kaspersky

Ландшафт угроз для систем промышленной автоматизации

Второе полугодие 2022

Kaspersky ICS CERT

06.03.2023

Version 1.1

2022 — цифры года ... 2
Россия, второе полугодие 2022 ... 3
Глобальная статистика по всем угрозам ... 6
Разнообразие обнаруженного вредоносного ПО ... 11
Категории вредоносных объектов ... 11
Вредоносные скрипты и фишинговые страницы (JS и HTML) и ресурсы из интернета из списка запрещенных ... 12
Программы-шпионы ... 13
Вредоносные документы (MSOffice+PDF) ... 14
Вредоносные программы для скрытого майнинга криптовалюты ... 14
Вирусы и черви ... 15
Вредоносные программы для AutoCAD ... 16
Программы-вымогатели ... 16
Основные источники угроз ... 18
Мир ... 18
Регионы и страны ... 20
Интернет ... 20
Съемные носители ... 21
Почтовые клиенты ... 22
Сетевые папки ... 24
Методика подготовки статистики ... 25

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

2022 — цифры года

Показатель	H1 2022	H2 2022	2022
Процент атакованных компьютеров АСУ в мире	31,8%	34,3%	40,6%
Основные источники угроз			
Интернет	16,5%	19,9%	24,0%
Почтовые клиенты	7,0%	6,4%	7,9%
Съемные носители	3,5%	3,8%	5,2%
Сетевые папки	0,6%	0,6%	0,8%
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы (JS и HTML)	12,9%	13,5%	17,3%
Ресурсы в интернете из списка запрещённых	9,5%	10,1%	13,2%
Троянцы-шпионы, бэкдоры и кейлоггеры	8,6%	7,1%	9,2%
Вредоносные документы (MSOffice+PDF)	5,5%	4,5%	6,2%
Черви (Worm)	2,8%	2,5%	3,5%
Вирусы (Virus)	2,4%	2,4%	3,2%
Майнеры — исполняемые файлы для ОС Windows	2,3%	1,5%	2,7%
Веб-майнеры, выполняемые в браузерах	1,8%	1,8%	2,5%
Вредоносные программы для AutoCAD	0,6%	0,6%	0,8%
Программы-вымогатели	0,6%	0,4%	0,7%

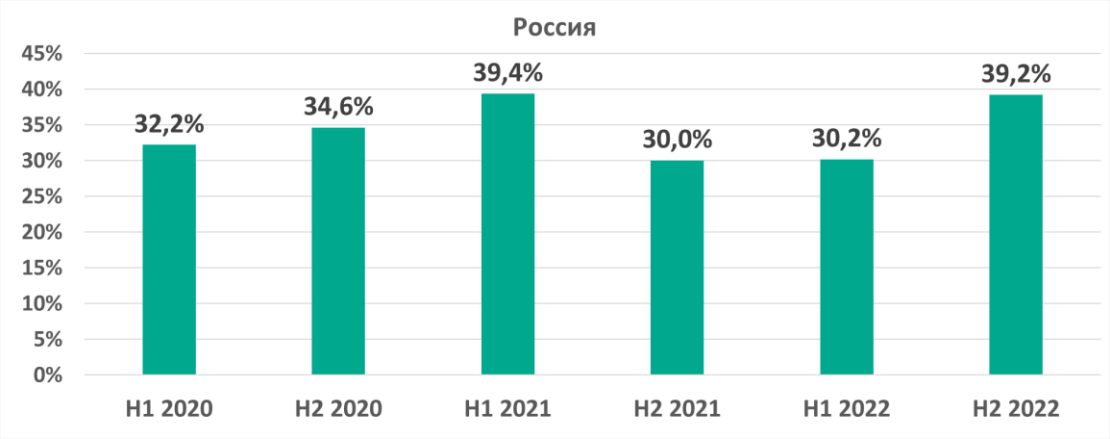
© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Россия, второе полугодие 2022

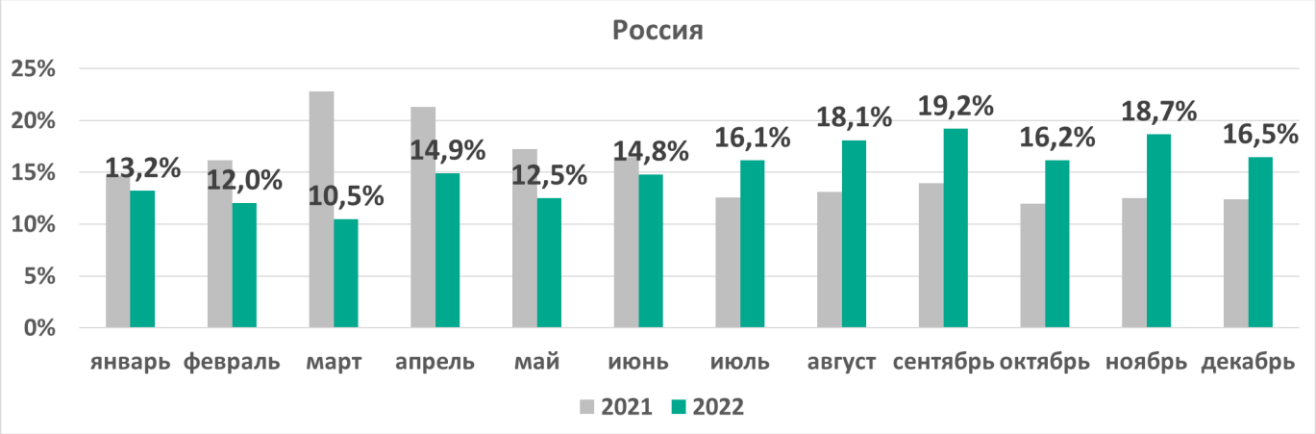
Во втором полугодии 2022 года **среди всех стран самое значительное изменение** процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, отмечено в России, где этот показатель увеличился на 9 п.п.

С 39,2% Россия поднялась с восьмого сразу на третье место в рейтинге регионов по этому показателю (напомним, что в наших отчетах мы рассматриваем Россию и как страну, и как регион, в который входит единственная страна).

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



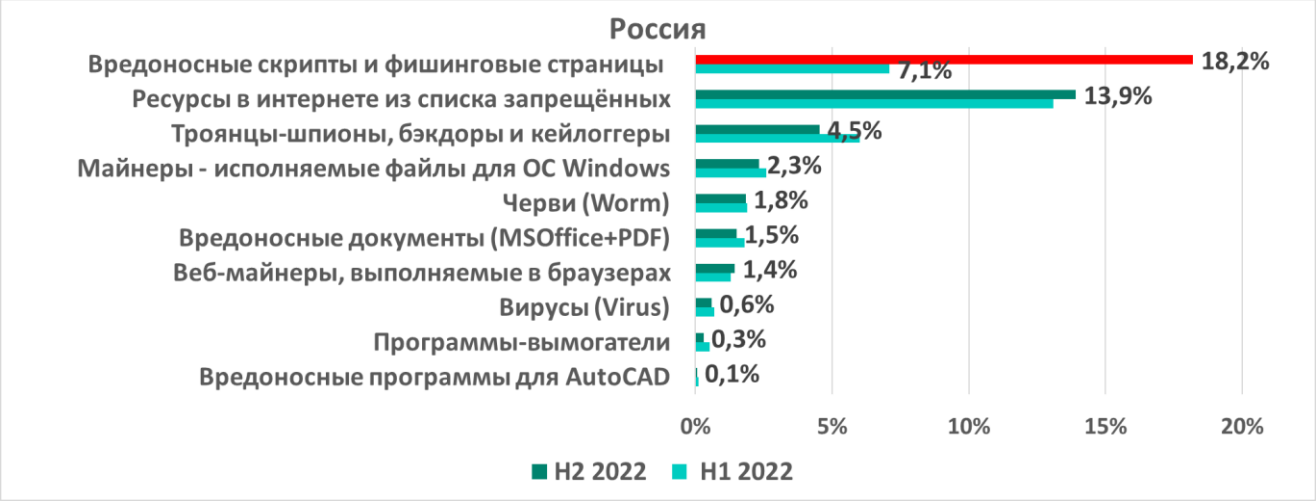
После перепадов в первом полугодии 2022 года месячного показателя процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, с началом второго полугодия он рос три месяца подряд. Отметим, что месячная динамика 2022 года совершенно не совпадает с картиной предыдущего, 2021 года.



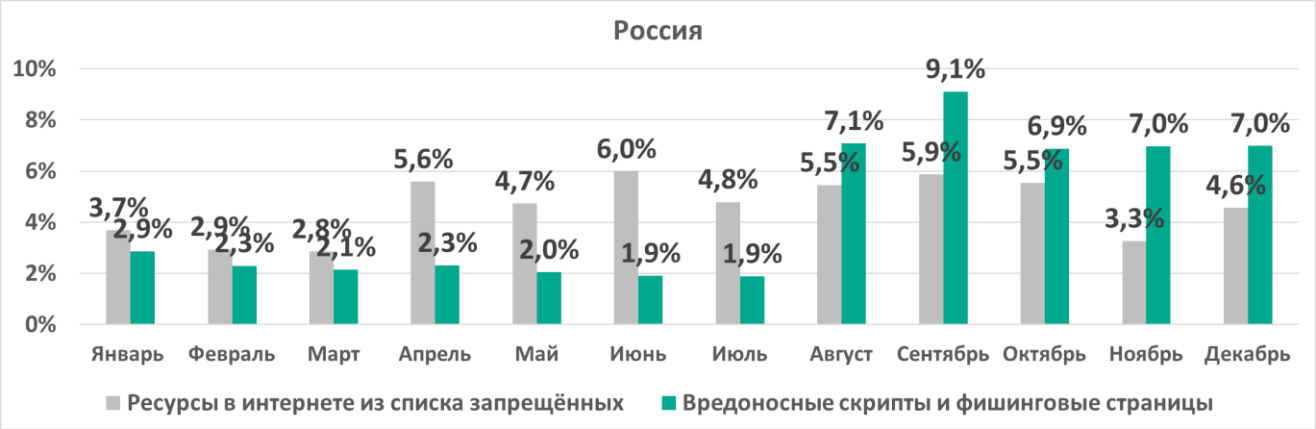
Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2021 и 2022 годов

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Увеличение в России процента компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2022 года, обусловлено резким ростом процента компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы (JS и HTML) — на 11,1 п.п.



Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий



Россия. Процент компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных и вредоносные скрипты и фишинговые страницы, январь — декабрь 2022

Резкий всплеск процента компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы в августе и сентябре 2022, и высокие показатели следующих месяцев года обусловлены массовым заражением сайтов (в том числе промышленных организаций), использующих устаревшую версию одной из популярных российских CMS. Отметим, что компьютеры АСУ, с которых в интернет можно попасть на произвольные сайты, — это по большей части АРМ операторов и инженеров.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Уязвимость, обнаруженная еще в марте 2022, позволяет атакующему выполнить произвольный код на стороне веб-сервера. В ходе массового заражения сайтов, которые не были своевременно обновлены, злоумышленники заражали используемые на сайте JavaScript файлы, встраивая код для перенаправления браузера на сторонние вредоносные веб-ресурсы и фишинговые страницы.

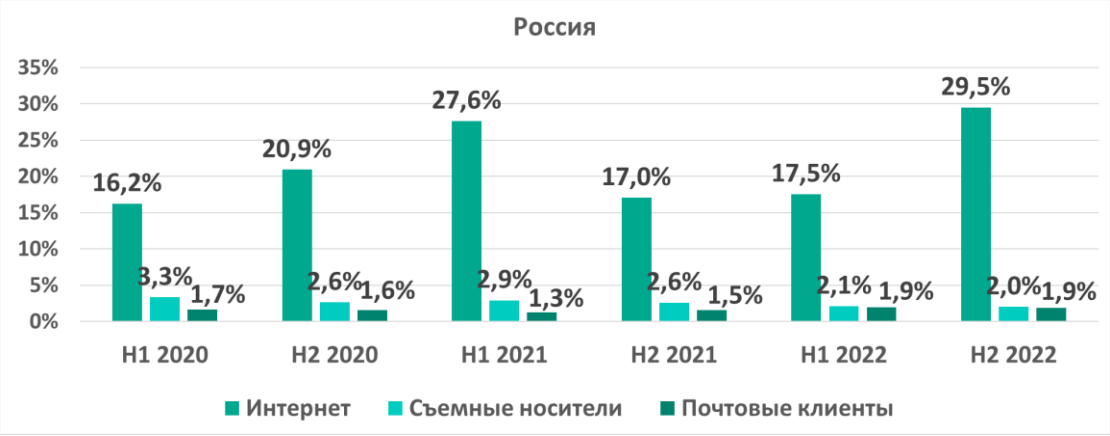
Помимо России, распространение вредоносных скриптов в результате массового заражения необновлённых веб-сайтов под управлением CMS также затронуло компьютеры АСУ в Белоруссии и в странах Центральной Азии. Процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, увеличился во втором полугодии 2022 года:

- в Белоруссии — на 10,3 п.п. и по итогам полугодия составил 17,8%;
- в Киргизии — на 16,4 п.п., 26,4% по итогам полугодия;
- в Узбекистане — на 7,8 п.п., 15,6% по итогам полугодия;
- в Казахстане — на 6,1 п.п., 14,1% по итогам полугодия.

Что касается роста (начиная с апреля 2022) процента компьютеров АСУ, на которых были заблокированы попытки доступа к вредоносным веб-ресурсам, то он по большей части обусловлен повышением активности потенциально опасных рекламных платформ, нередко используемых для распространения вредоносного ПО под видом рекламы на различных веб-ресурсах.

В России во втором полугодии 2022 года процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, увеличился на 12 п.п.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников

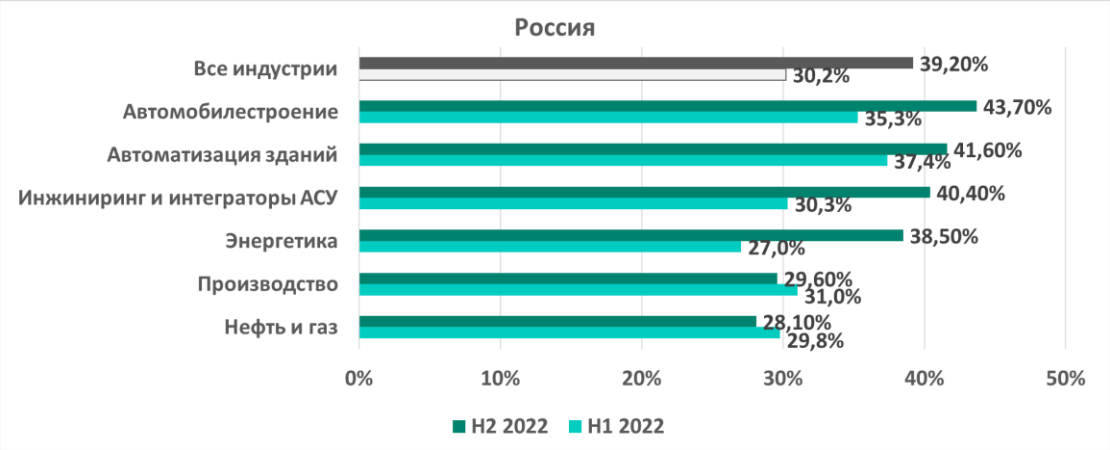


Во втором полугодии 2022 года в России в большинстве отраслей вырос (в некоторых отраслях весьма значительно) процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, — как вследствие массового распространения вредоносных скриптов, так и из-за небольшого

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

увеличения в России процента компьютеров АСУ, на которых было заблокировано шпионское ПО.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях

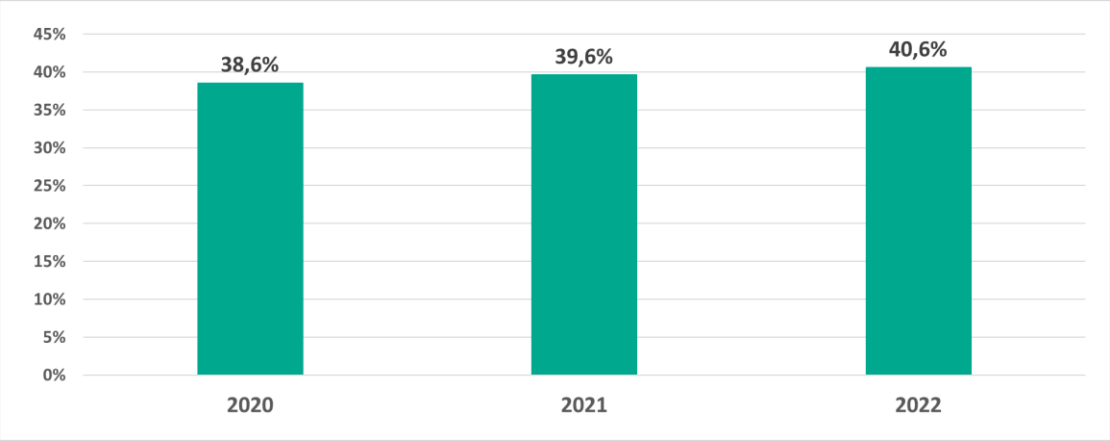


Уменьшение показателя по сравнению с первым полугодием 2022 года в производственной и нефтегазовой отраслях связано со снижением показателей для интернет- и почтовых угроз.

Глобальная статистика по всем угрозам

По итогам 2022 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, составил 40,6%. Как и в 2021 году, он увеличился по сравнению с предыдущим годом на 1 п.п.

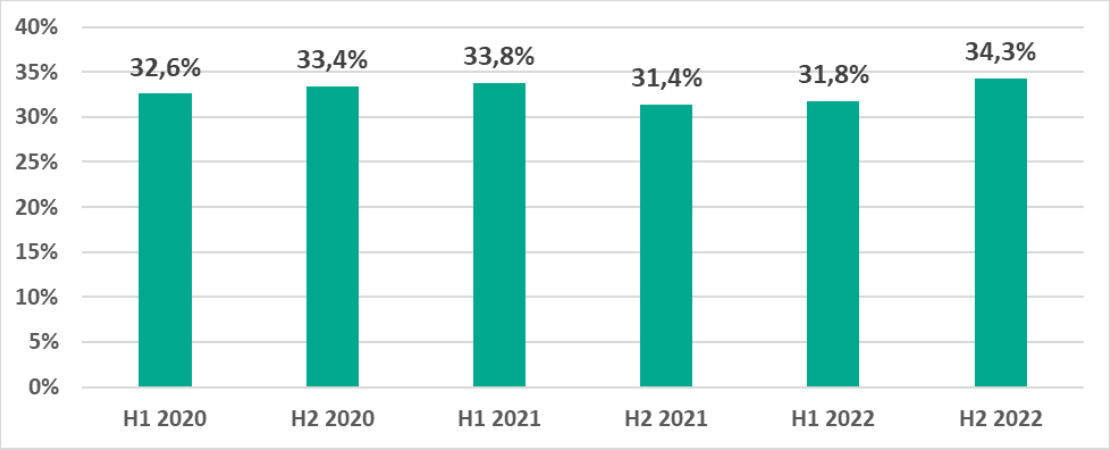
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, 2020 — 2022 годы



© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

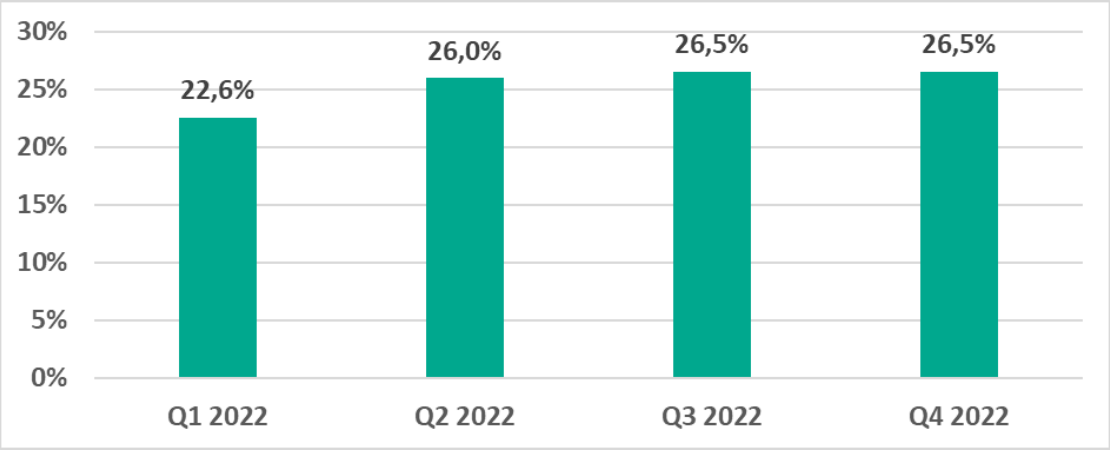
Однако если в первом полугодии 2022 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по сравнению с предыдущим увеличился всего на 0,4 п.п., то во второй половине года он вырос на 3,5 п.п. и достиг 34,3%. Это ненамного, но превышает показатели полугодий не только 2021, но и 2020 годов.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



