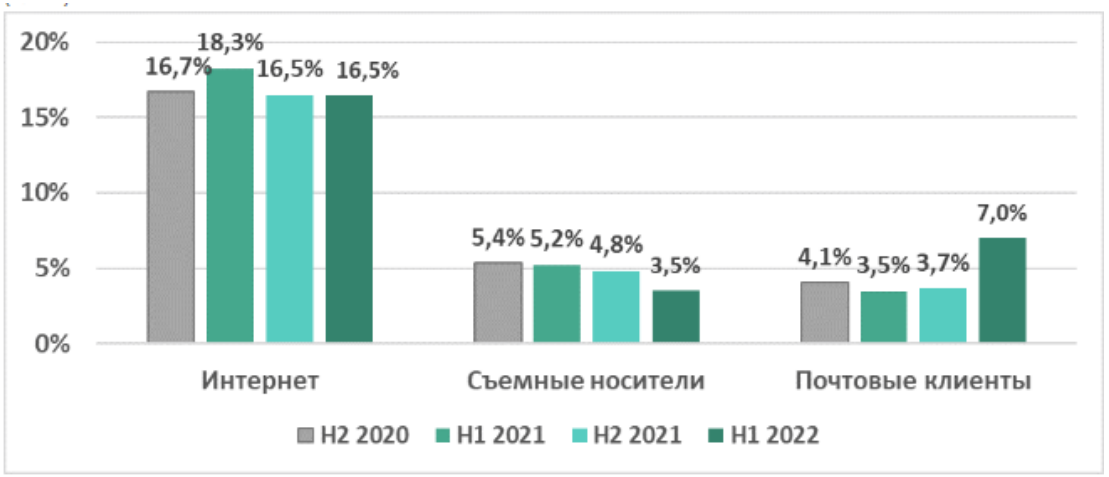
- В первом полугодии 2022 года вредоносные объекты хотя бы раз были заблокированы на 31,8% компьютеров АСУ в мире.

