kaspersky

Ландшафт угроз для систем промышленной автоматизации

Второе полугодие 2021

Kaspersky ICS CERT

03.03.2022 Version 1.0

2021 — цифры

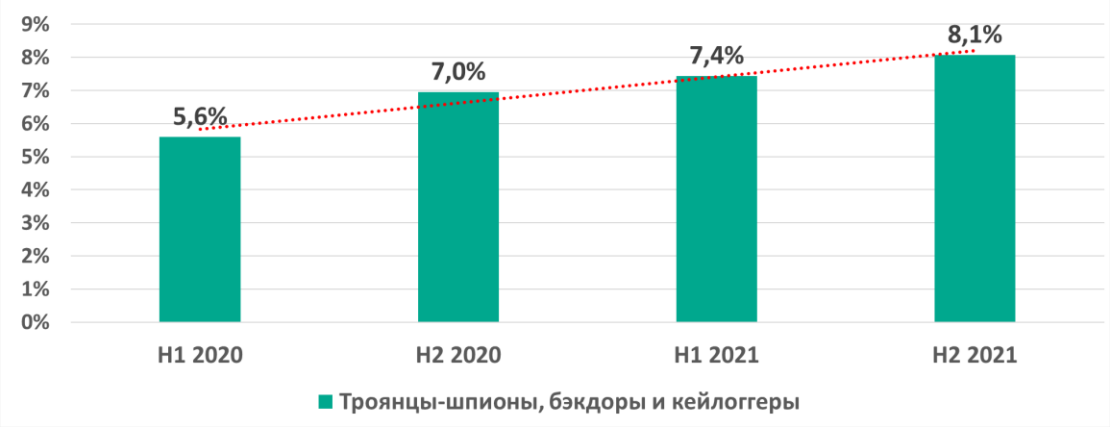
Показатель	H1 2021	H2 2021	2021
Процент атакованных компьютеров АСУ в мире	33,8%	31,4%	39,6%
Процент атакованных компьютеров АСУ в регионах			
Северная Европа	11,1%	10,4%	12,1%
США и Канада	16,5%	17,2%	19,7%
Западная Европа	15,3%	15,8%	20,2%
Австралия и Новая Зеландия	23,7%	21,4%	26,5%
Восточная Европа	29,5%	28,4%	32,4%
Южная Европа	29,4%	25,1%	33,0%
Латинская Америка	32,8%	32,5%	38,7%
Южная Азия	35,2%	35,6%	41,0%
Ближний Восток	37,3%	34,3%	42,0%
Россия	39,4%	30,0%	42,3%
Центральная Азия	42,0%	37,9%	44,7%
Восточная Азия	43,2%	40,5%	48,1%
Африка	46,1%	43,4%	50,9%
Юго-Восточная Азия	44,2%	47,6%	51,2%
Основные источники угроз в мире			
Интернет	18,3%	16,5%	22,2%
Съемные носители	5,2%	4,8%	6,7%
Почтовые клиенты	3,5%	3,7%	4,2%

Тенденции

С первого полугодия 2020 вырос процент компьютеров АСУ, на которых блокируется:

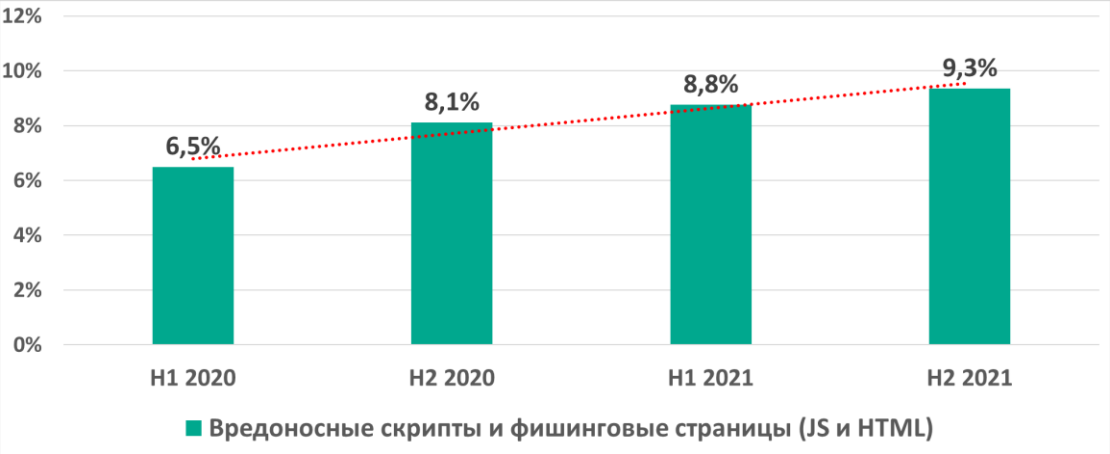
- **Шпионское ПО** — в 1,4 раза — с 5,6% до 8,1%.