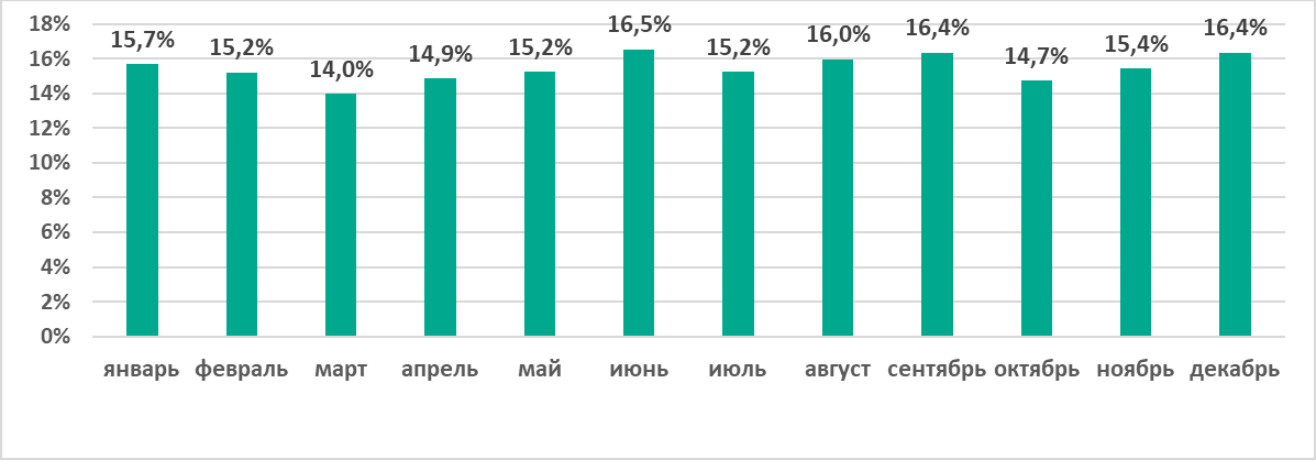
Как видно на графике ниже, минимальный процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, был в первом квартале 2022 года, а основной прирост пришелся на второй квартал. Проценты за кварталы третьего и четвертого полугодий оказались одинаковыми.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по кварталам 2022 года



Самыми «горячими» месяцами года стали июнь, сентябрь и декабрь. Наименьшие значения были отмечены в марте и октябре.

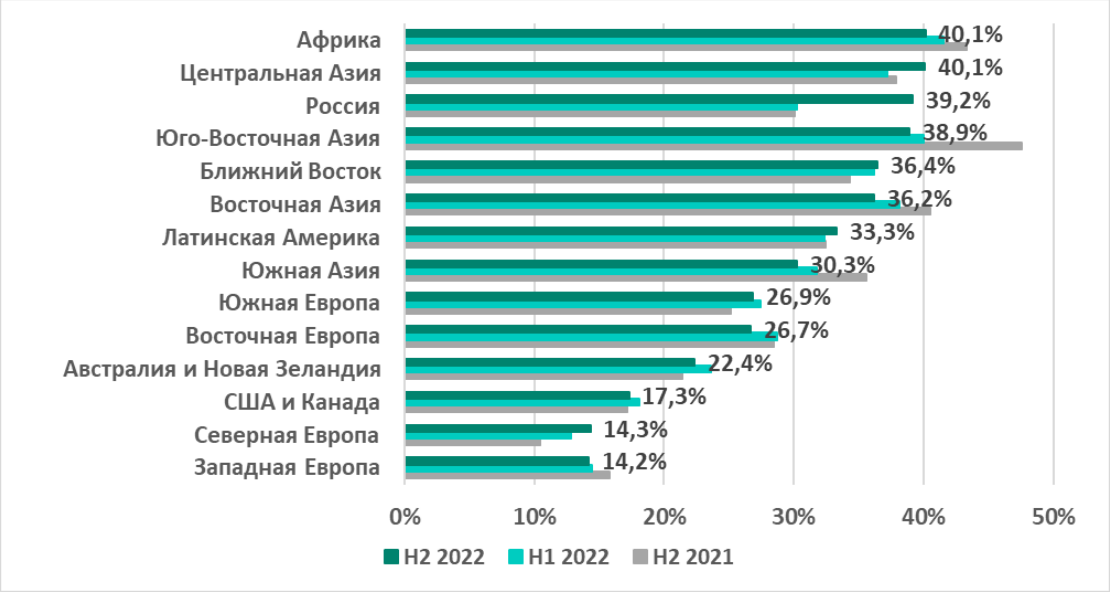
© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2022

В регионах мира доля компьютеров АСУ, на которых была предотвращена вредоносная активность, варьирует от 40,1% в лидирующих по этому показателю Африке и Центральной Азии до 14,2% и 14,3% в наиболее благополучных Западной и Северной Европе.

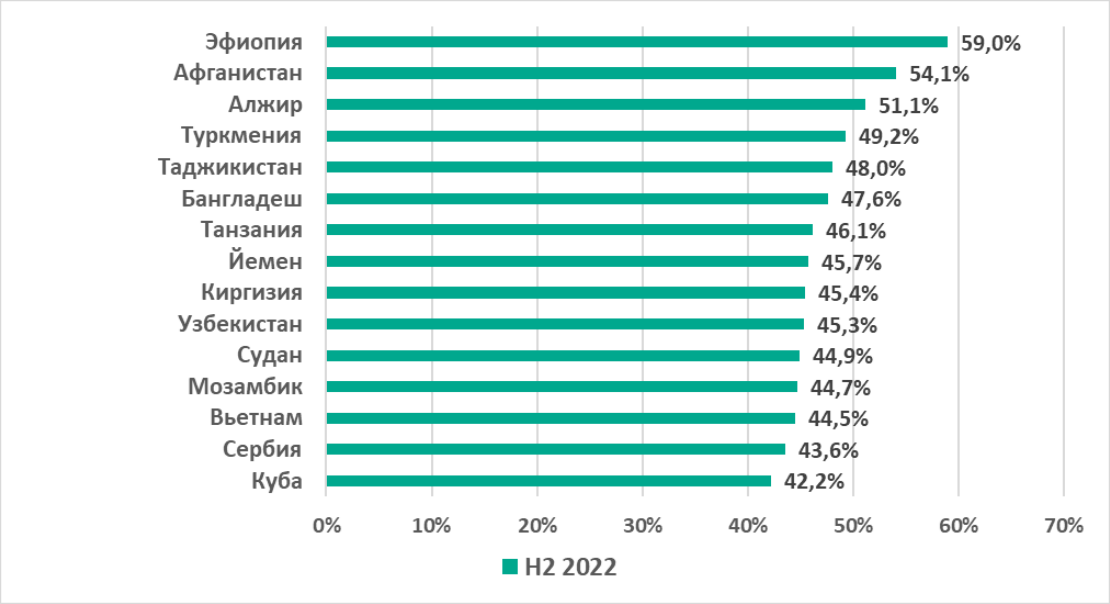
Рейтинг регионов мира по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2022



Ситуация в странах даже из одного региона может отличаться весьма значительно. Например, на Ближнем Востоке в большинстве стран процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по итогам второго полугодия 2022 попадает в диапазон 30 — 40%. Однако в Йемене он составил 45,7%, в то же время в Израиле — 12,1%, и Йемен по итогам полугодия попадает в десятку стран и территорий с наибольшими показателями, а Израиль — с наименьшими.

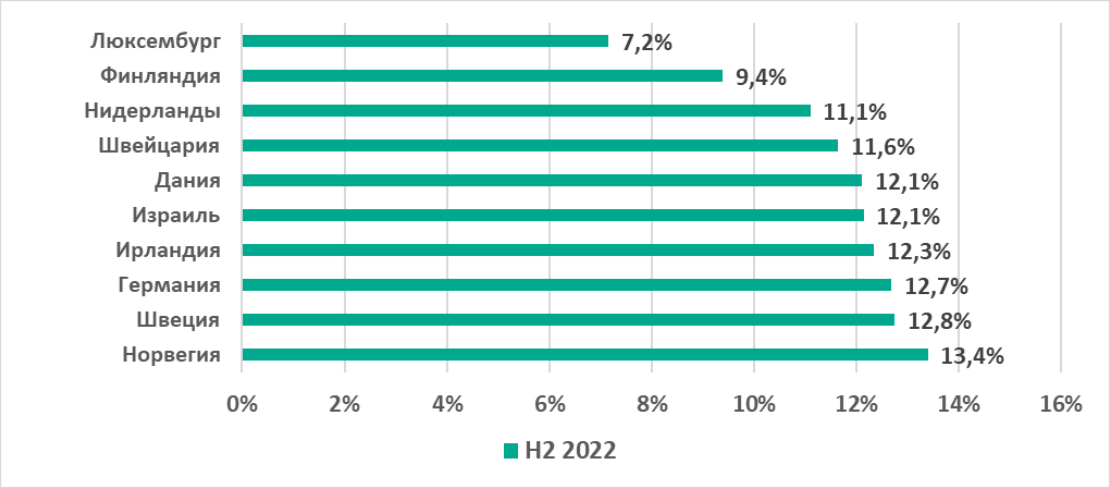
© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2022



Среди 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2022, преобладают страны Африки и Центральной Азии. В десятке стран с наименьшими показателями за исключением Израиля все страны европейские.