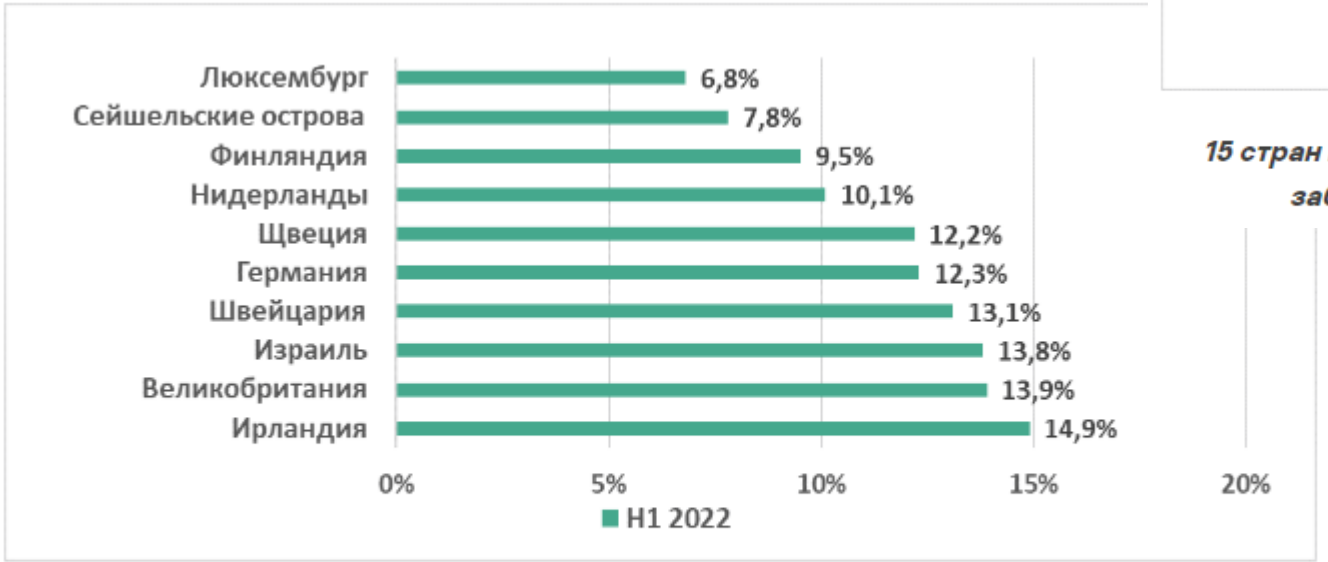


Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты

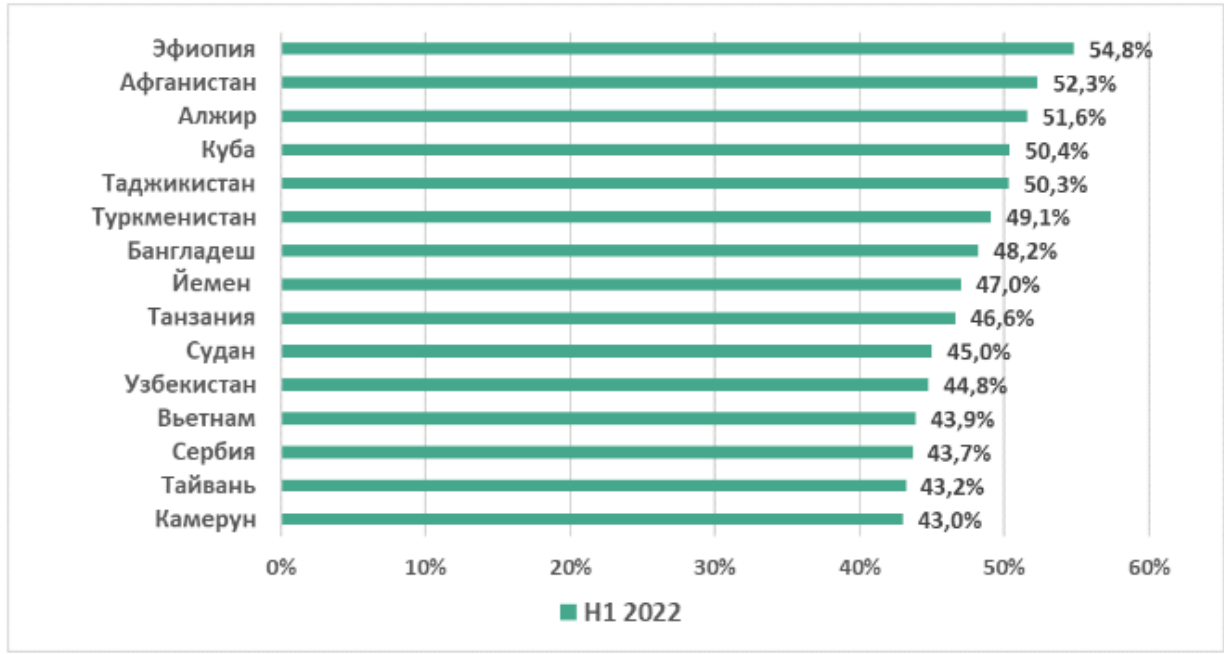


Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионах мира

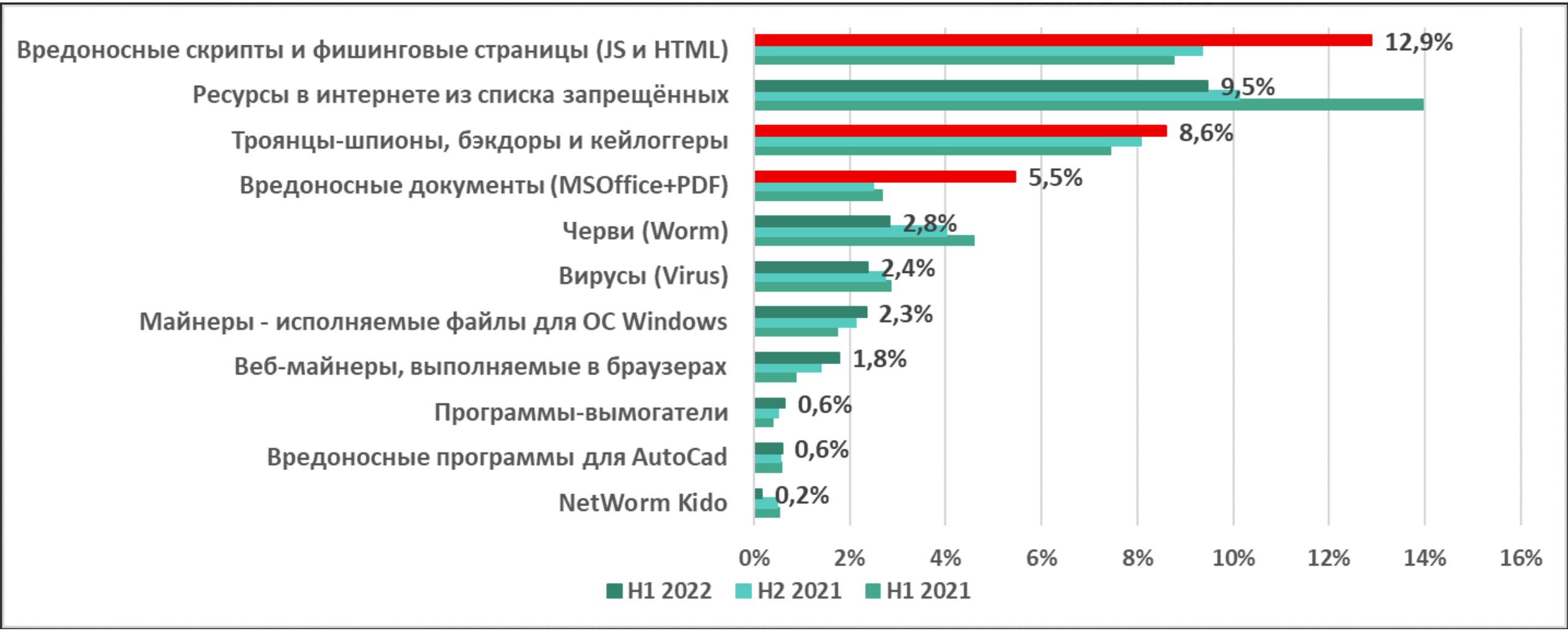




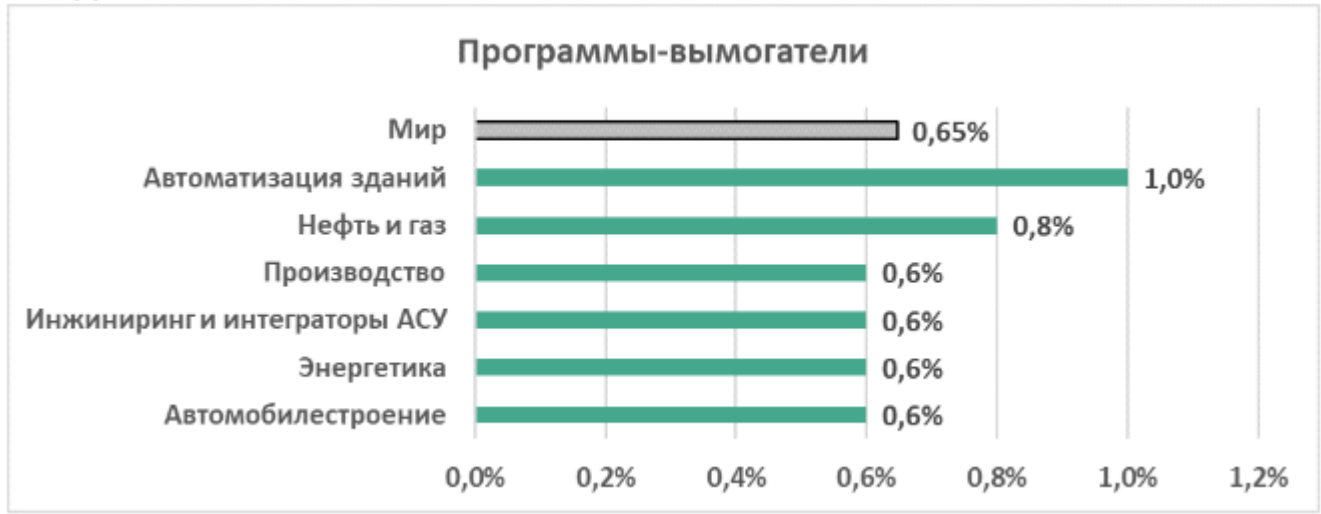
10 стран и территорий с наименьшей долей компьютеров АСУ, на которых были заблокированы вредоносные объекты, первое полугодие 2022 года