Процент компьютеров АСУ, на которых было заблокировано шпионское ПО



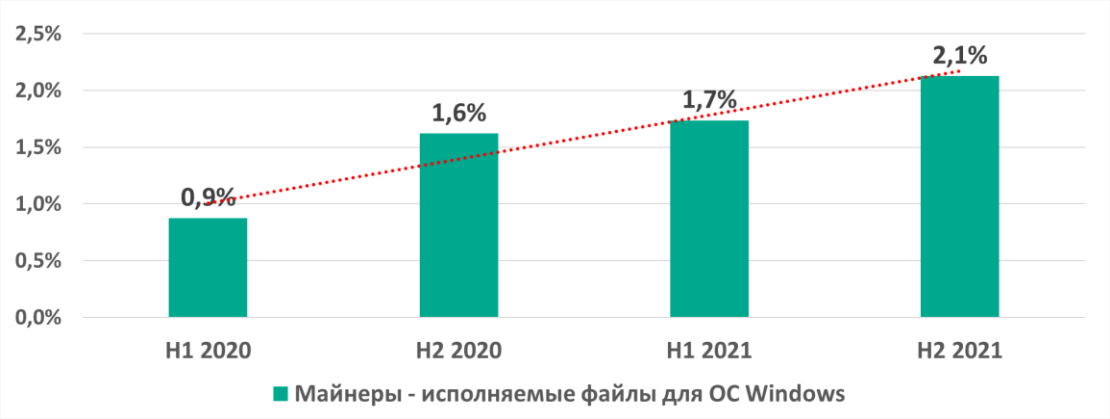
- **Вредоносные скрипты и фишинговые страницы** — в 1,4 раза — с 6,5% до 9,3%.

Процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишиновые страницы (JS и HTML)



- **Майнеры — исполняемые файлы для ОС Windows** — более чем вдвое — с 0,9% до 2,1%.

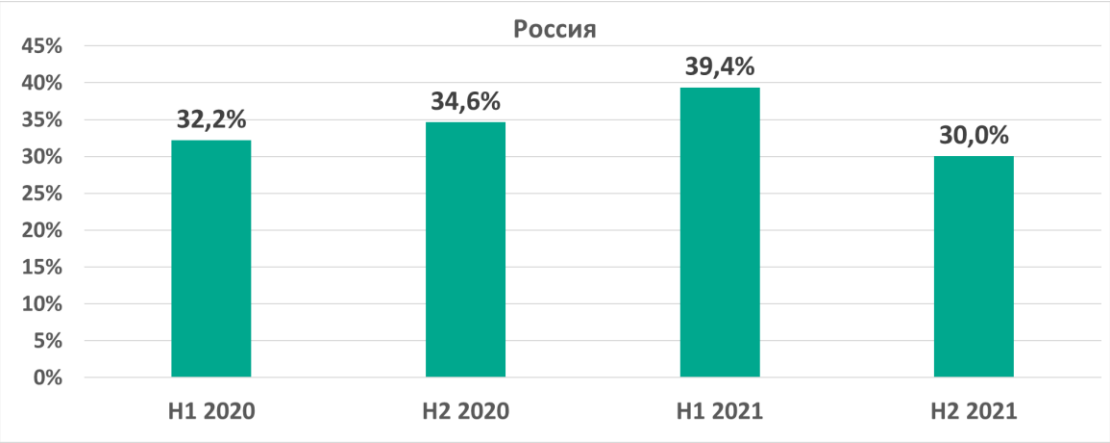
Процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows



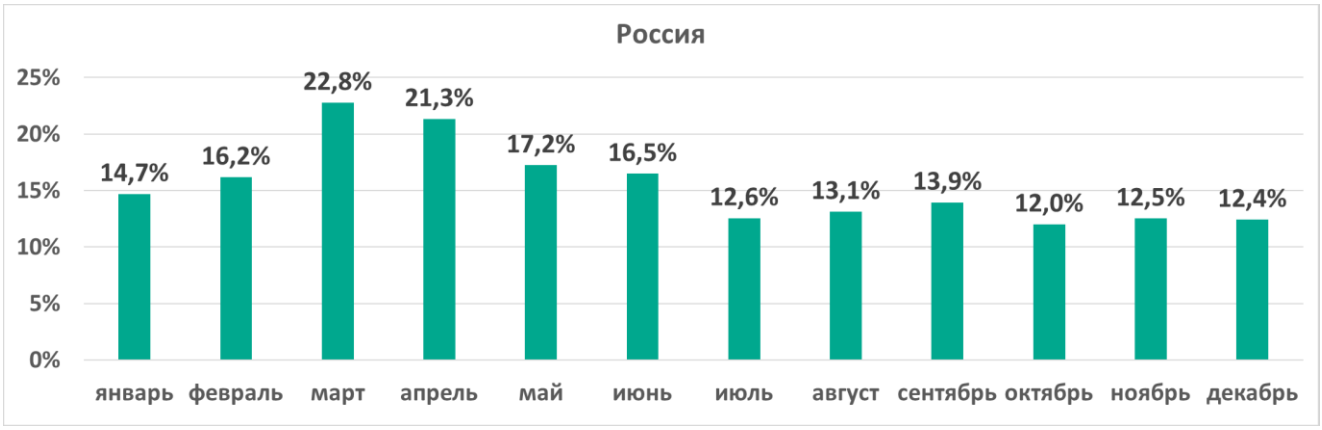
Россия, второе полугодие 2021

В России во втором полугодии 2021 года хотя бы один раз вредоносные объекты были заблокированы на 30% компьютеров АСУ. Это на 9,4 п.п. меньше, чем в предыдущем полугодии. Столь заметное снижение наблюдается в России впервые за полтора года.