10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2022

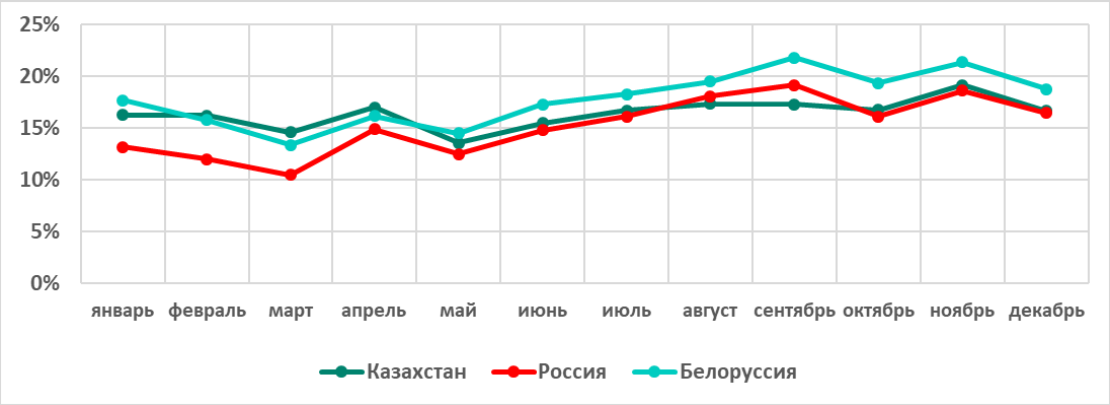


Наибольшее увеличение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, во втором полугодии 2022 года зафиксировано в России — на 9 п.п. — и в Белоруссии — на 6,9 п.п.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

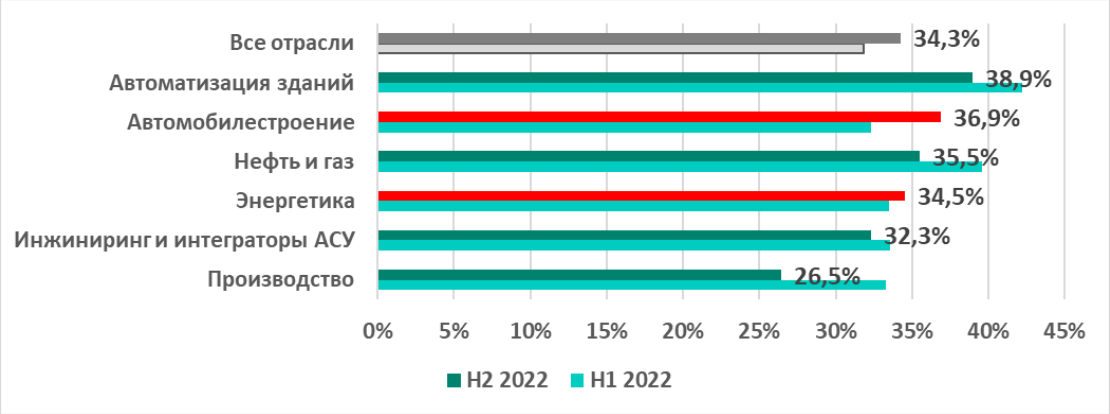
Мы обратили внимание на некоторое сходство динамики по месяцам процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, в этих двух странах. Еще одна страна со схожей динамикой — Казахстан.

Россия, Белоруссия и Казахстан. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам 2022 года



Отличается ситуация и в разных отраслях. Как видно на графике ниже, во втором полугодии 2022 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличился в автомобилестроении (+4,6 п.п.) и в энергетике (+1 п.п.). В остальных исследуемых отраслях показатель уменьшился.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях

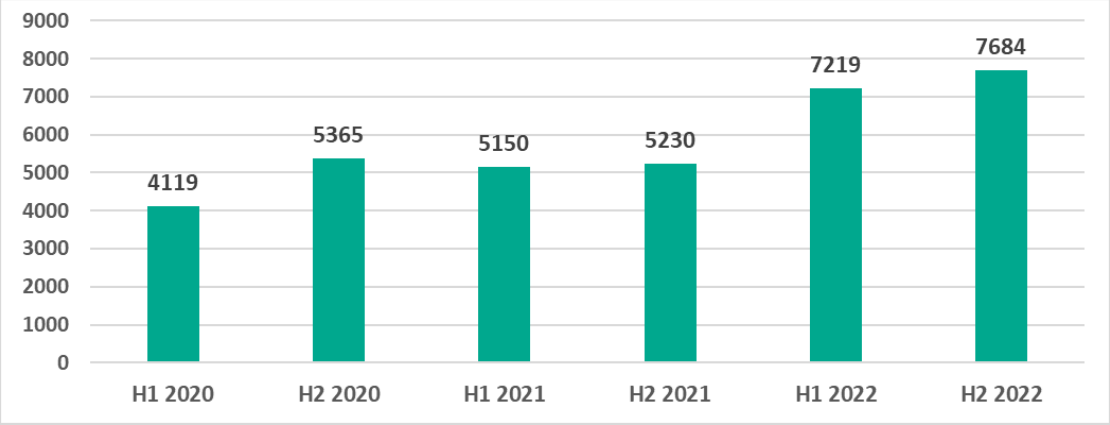


© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Разнообразие обнаруженного вредоносного ПО

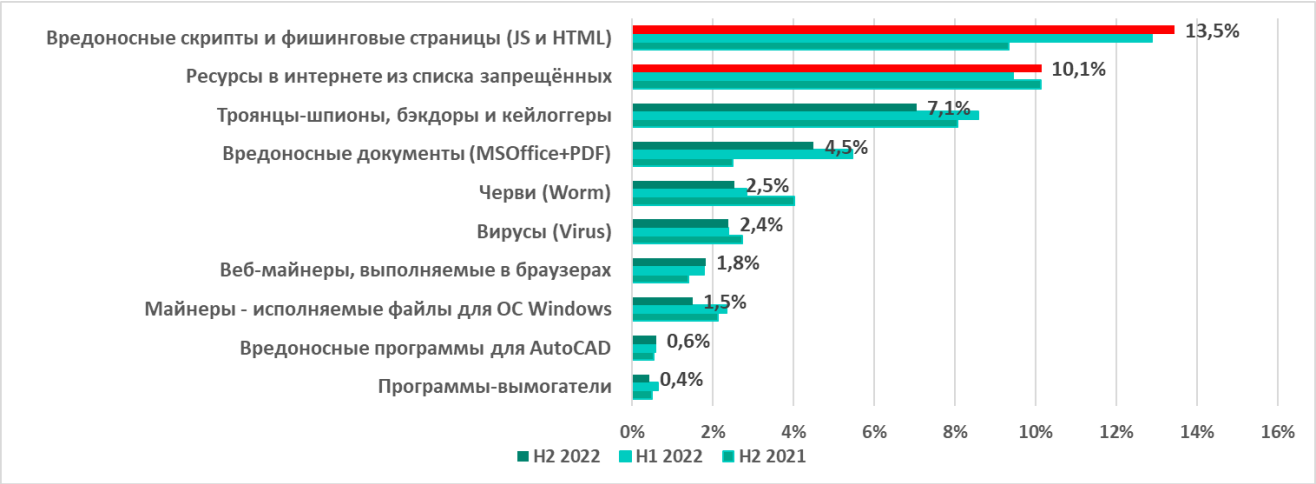
Во втором полугодии 2022 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано вредоносное ПО из 7684 различных семейств.

Количество семейств вредоносного ПО, заблокированного на компьютерах АСУ



Категории вредоносных объектов

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям. Краткое описание каждого типа угроз представлено в отдельном документе.



Процент компьютеров АСУ*, на которых была предотвращена активность вредоносных объектов различных категорий

*Заметим, что получившиеся проценты некорректно суммировать, потому что во многих случаях на одном компьютере за отчётный период могли быть заблокированы угрозы двух и более типов.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

В первом полугодии 2022 года в аналогичном рейтинге увеличились показатели нескольких категорий вредоносных объектов. Во втором полугодии подросли только две лидирующие в этом рейтинге категории — вредоносные скрипты и фишинговые страницы (JS и HTML) и ресурсы из интернета из списка запрещённых. Показатели остальных категорий вредоносных объектов во втором полугодии 2022 года либо уменьшились, либо остались без изменений.

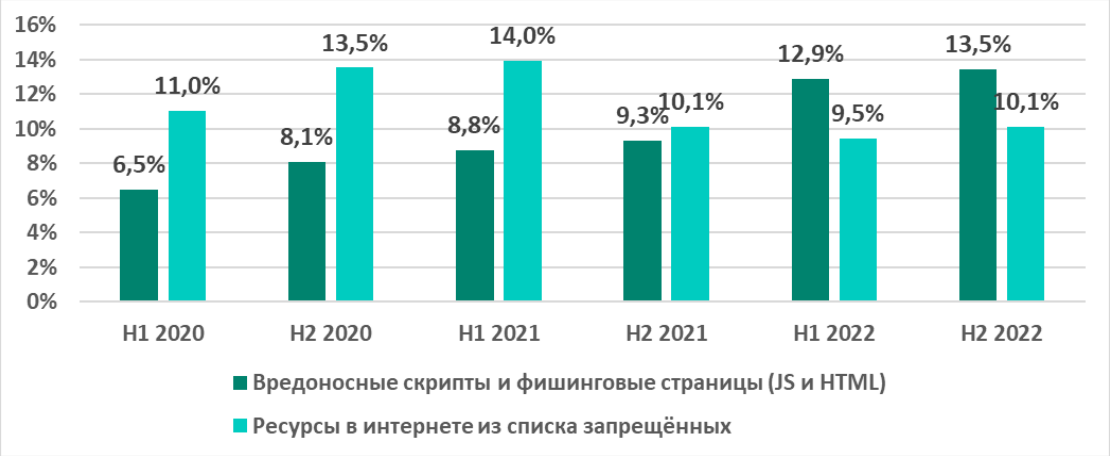
Вредоносные скрипты и фишинговые страницы (JS и HTML) и ресурсы из интернета из списка запрещенных

Вредоносные скрипты и фишинговые страницы (JS и HTML) распространяются как в интернете, так и в письмах, рассылаемых в электронной почте. Для распространения вредоносных скриптов и фишинговых страниц используется значительная часть ресурсов из интернета из списка запрещённых.

Вредоносные скрипты применяются злоумышленниками для выполнения большого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО и/или программ для скрытого майнинга криптовалюты).

В 2022 году вредоносные скрипты и фишинговые страницы потеснили в этом рейтинге многолетнего лидера — ресурсы из интернета из списка запрещённых.

Процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы и ресурсы в интернете из списка запрещенных



Рост активности угроз этих двух категорий очевидно внес значительный вклад в увеличение во втором полугодии 2022 года процента компьютеров АСУ, на которых блокировались угрозы, источником которых стал интернет (см. ниже).

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Среди регионов самый высокий процент компьютеров АСУ, на которых были заблокированы ресурсы из интернета из списка запрещенных, в Центральной Азии и в России (15,2% и 13,9% соответственно). Неудивительно, что эти регионы лидируют по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета.