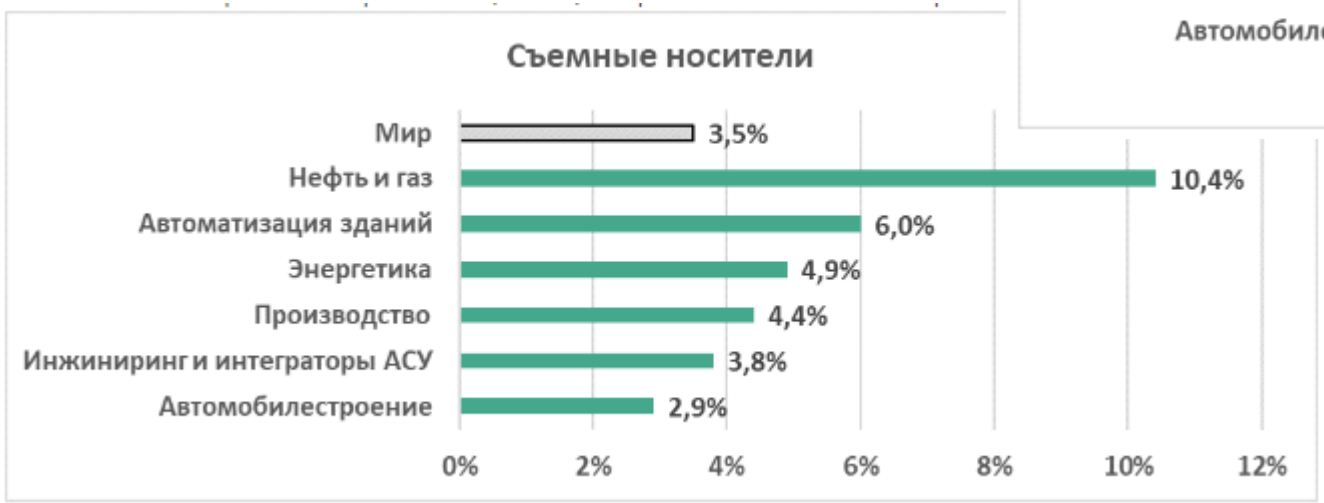


15 стран и территорий с наибольшей долей компьютеров АСУ, на которых были заблокированы вредоносные объекты, первое полугодие 2022 года


Вредоносные скрипты и фишинговые страницы (JS и HTML)
12,9%
Ресурсы в интернете из списка запрещённых
9,5%
Троянцы-шпионы, бэкдоры и кейлоггеры
8,6%
Вредоносные документы (MSOffice+PDF)
5,5%
Черви (Worm)
2,8%
Вирусы (Virus)
2,4%
Майнеры - исполняемые файлы для ОС Windows
2,3%
Веб-майнеры, выполняемые в браузерах
1,8%
Программы-вымогатели
0,6%
Вредоносные программы для AutoCad
0,6%
NetWorm Kido
0,2%
0%
2%
4%
6%
8%
10%
12%
14%
16%
H1 2022
H2 2021
H1 2021


Почтовые клиенты
Мир
Автоматизация зданий
Автомобилестроение
Энергетика
Инжиниринг и интеграторы АСУ
Производство
Нефть и газ
7,0%
14,4%
8,0%
7,5%
5,8%
4,0%
3,3%
0%
2%
4%
6%
8%
10%


Программы-вымогатели
Мир
Автоматизация зданий
Нефть и газ
Производство
Инжиниринг и интеграторы АСУ
Энергетика
Автомобилестроение
0,65%
1,0%
0,8%
0,6%
0,6%
0,6%
0,6%
0,0%
0,2%
0,4%
0,6%
0,8%
1,0%
1,2%


Съемные носители
Мир
Нефть и газ
Автоматизация зданий
Энергетика
Производство
Инжиниринг и интеграторы АСУ
Автомобилестроение
3,5%
10,4%
6,0%
4,9%
4,4%
3,8%
2,9%
0%
2%
4%
6%
8%
10%
12%