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



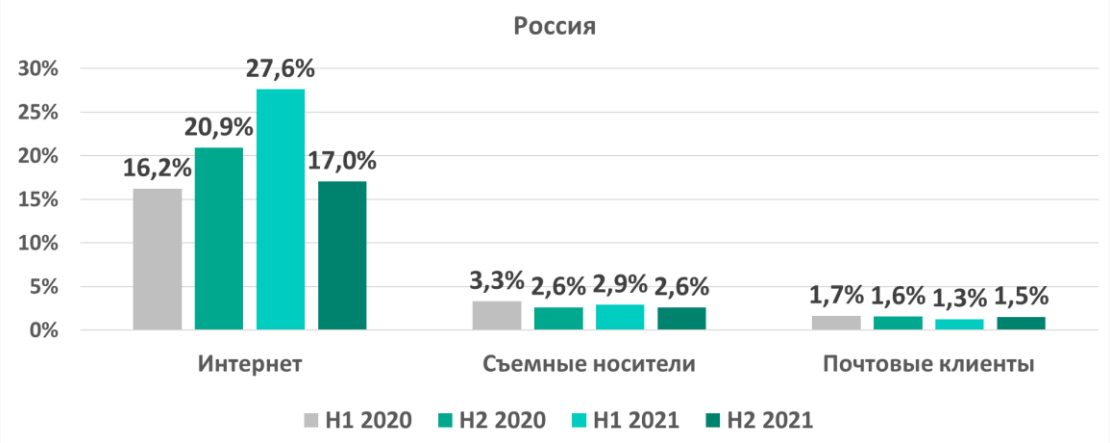
В первом полугодии процент ежемесячно атакуемых компьютеров АСУ в России был заметно выше, чем во втором полугодии. Самый высокий показатель был отмечен в марте (22,8%), самый низкий — в октябре (12,0%).



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

Уменьшение в России процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, обусловлено резким снижением процента компьютеров АСУ, на которых были заблокированы угрозы из интернета. Этот показатель рос с 2020 года, но во втором полугодии 2021 вернулся к значениям, близким к показателю первой половины 2020.

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



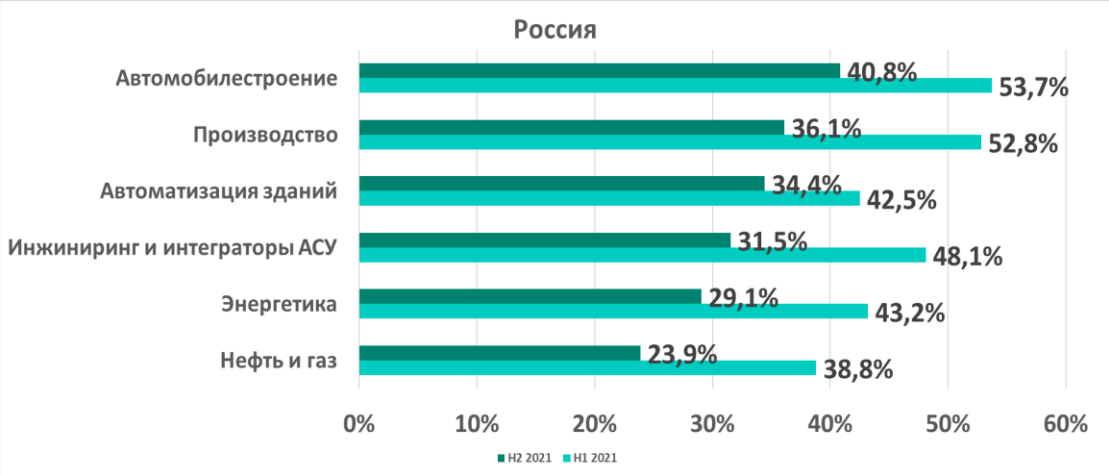
Снижение процента атакованных компьютеров связано с уменьшением процента компьютеров АСУ, на которых блокировался доступ к веб-ресурсам из списка запрещенных. Такое значительное изменение ландшафта угроз связано с рядом факторов, в частности:

- с проактивным блокированием скриптов, встраиваемых в расширения для веб-браузеров и позволяющих удаленно загружать и выполнять произвольный код JS;
- с уменьшением количества веб-ресурсов, которые прямо или косвенно (например, через рекламные модули, которые также способны загружать произвольный JS код из недоверенных источников) распространяли вредоносные скрипты.

Топ таких ресурсов и связанные с ними вредоносные скрипты были в значительной мере распространены на территории России и в странах СНГ. Именно поэтому наиболее заметно процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился в России (-9,3 п.п.) и Беларуси (-11,3 п.п.).

По тем же причинам во втором полугодии 2021 в России уменьшились показатели исследуемых индустрий.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых индустриях, первое и второе полугодия 2021



Общая статистика по миру

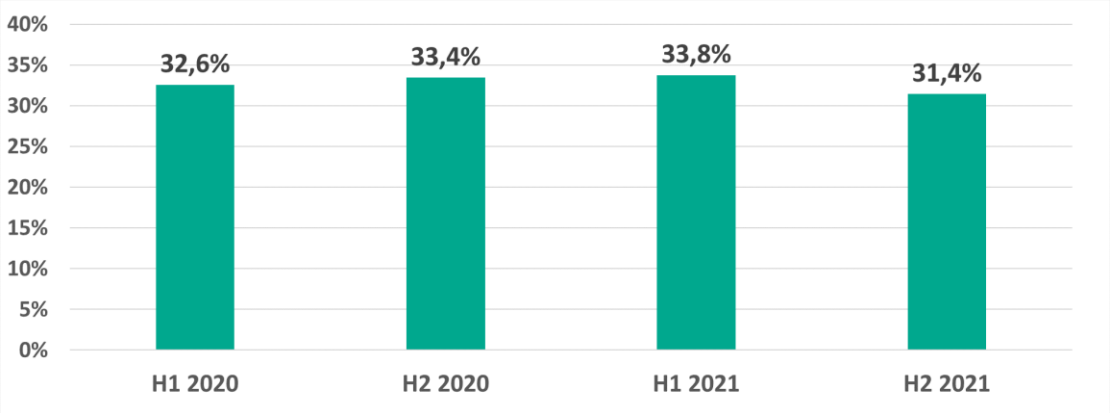
2021 — второй год жизни и работы в условиях, осложненных пандемией. В отличие от 2020, в 2021 к пандемии привыкли — и сотрудники промышленных компаний, и специалисты по ИТ безопасности, и злоумышленники. Если рассматривать статистику за 2020 и 2021 годы, то год 2021 кажется более стабильным, особенно его вторая половина.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