Эти же регионы внесли основной вклад в рост процента компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы. Причиной этого стало массовое заражение сайтов (в том числе промышленных организаций), использующих необновлённую и устаревшую версию CMS, о которой мы писали выше.

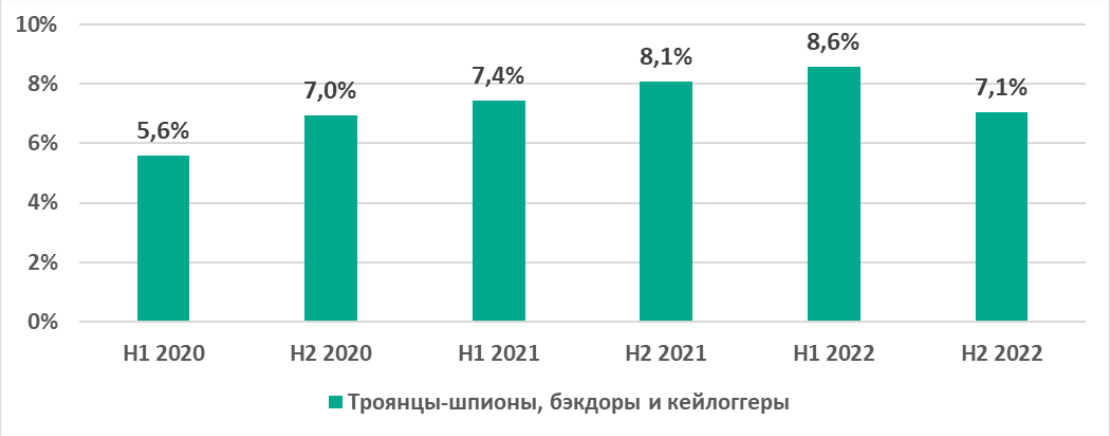
В России был отмечен самый высокий показатель из всех регионов (18,2%) и самый значительный рост — +11 п.п. по сравнению с первым полугодием. Центральная Азия с 14,2% заняла четвертое место в рейтинге регионов по этому показателю, однако в регионе также отмечен его заметный рост за второе полугодие — +5,7 п.п.

В остальных регионах мира процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, не увеличился.

Программы-шпионы

На 1,5 п.п. уменьшился процент компьютеров АСУ, на которых блокируются программы-шпионы. Рост этого показателя мы наблюдали с 2020 года до первого полугодия 2022 года включительно.

Процент компьютеров АСУ, на которых были заблокированы программы-шпионы



Отметим, что во втором полугодии 2022 года процент компьютеров АСУ, на которых были заблокированы программы-шпионы, в Африке составил 12%. Это максимум среди всех регионов. Высок также этот показатель в Юго-Восточной Азии (10%) и на Ближнем Востоке (9,8%).

Среди стран и территорий по этому показателю лидируют Йемен (22,3%), Алжир (18,3%), Шри-Ланка (18,3%) и Сербия (17,2%).

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Вредоносные документы (MSOffice+PDF)

Уменьшился на 1 п.п. и процент компьютеров АСУ, на которых были заблокированы вредоносные документы (MSOffice+PDF) — с 5,5% до 4,5%. Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров.

Среди регионов самый высокий процент компьютеров АСУ, на которых были заблокированы вредоносные документы, — в Южной Европе (6,9%) и в Латинской Америке (6,9%). Эти же регионы лидируют по проценту компьютеров АСУ, на которых были заблокированы угрозы из почты.

Вредоносные программы для скрытого майнинга криптовалюты

Процент компьютеров АСУ, на которых были заблокированы вредоносные майнеры — исполняемые файлы для ОС Windows, уменьшился на 0,8 п.п. Показатель веб-майнеров во втором полугодии 2022 года остался таким же, как в первом.

Процент компьютеров АСУ, на которых были заблокированы вредоносные программы для скрытого майнинга криптовалюты

Майнеры часто распространяются на сайтах, на которые пользователей перенаправляют вредоносные скрипты, размещённые злоумышленниками на различных медиаресурсах и сайтах с пиратским контентом.

Среди регионов во втором полугодии 2022 года лидируют по проценту компьютеров АСУ, на которых были заблокированы: майнеры - исполняемые файлы для ОС Windows — Центральная Азия (3,8%); веб-майнеры — Африка (3,4%).

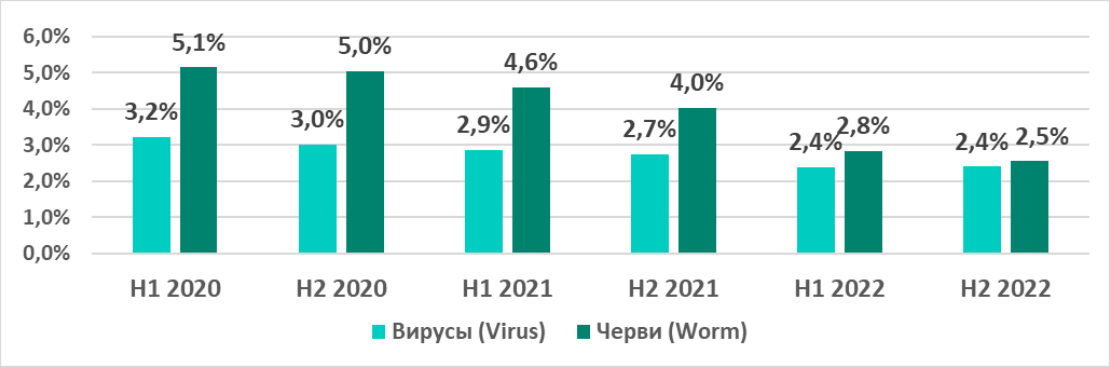
Среди трех стран, лидирующих по веб-майнерам, наряду с Йеменом (9,3%) и Египтом (7,8%) неожиданно оказалась и европейская страна — Сербия (7,5%).

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Вирусы и черви

Продолжает уменьшаться процент компьютеров АСУ, на которых блокируются вирусы и черви. Мы полагаем, что это косвенно свидетельствует о планомерной работе по развёртыванию защитных решений в ОТ-инфраструктурах, что устраняет очаги заражения и препятствует распространению самораспространяющегося вредоносного ПО.

Процент компьютеров АСУ, на которых были заблокированы вирусы и черви



Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

Уменьшение процента компьютеров АСУ, на которых блокируется такое вредоносное ПО, обусловлено, в том числе, и более тщательной проверкой съемных носителей.

Между тем, процент компьютеров АСУ, на которых детектируются черви, по-прежнему весьма высок в Африке (7,1%), которая, как следствие, лидирует среди регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей. А вирусы остаются актуальной проблемой для Юго-Восточной Азии (8,1%).

Среди распространяющихся вирусов и червей довольно много старых, их командные серверы уже отключены. Однако они не только ослабляют безопасность зараженных систем — например, открывая сетевые порты и изменяя конфигурацию, — но также могут приводить к сбоям в работе ПО и отказам в обслуживании.

В сетях АСУ встречаются и новые версии червей, используемые злоумышленниками для распространения в сети шпионского ПО, программ-вымогателей и майнеров. Чаще всего для распространения по сети эти черви используют эксплойты для исправленных производителями, но еще актуальных в технологических сетях уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Вредоносные программы для AutoCAD

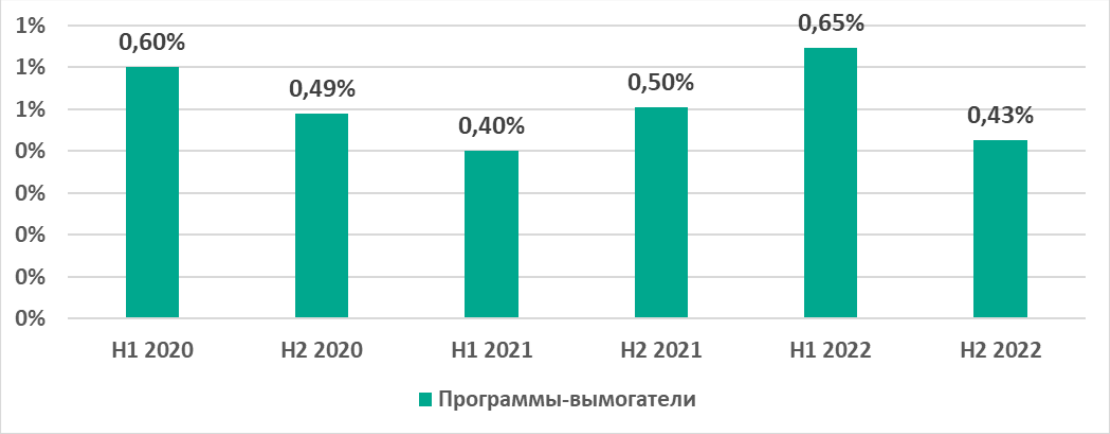
Вредоносное ПО для AutoCAD, в частности вирусы, детектируются преимущественно в Восточной Азии (3,1%) — на компьютерах технологических сетей, в том числе в сетевых папках и на рабочих станциях инженеров.

Среди стран по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, лидируют Эфиопия (5,8%), Шри-Ланка (5,0%) и Китай (4,9%). Показатели остальных стран — от 3,2% до 0,01%.