Развитие информационных угроз во втором квартале 2022 года. Мобильная статистика

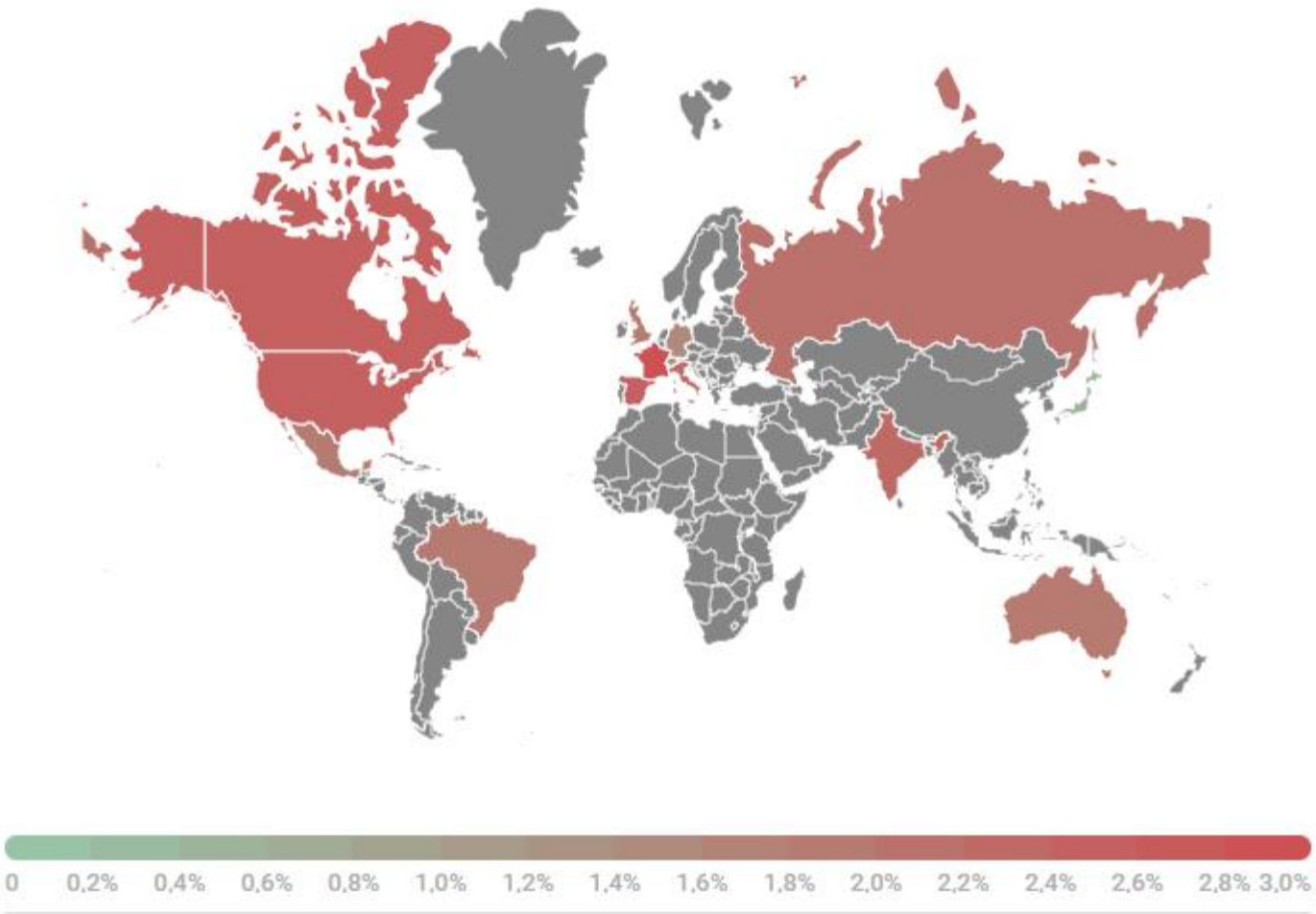
TOP 10 мобильных банкеров

	Вердикт	%*
1	Trojan-Banker.AndroidOS.Bian.h	23,22
2	Trojan-Banker.AndroidOS.Anubis.t	10,48
3	Trojan-Banker.AndroidOS.Svpeng.q	7,88
4	Trojan-Banker.AndroidOS.Asacub.ce	4,48
5	Trojan-Banker.AndroidOS.Sova.g	4,32
6	Trojan-Banker.AndroidOS.Gustuff.d	4,04
7	Trojan-Banker.AndroidOS.Ermak.a	4,00
8	Trojan-Banker.AndroidOS.Agent.ep	3,66
9	Trojan-Banker.AndroidOS.Agent.eq	3,58
10	Trojan-Banker.AndroidOS.Faketoken.z	2,51

TOP 10 мобильных вымогателей

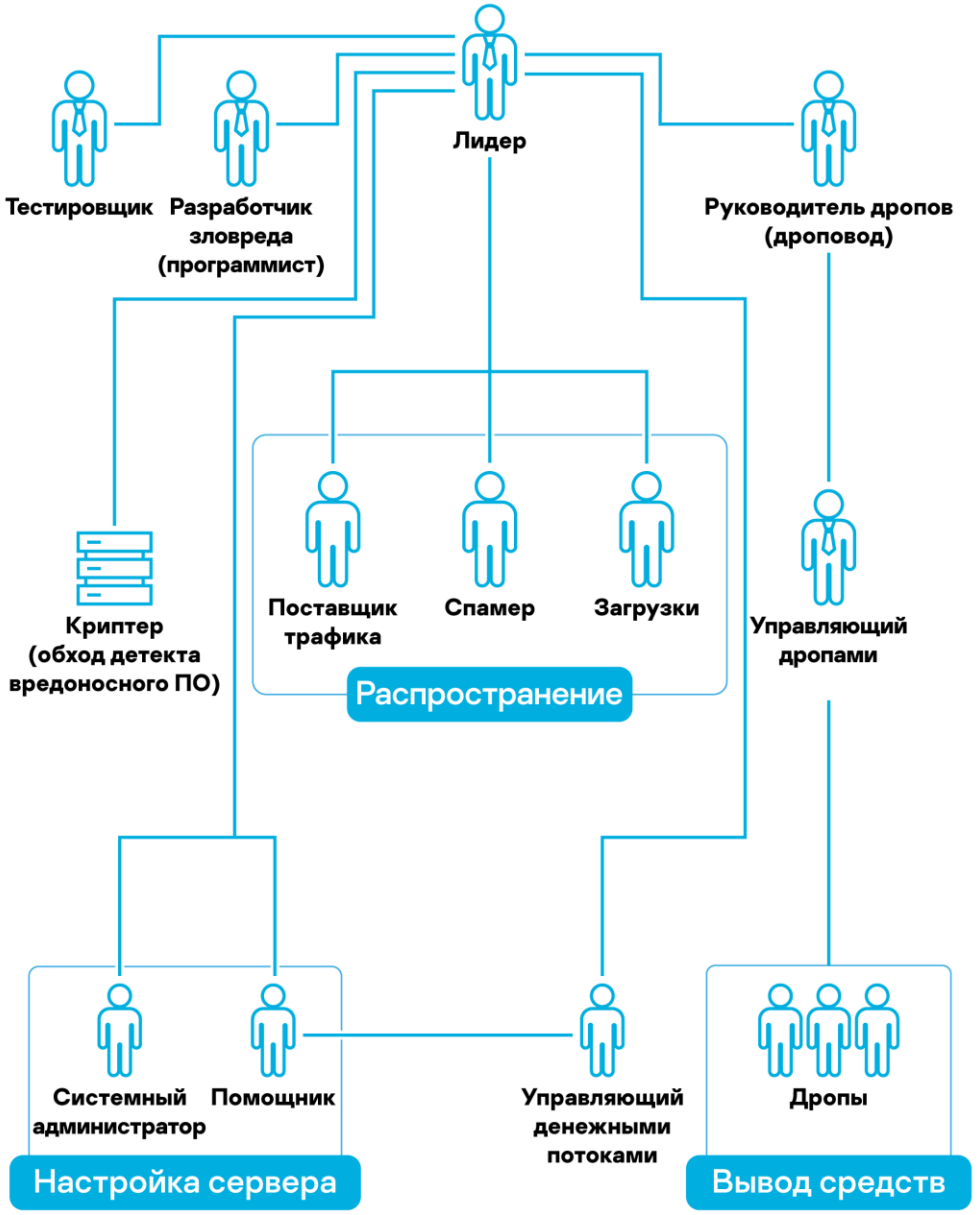
	Вердикт	%*
1	Trojan-Ransom.AndroidOS.Pigetrl.a	76,81
2	Trojan-Ransom.AndroidOS.Rkor.ch	2,66
3	Trojan-Ransom.AndroidOS.Small.as	2,51
4	Trojan-Ransom.AndroidOS.Rkor.br	1,46
5	Trojan-Ransom.AndroidOS.Rkor.bi	1,40
6	Trojan-Ransom.AndroidOS.Svpeng.ah	1,29
7	Trojan-Ransom.AndroidOS.Congur.cw	1,23
8	Trojan-Ransom.AndroidOS.Small.cj	1,14
9	Trojan-Ransom.AndroidOS.Svpeng.ac	1,14
10	Trojan-Ransom.AndroidOS.Congur.bf	1,07