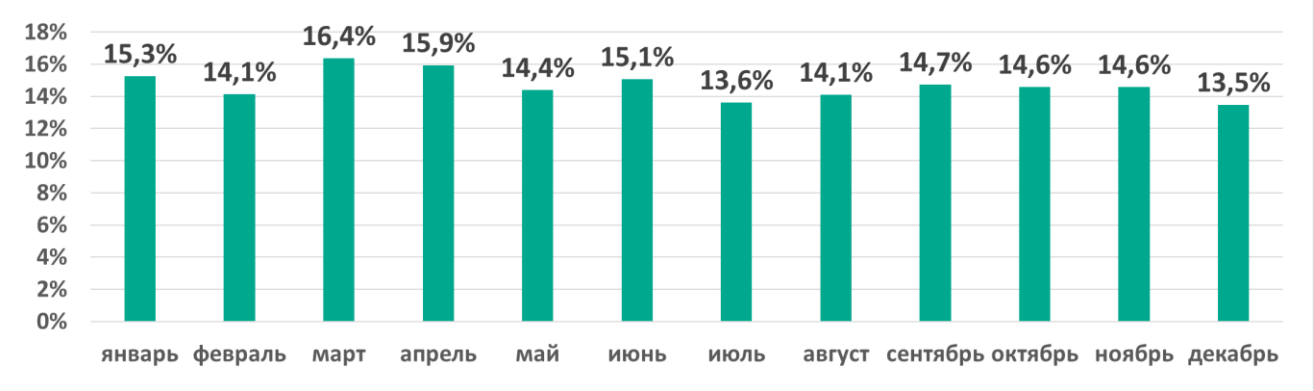
В 2021 году процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличился по сравнению с 2020 на 1 п.п.– с 38,6% до 39,6%.

Однако если рассматривать ситуацию по полугодиям, то картинка выглядит более оптимистичной: во второй половине 2021 года впервые за полтора года показатель снизился (на 1,4 п.п.).

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



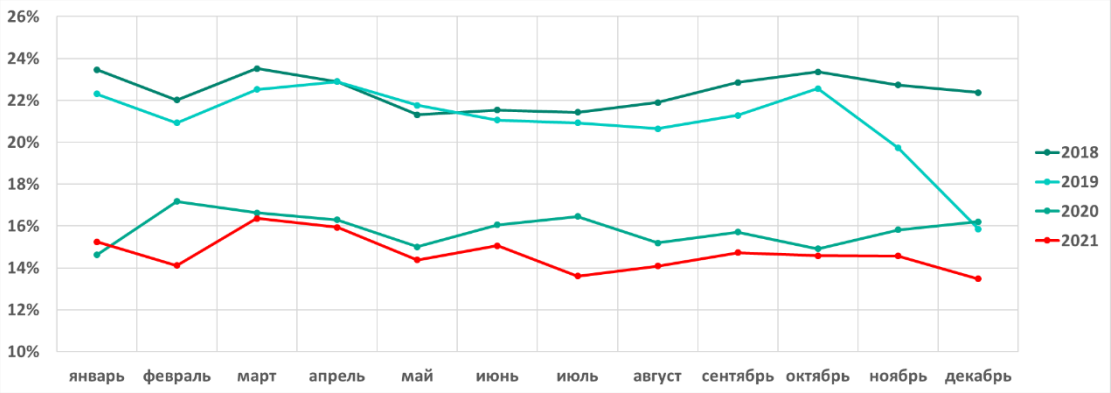
На графике, отражающем динамику изменения процента атакованных компьютеров АСУ по месяцам, видно, что показатели второго полугодия 2021 были более стабильными, чем первого — с более низкими значениями и без резких перепадов.



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2021

Отметим также, что вектор изменения показателя от месяца к месяцу (больше — меньше) в 2021 году чаще совпадает с изменениями аналогичных показателей за 2019 и особенно за 2018 год, чем за 2020. В частности, мы видим падение в июле и августе, связанное, как мы предполагаем, с наступлением традиционного времени отпусков. Однако по сравнению с 2018 и 2019 годами летнее понижение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, не так ярко выражено.

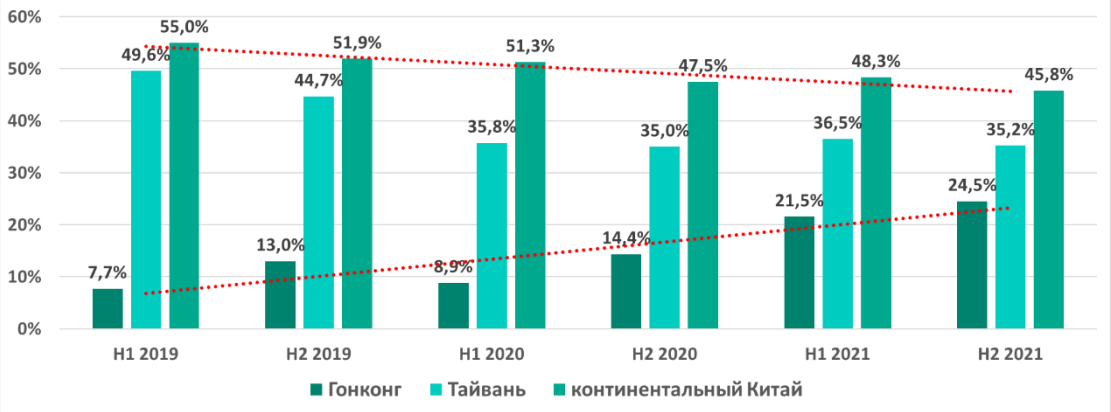
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2018 — 2021