Программы-вымогатели

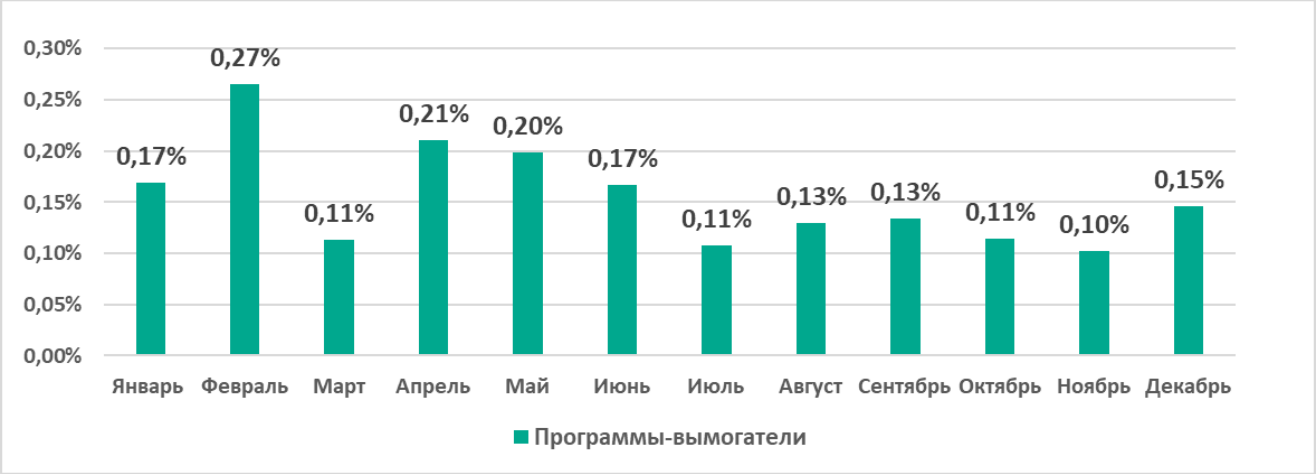
Во втором полугодии 2022 года вредоносные программы-вымогатели были заблокированы на 0,43% компьютеров АСУ.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели



Наибольший процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, в течение 2022 года был отмечен в феврале (0,27%), наименьший — в ноябре (0,10%).

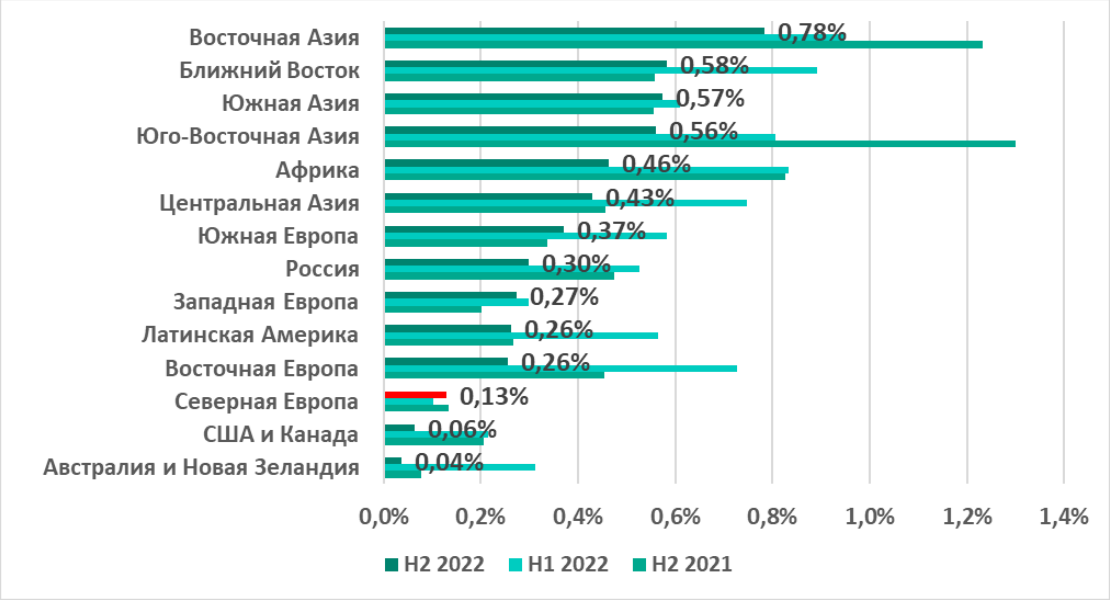
© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь — декабрь 2022

Во втором полугодии 2022 процент атакованных вымогателями компьютеров АСУ уменьшился практически во всех регионах мира, лишь в Северной Европе отмечен незначительный рост (+0,03 п.п.).

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2022



Рейтинг регионов по-прежнему возглавляют Восточная Азия и Ближний Восток, а Африку с третьего места потеснили Южная и Юго-Восточная Азия.

Среди стран и территорий во втором полугодии 2022 года по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, лидируют Йемен и Афганистан. В Афганистане по сравнению с первым полугодием процент увеличился на максимальные среди всех стран 3,22 п.п.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2022

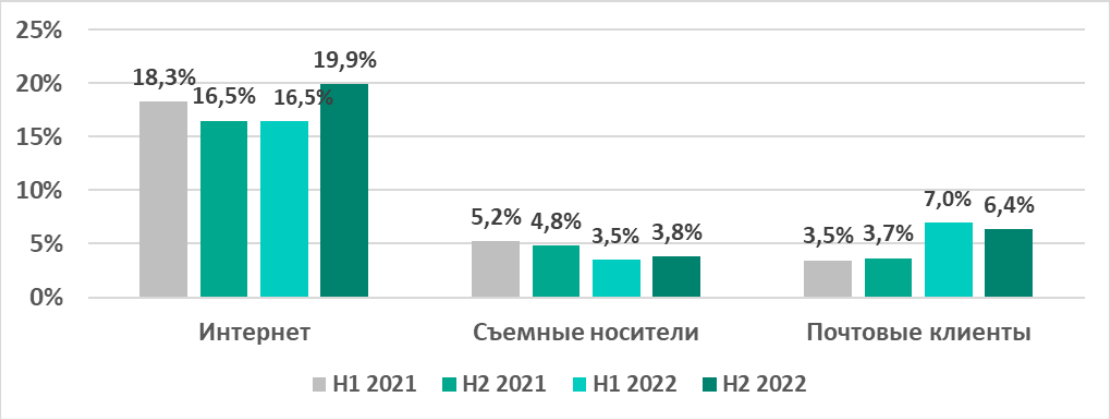
Отметим, что по итогам полугодия в этот рейтинг попала и одна европейская страна — Северная Македония.

Основные источники угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, съемные носители и почтовые клиенты. Отметим, что источники заблокированных угроз надёжно установить удается не во всех случаях.

Мир

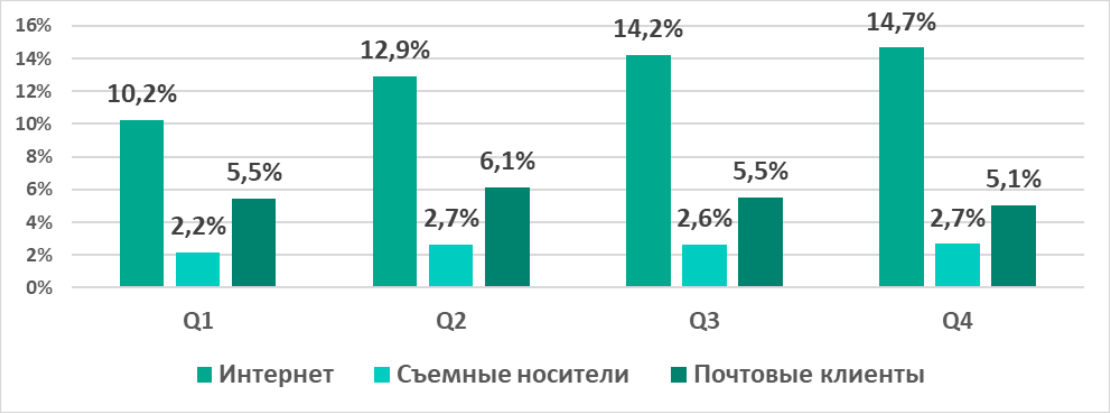
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников



От квартала к кварталу 2022 года рос процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, в то время как максимум угроз из электронной почты пришелся на второй квартал — заметный для этого показателя рост был отмечен в июне.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

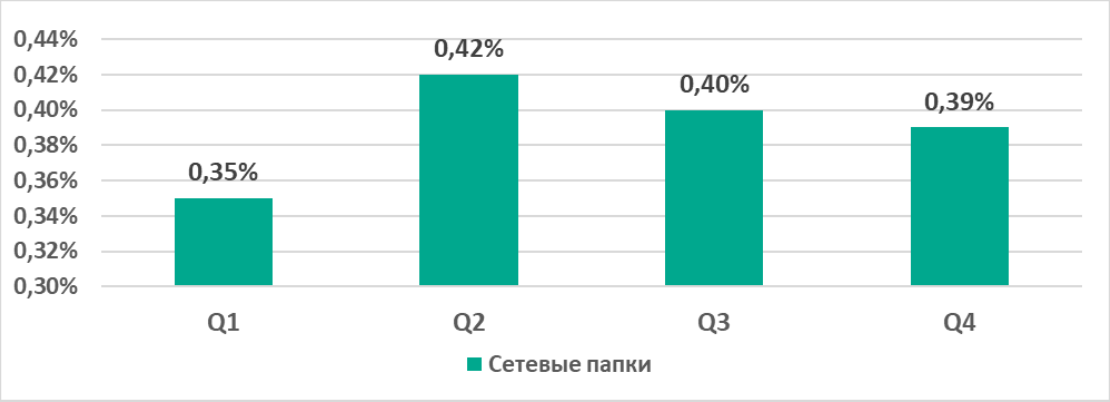
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников, Q1 — Q4 2022 года



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из почты, январь — декабрь 2022 года

Заметно увеличился во втором квартале 2022 года и процент компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в сетевых папках, Q1 — Q4 2022 года



Во втором полугодии 2022 года угрозы, источником которых стали сетевые папки, были заблокированы на 0,6% компьютеров АСУ.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

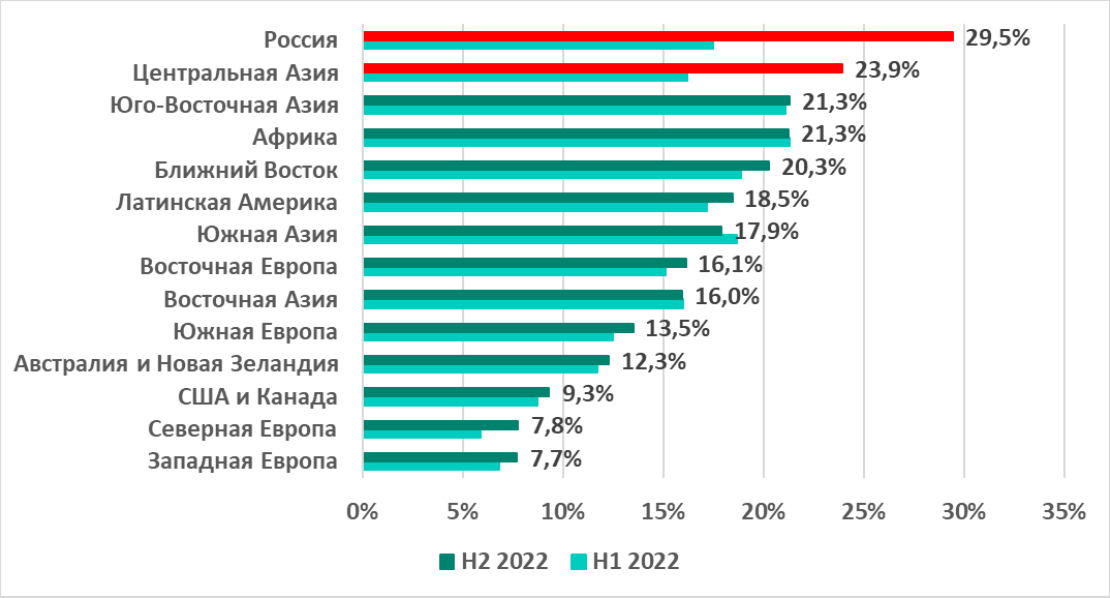
Как и в случае с общей статистикой по всем угрозам, процент компьютеров АСУ, на которых заблокированы вредоносные объекты из различных источников, отличается в разных регионах и странах.