География угроз для macOS



	Вердикт	%*
1	AdWare.OSX.Amc.e	25,61
2	AdWare.OSX.Agent.ai	12,08
3	AdWare.OSX.Pirrit.j	7,84
4	AdWare.OSX.Pirrit.ac	7,58
5	AdWare.OSX.Pirrit.o	6,48
6	Monitor.OSX.HistGrabber.b	5,27
7	AdWare.OSX.Agent.u	4,27
8	AdWare.OSX.Bnodlero.at	3,99
9	Trojan-Downloader.OSX.Shlayer.a	3,87
10	Downloader.OSX.Agent.k	3,67
11	AdWare.OSX.Pirrit.aa	3,35
12	AdWare.OSX.Pirrit.ae	3,24
13	Backdoor.OSX.Twenbc.e	3,16

Что было и что стало: сравнение структуры киберпреступных групп в 2016 и 2021 годах



Такие изменения, как удорожание уязвимостей, переход на облачные серверы и появление доступных готовых инструментов для атаки, привели к сокращению численности киберпреступных групп.

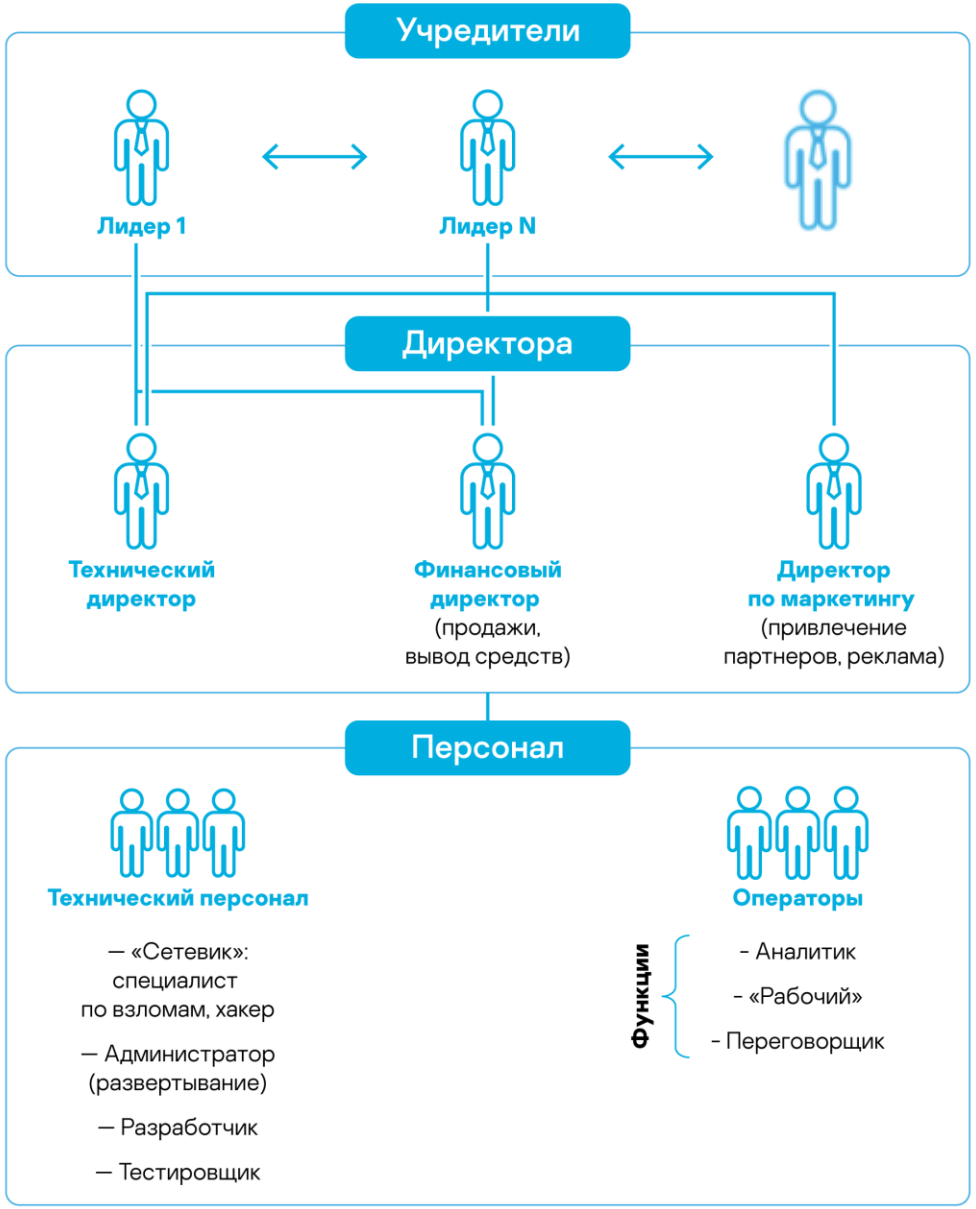
Им больше не нужны системные администраторы для обслуживания физической инфраструктуры — облачные сервисы упростили этот аспект. Злоумышленники перестали создавать собственное вредоносное ПО.