В разных странах ситуация значительно отличается. Так, процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, во втором полугодии 2021 варьирует от 8,5% в Люксембурге до 54,9% во Вьетнаме.

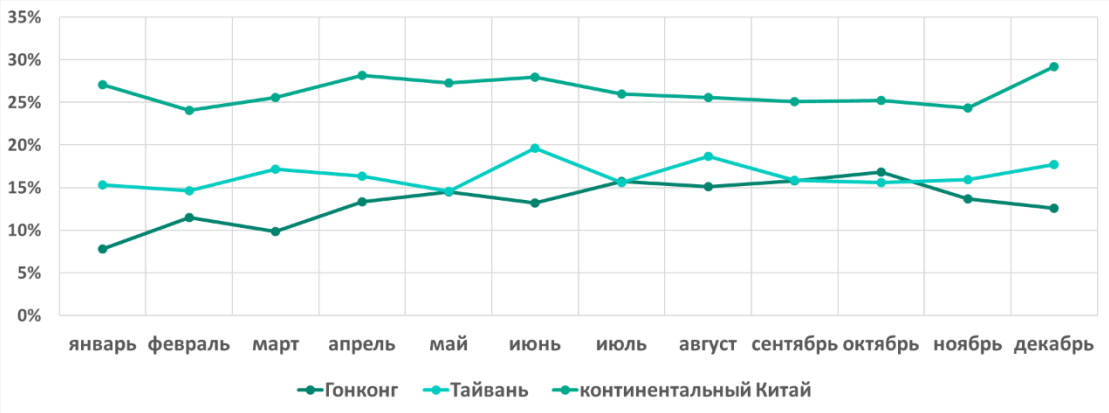
Динамика изменений показателя в разных странах и территориях оказывается различной. Так, например, в Гонконге этот показатель продолжает расти. В то же время процент атакованных компьютеров АСУ в Тайване и, что особенно заметно, в континентальном Китае постепенно уменьшается.

Гонконг, Тайвань и континенталь-ный Китай. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



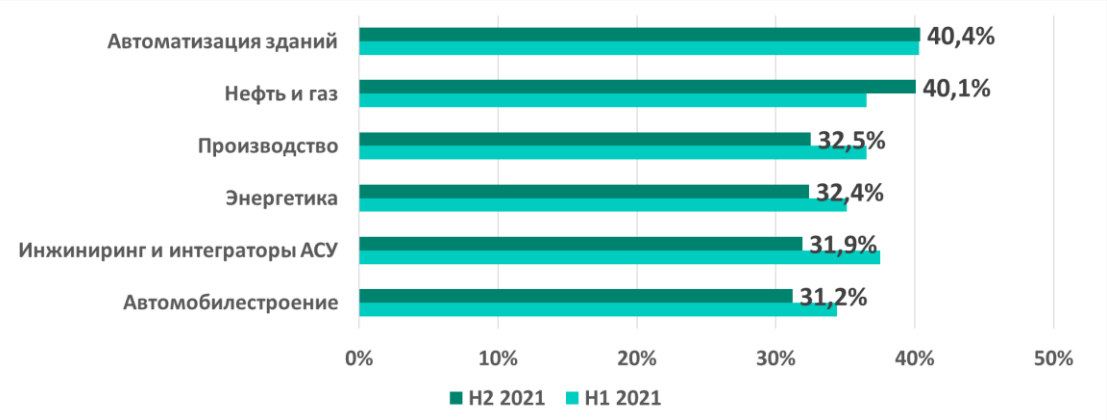
Любопытно, что при этом динамика процента атакованных компьютеров АСУ в Тайване и Гонконге по месяцам 2021 года оказывается противоположной, показатели находятся в противофазах — когда растёт показатель в Гонконге, он уменьшается в Тайване, — и наоборот.

Гонконг, Тайвань и континенталь-ный Китай. Процент компьютеров АСУ, на которых были заблокиро-ваны вредонос-ные объекты, январь — декабрь 2021