Регионы и страны

Интернет

Во втором полугодии 2022 года в регионах Россия и Центральная Азия был отмечен весьма значительный рост процента компьютеров АСУ, на которых были заблокированы угрозы из интернета, — на 12 и 7,8 п.п. соответственно. В результате эти регионы заняли первые в места в рейтинге по этому показателю, потеснив традиционных лидеров — Африку, Юго-Восточную Азию и Ближний Восток.

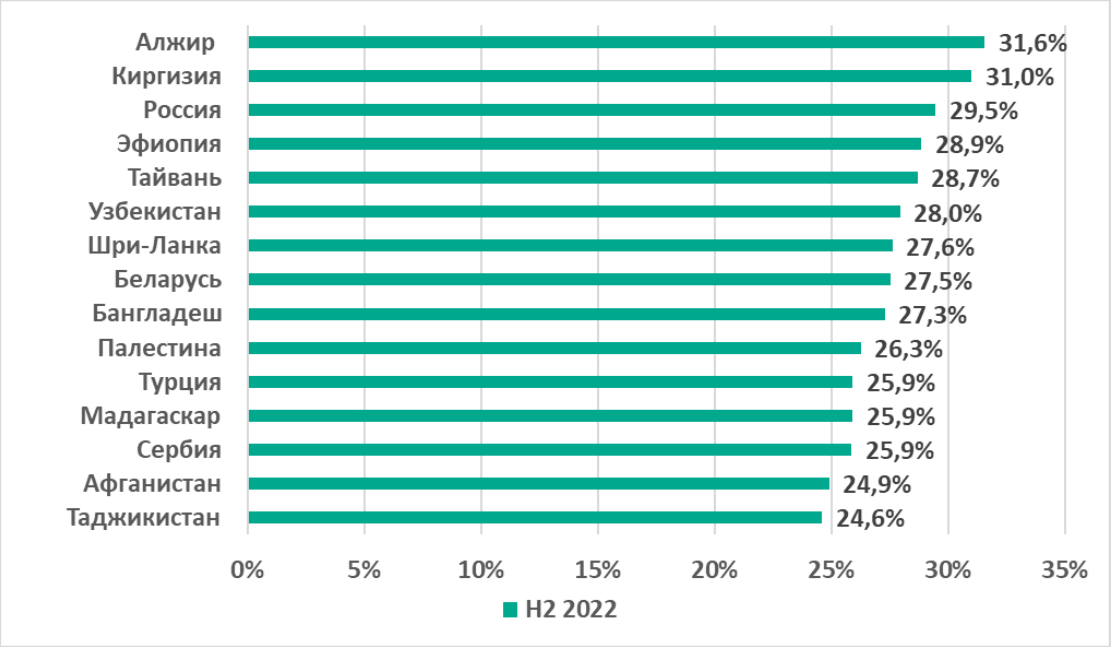
Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2022



Резкий рост в России процента компьютеров АСУ, на которых были заблокированы угрозы из интернета, привел к тому, что по этому показателю страна оказалась в тройке лидеров среди стран и территорий мира.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2022

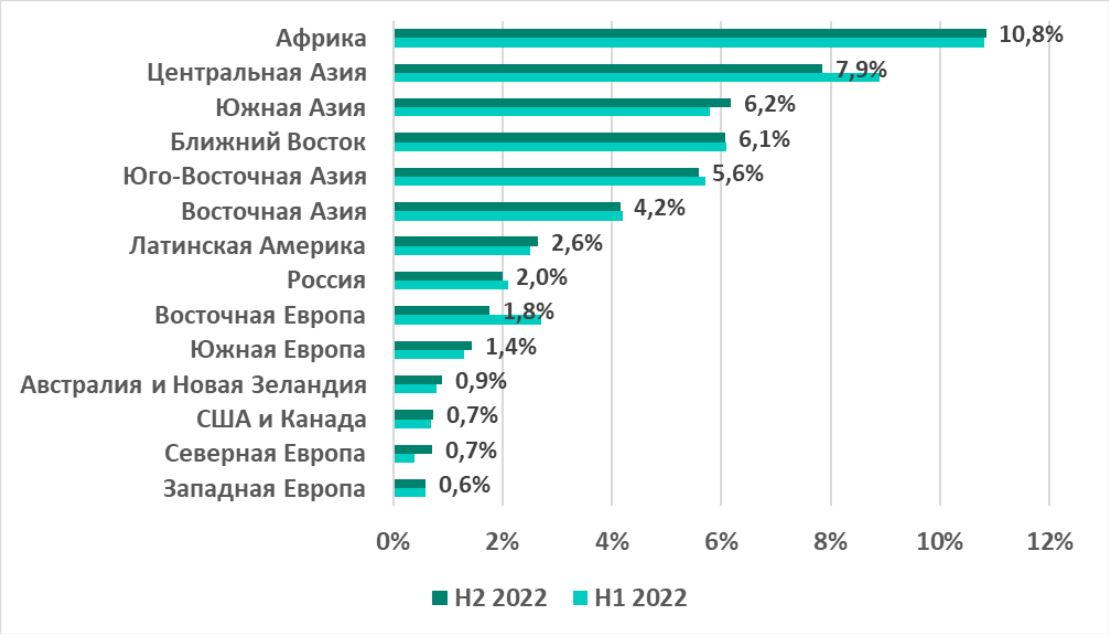


Отметим, что для России не характерны столь высокие позиции в обоих рейтингах.

Съемные носители

Рейтинг регионов по проценту компьютеров АСУ, на которых при подключении съемных носителей было заблокировано вредоносное ПО, традиционно возглавляет Африка.

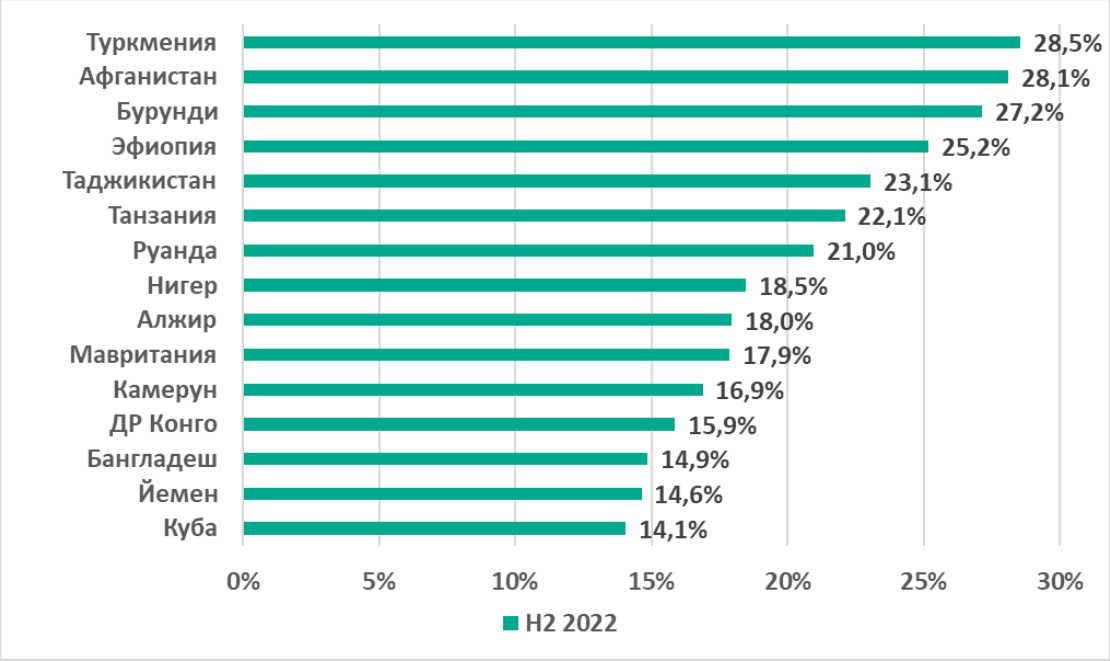
Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, второе полугодие 2022



© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Среди 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, преобладают страны Африки.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, второе полугодие 2022

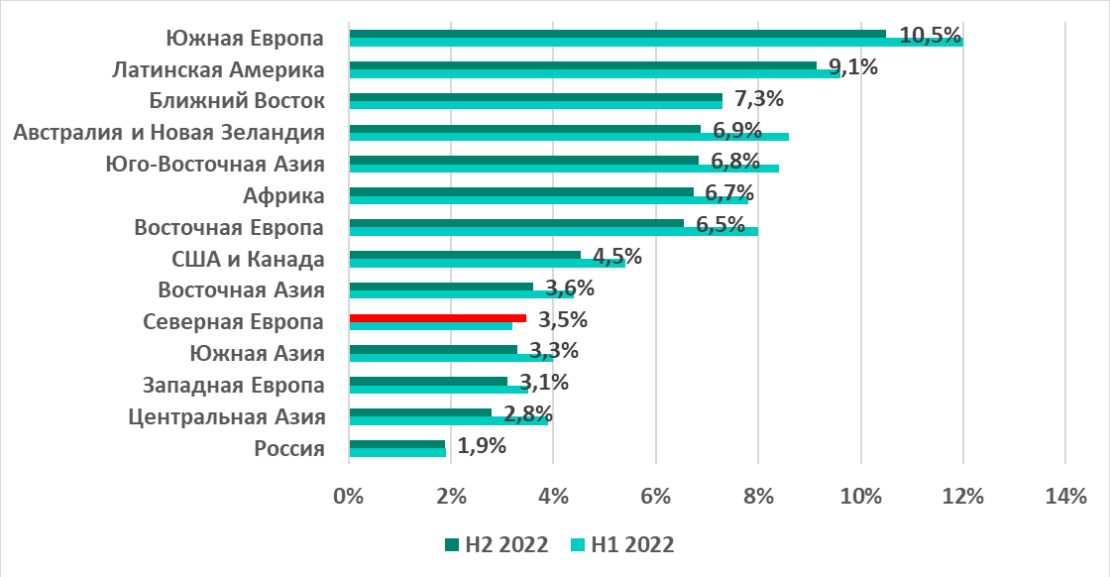


Почтовые клиенты

Южная Европа, которая в первой половине 2022 года возглавила рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, во втором полугодии сохранила лидирующую позицию в этом рейтинге. Единственным регионом, в котором во втором полугодии 2022 года показатель вырос (всего на 0,3 п.п.), стала Северная Европа.