Если раньше крупным группам требовались как минимум два специалиста для разработки разных частей программы (например, клиентской и серверной), то теперь достаточно одного оператора.

Вместо покупки переходов на вредоносные сайты преступники покупают данные — для доступа к корпоративным сетям, учетным записям и т. д. Причем эту задачу тоже можно передать сторонним исполнителям

Злоумышленники оптимизировали цепочку атаки, а их команды стали более гибкими.

kaspersky



Что было и что стало: сравнение структуры киберпреступных групп в 2016 и 2021 годах

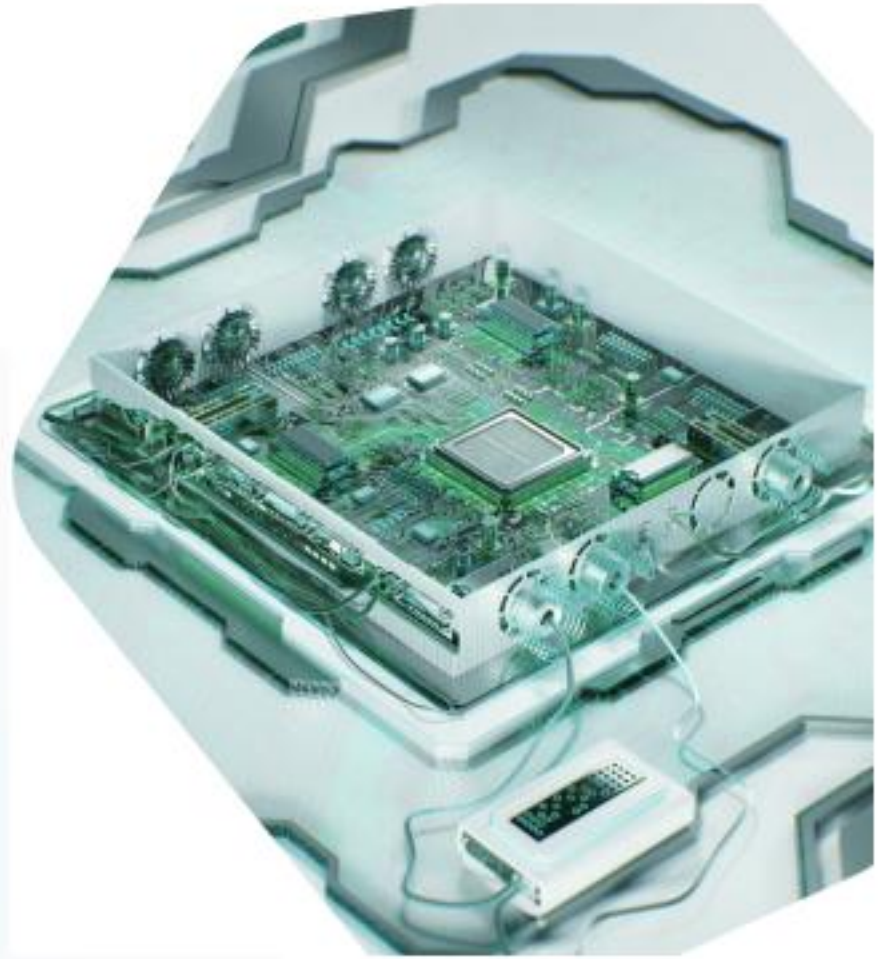
Тестировщики, как и разработчики, тоже больше не нужны. Длинные цепочки атаки, включающие эксплойты для разных уязвимостей, стали короче. Таким образом, создатели эксплойтов, которые специализировались на клиентской части, остались без работы

В теневом интернете все чаще появляется вредоносное ПО с открытым исходным кодом. Они бесплатно публикуют его в открытом доступе, позволяя новым игрокам легко начать криминальную карьеру. Так, создатели банковского троянца Cerberus раскрыли его исходный код в октябре 2020 года, а разработчики печально известного шифровальщика Babuk — в начале сентября 2021-го.