Некоторые индустрии

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

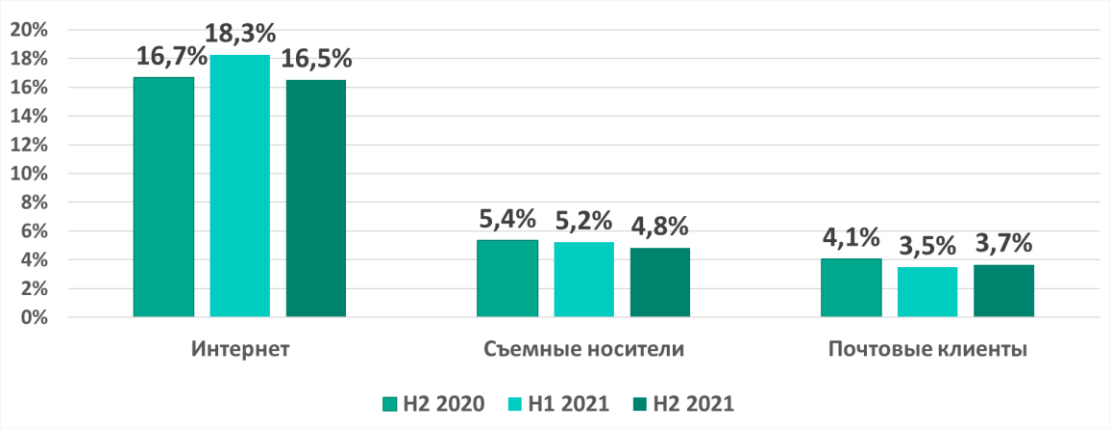


Нефтегазовая отрасль — единственная индустрия, где во втором полугодии вырос процент компьютеров АСУ, на которых были заблокированы вредоносные объекты (+ 3,5 п.п.). Напомним, что в первом полугодии 2021 года уменьшились показатели всех исследуемых индустрий, наиболее значительно как раз в нефтегазовой (-7,5 п.п.).

Основные источники угроз

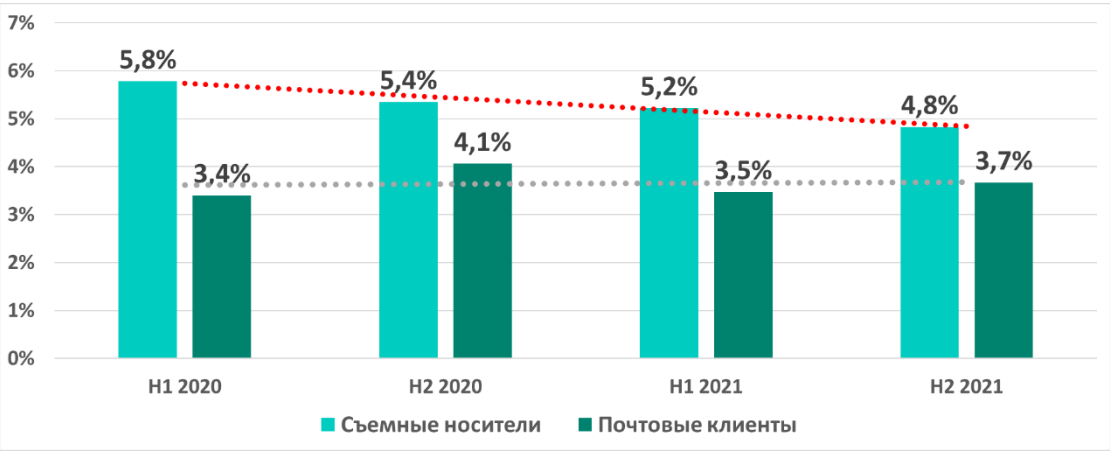
Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, съемные носители и электронная почта. Отметим, что источники заблокированных угроз надёжно установить удается не во всех случаях.

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



Интернет традиционно лидирует, съемные носители в статистике по миру занимают второе место, а почтовые клиенты — третье. Однако постепенно меняется соотношение между последними двумя источниками. От полугодия к полугодию показатель съемных носителей падает.

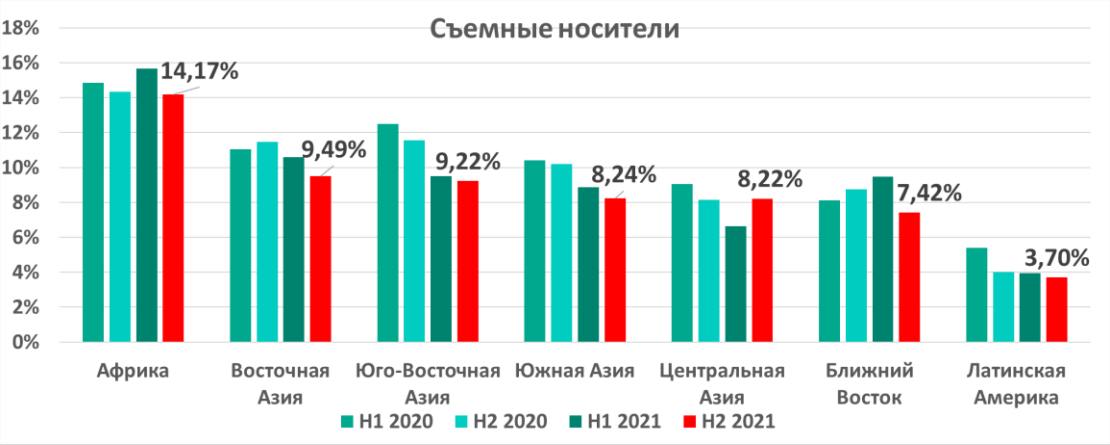
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты при подключении съемных носителей и в почтовых вложениях



По нашему мнению, падение процента компьютеров АСУ, на которых вредоносное ПО заблокировано при подключении съёмных носителей, свидетельствует о том, что на предприятиях ведётся планомерная работа по повышению минимального уровня защиты — в сети снижается количество незащищённых систем, являющихся внутренним источником заражения вредоносным ПО через съёмные носители (в основном, «червями»).