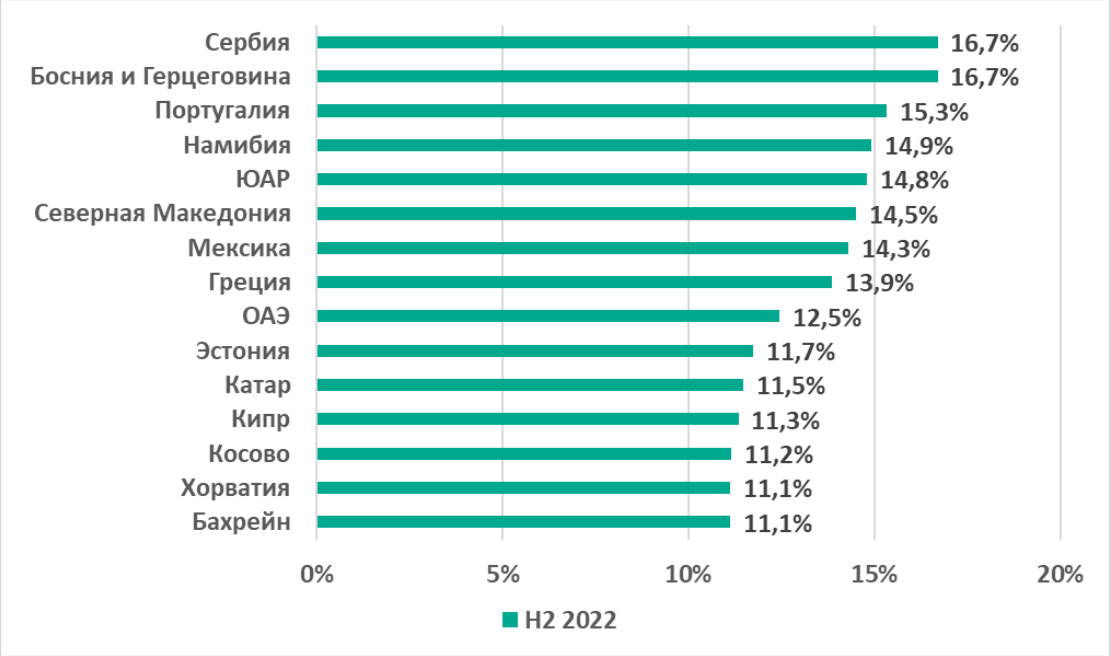
© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, второе полугодие 2022



В список 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, попали страны как из Южной Европы, так и из других регионов.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, второе полугодие 2022



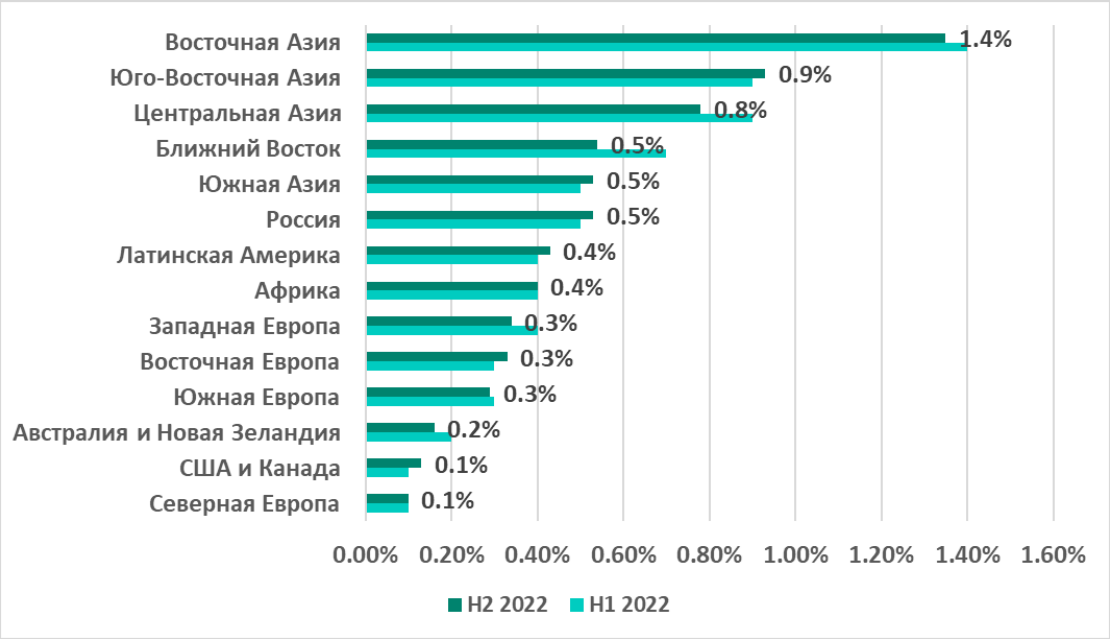
Мы рекомендуем специалистам по безопасности в этих странах обратить особое внимание на защиту сотрудников предприятий от фишинговых рассылок.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Сетевые папки

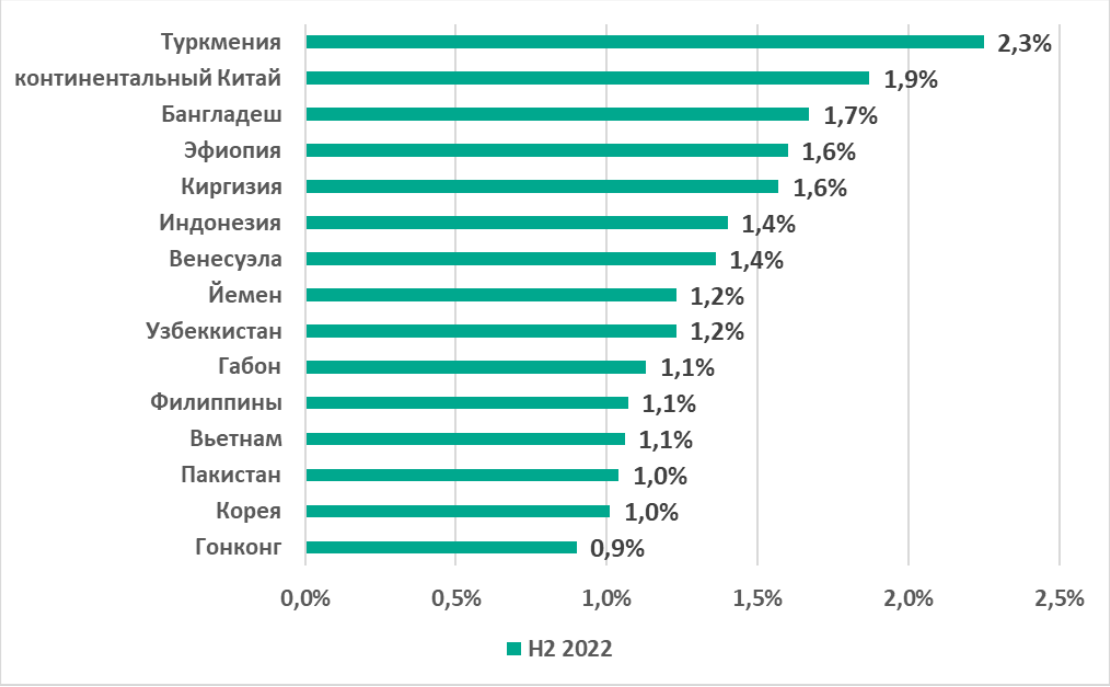
Один из минорных источников вредоносных объектов. Больше всего процент компьютеров АСУ, на которых угрозы блокируются в сетевых папках, в Восточной, Юго-Восточной и Центральной Азии.

Рейтинг регионов по проценту компьютеров АСУ, на которых вредоносные объекты были заблокированы в сетевых папках, второе полугодие 2022



Среди стран и территорий лидируют Туркмения, континентальный Китай и Бангладеш.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых вредоносные объекты были заблокированы в сетевых папках, второе полугодие 2022



© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Методика подготовки статистики

В отчете представлены результаты анализа статистических данных, полученных с помощью распределенной антивирусной сети Kaspersky Security Network (KSN). Данные получены от тех пользователей KSN, которые добровольно подтвердили свое согласие на их анонимную передачу и обработку с целью, описанной в Соглашении KSN для установленного на их компьютере продукта «Лаборатории Касперского».

Подключение к сети KSN даёт нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счёт обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за её объёма и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные в значительной мере не только помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT[1].

Статистические данные, представленные в отчете, получены с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky ICS CERT относит к технологической инфраструктуре организаций. В эту группу входят компьютеры, работающие на операционных системах Windows и выполняющие одну или несколько функций:

- серверы управления и сбора данных (SCADA);
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human Machine Interface (HMI);
- компьютеры, используемые для администрирования технологических сетей;
- компьютеры, используемые для разработки ПО для систем промышленной автоматизации.

[1] Организациям, в отношении любых данных которых наложены ограничения на их передачу во вне периметра организации, рекомендуем рассмотреть вариант использования сервиса Kaspersky Private Security Network.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Атакованными мы считаем те компьютеры, на которых в течение исследуемого периода (на графиках выше это месяц, полугодие, год — в зависимости от контекста) защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете процента машин, на которых было предотвращено заражение вредоносным ПО, используется количество компьютеров, атакованных в течение исследуемого периода, по отношению ко всем компьютерам из нашей выборки, с которых в течение исследуемого периода мы получали обезличенную информацию.

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com

© 2023 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»