Итого, для проведения успешной атаки в 2021 году киберпреступной группе нужны: руководитель; оператор вредоносного ПО; специалист, который обеспечит доступ к сети; и специалист по финансам, чтобы извлечь и обналичить украденные средства.

kaspersky

Кибериммунитет



новый подход к разработке безопасных IT-решений

Кибериммунитет

Конструктивная безопасность
Secure-by-design

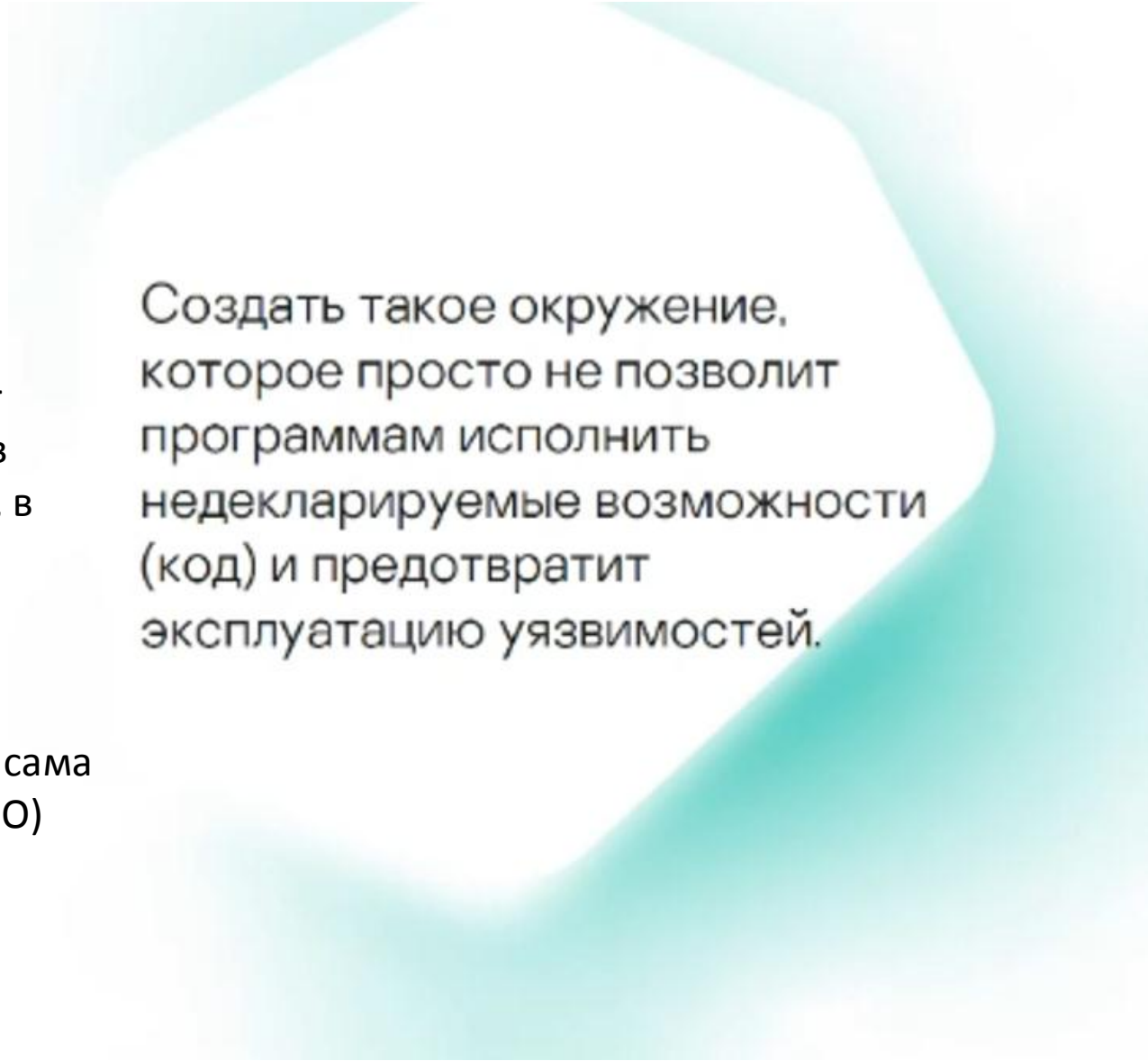
- Требования по безопасности учитываются наравне с другими бизнес-требованиями с самого начала раработки

- Методология разработки, позволяющая разрабатывать ПО способное устойчиво работать в неблагоприятной информационной среде

Выполнение требований доверия и информационной безопасности может обеспечить подход, получивший название Secure-by-Design (Конструктивная Информационная Безопасность, или информационная безопасность, предусмотренная конструктивно.

При таком подходе системы и устройства приобретают свойства безопасности ещё на этапе проектирования, в ходе которого учитываются аспекты, ранее относимые, в основном, к разработке специализированных СЗИ: формирование требований по информационной безопасности, модели угроз и нарушителя и т.д.

Таким образом, основным средством защиты является сама архитектура устройства, программного обеспечения (ПО) или системы, обеспечивающая их надежное функционирование в «агрессивной информационной среде»



Доверенная среда

На каждом уровне системы есть свои методики и механизмы повышения уровня доверия

Доверенная пользовательская среда
Наложенные средства безопасности
Безопасность приложений

Доверенная системная среда
Средства администрирования
Интегрированная безопасность

Домены безопасности,
Доверенная загрузка, обновление
Программная виртуализация

Доверенная среда исполнения
Аппаратная виртуализация
Доверенные приложения, алгоритмы

Доверенное аппаратное ядро
Защищенная область памяти
Защищенные ключи и сертификаты

Наследование доверия между уровнями системы

Стратегия развития применения кибериммунного подхода (в том числе KasperskyOS)

Продукт

KISG 1000

KISG 100

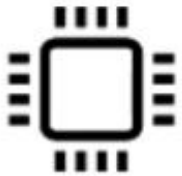
Продукт

KSRW

Прототип

Прототип

Прототип



Исследования

Исследования

IoT-шлюзы CPE

Тонкие клиенты

Умный контроллер

Система дистрибуции приложений и UEM

Мобильные устройства

Встроенная безопасность (In Chip Security) ARM TZ, RISC-V MultiZone

Конфиденциально

Россия. Апрель 2020


РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

№ 788764

Cyber Immunity

UK. Январь 2021


TRADE MARKS REGISTRY

REGISTRATION CERTIFICATE

REGISTRAR

Representation of Mark
KASPERSKY CYBER IMMUNITY

USA. Март 2022


United States of America

United States Patent and Trademark Office

KASPERSKY CYBER IMMUNITY

Reg. No. 6,688,542

Registered Mar. 22, 2022

Int. Cl.: 9, 42

Service Mark

Trademark

Principal Register

Стандарты разработки информационных систем ТК362/РГ-8

Лаборатория Касперского –
Участие в создании современных стандартов (ГОСТов) разработки информационных систем, устойчивых к деструктивным воздействиям