Основной вклад в мировые показатели по проценту компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, вносят Африка и Азия. В Африке этот процент самый высокий в мире, и за два года он уменьшился незначительно. В Юго-Восточной, Восточной, и Южной Азии показатель уже несколько полугодий снижается, что и сказывается на средних по миру результатах.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты при подключении съемных носителей, в некоторых регионах

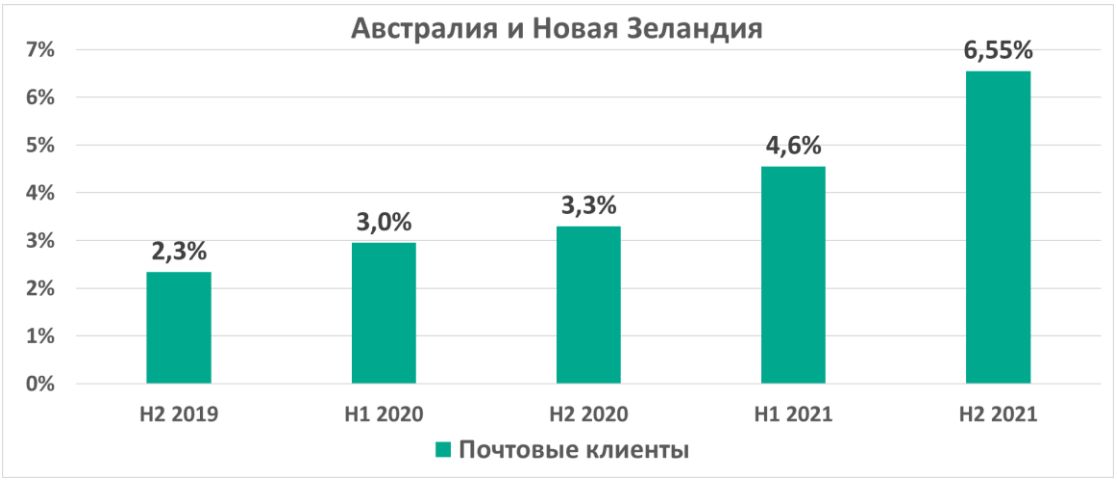


В Центральной Азии процент компьютеров АСУ, на которых блокировались угрозы при подключении съемных носителей, также уменьшался от полугодия к полугодию — за исключением второго полугодия 2021, когда он вырос. А вот на Ближнем Востоке ситуация противоположная: в этом регионе показатель рос вплоть до второго полугодия 2021, а в последнем полугодии упал.

Несмотря на обнадеживающую динамику в мировой статистике, в некоторых странах процент компьютеров АСУ, где угрозы блокируются при подключении съемных носителей, все еще очень высок. Во втором полугодии 2021 лидирует Алжир с 19,7%. В то же время в Японии и в Дании на съемных носителях при подключении их к компьютерам АСУ вредоносного ПО практически не зафиксировано.

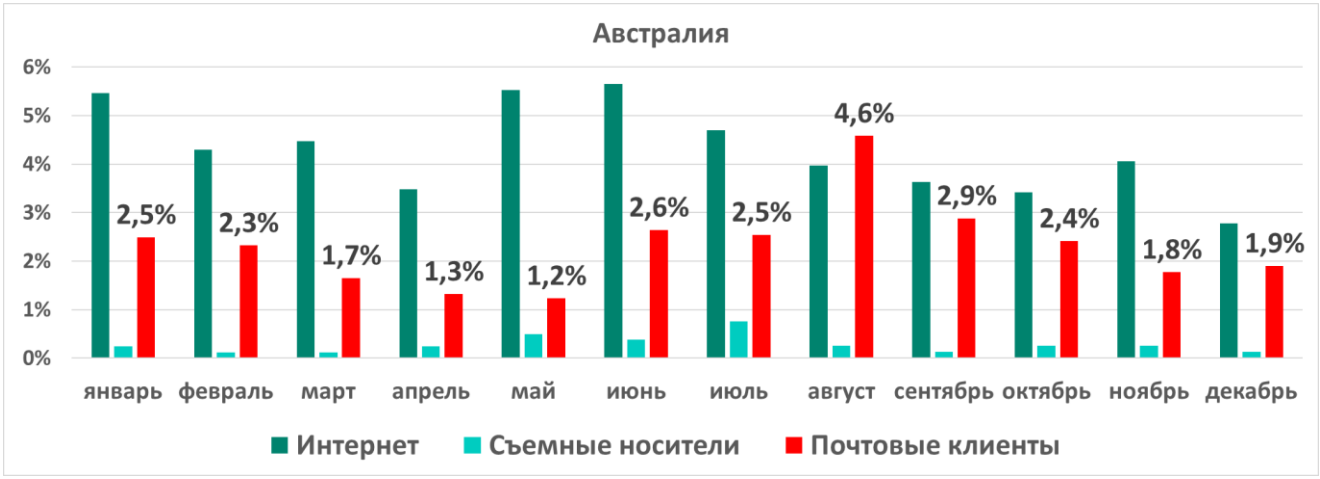
Регионы Австралия и Новая Зеландия и Южная Европа по итогам второго полугодия 2021 лидируют в рейтинге по проценту компьютеров АСУ, на которых были заблокированы **вредоносные объекты в почтовых вложениях**. В Южной Европе этот показатель традиционно высокий, а вот в Австралии и Новой Зеландии за два года он вырос почти в три раза.

Южная Европа. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в почтовых вложениях



Австралия и Новая Зеландия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в почтовых вложениях

В этих регионах почта вносит заметный вклад в поток угроз. Например, в Австралии в августе 2021 года процент компьютеров АСУ, на которых были заблокированы вредоносные вложения в электронных письмах, превысил показатели остальных источников угроз, в том числе интернета.