Методология разработки доверенных приложений secure-by-design
Система оценки зрелости безопасности
Принцип многочисленных независимых уровней безопасности (MILS)
Доверенные операционные системы. Термины, определения, классификация
IoT. Системы с разделением доменов

«Лаборатория Касперского» переносит часть своей инфраструктуры в Швейцарию и открывает Центры прозрачности

Хранение и обработка пользовательских данных

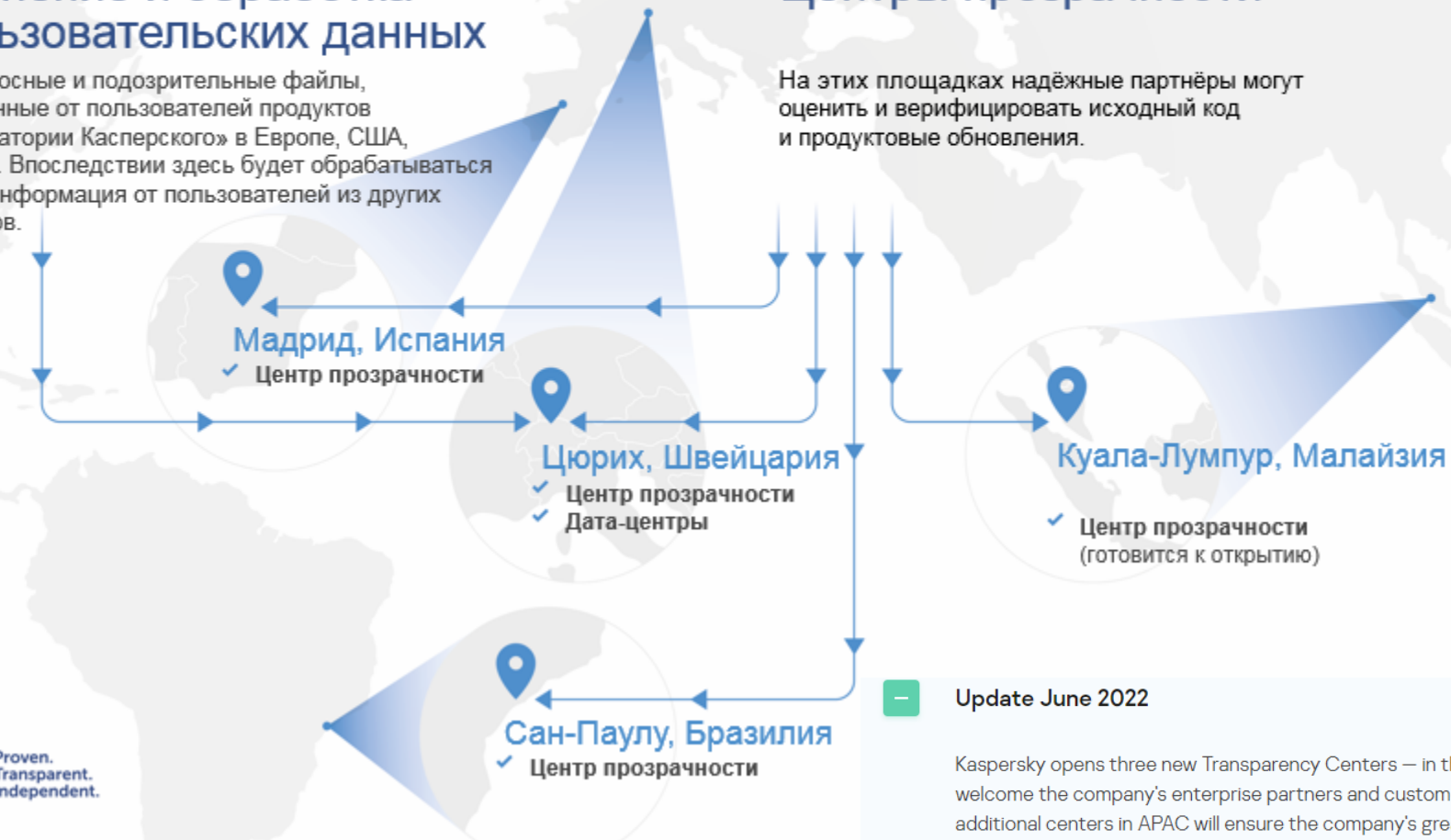
Вредоносные и подозрительные файлы, полученные от пользователей продуктов «Лаборатории Касперского» в Европе, США, Канаде. Впоследствии здесь будет обрабатываться также информация от пользователей из других регионов.

Центры прозрачности

На этих площадках надёжные партнёры могут оценить и верифицировать исходный код и продуктовые обновления.

Независимый обзор

Сторонняя оценка внутренних процессов с целью проверки решений «Лаборатории Касперского» на целостность.
В 2019 году компания успешно прошла аудит по контрольным процедурам в сервисных организациях – Service Organization Control for Service Organizations (SOC 2) Type 1.



Программа Bug Bounty

Инициатива предусматривает привлечение сторонних исследователей и выплату им вознаграждения в случае обнаружения критических брешей в продуктах «Лаборатории Касперского».

Proven. Transparent. Independent.

Update June 2022

Kaspersky opens three new Transparency Centers — in the United States, Japan and Singapore. The newly opened facilities will welcome the company's enterprise partners and customers, including state agencies and regulators, responsible for cybersecurity. Two additional centers in APAC will ensure the company's greater proximity to stakeholders in the region, while the center in Woburn will serve as the new venue for the company's North American Transparency Center, which used to be located in New Brunswick, Canada.

https://www.kaspersky.com/transparency-center-offices

kaspersky

Спасибо!

Andrey.Yarnikh@kaspersky.com