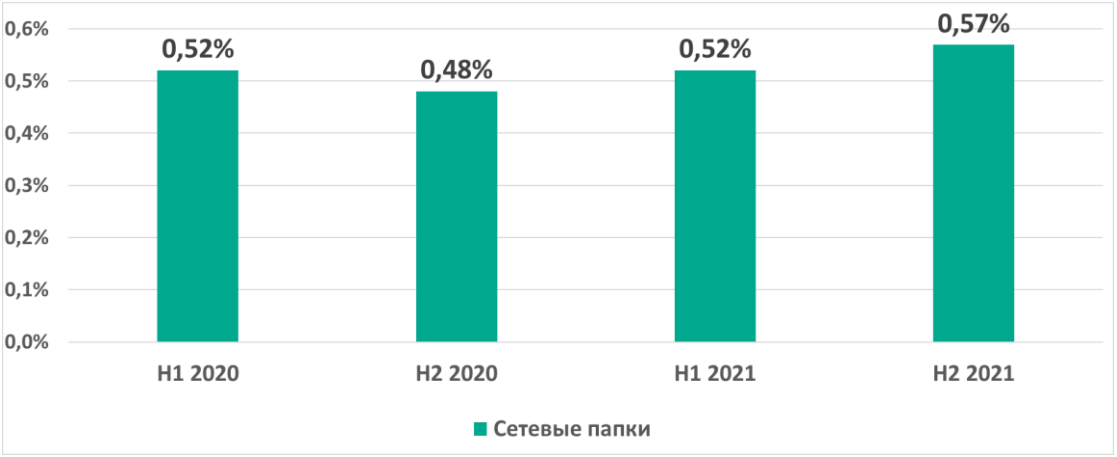


Австралия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из разных источников, январь — декабрь 2021

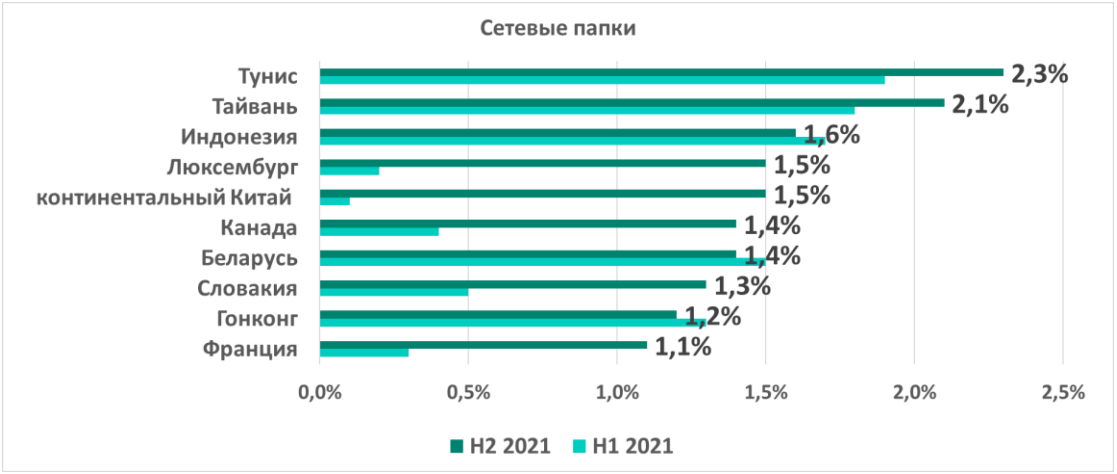
Мы рекомендуем специалистам по безопасности в этих регионах обратить особое внимание на защиту сотрудников предприятий от фишинговых рассылок.

Сетевые папки — один из минорных источников вредоносных объектов. На компьютеры АСУ, где вредоносные объекты были заблокированы в сетевых папках, приходится всего 0,57%, однако этот показатель потихоньку растет и в некоторых странах и территориях уже превышает 1%.

Процент компьютеров АСУ, на которых вредоносные объекты были заблокированы в сетевых папках



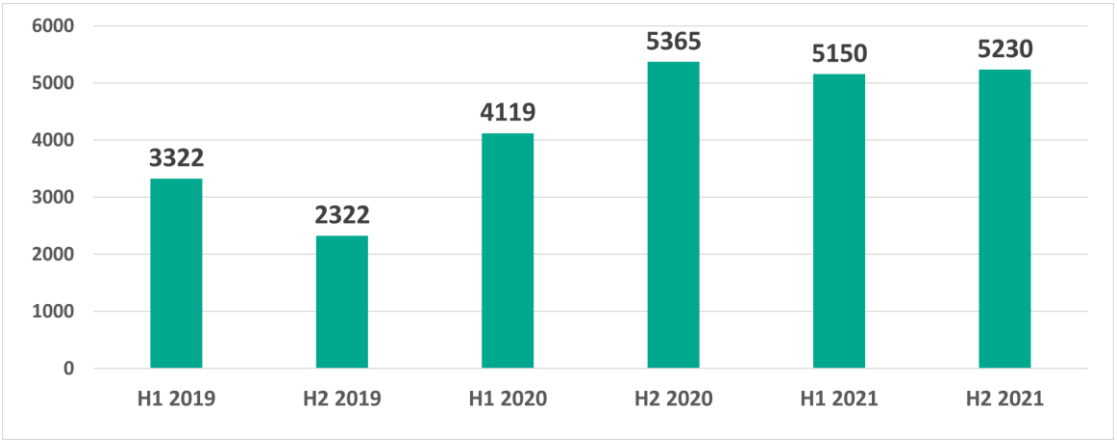
Страны и территории с максимальным процентом компьютеров АСУ, на которых вредоносные объекты были заблокированы в сетевых папках во втором полугодии 2021



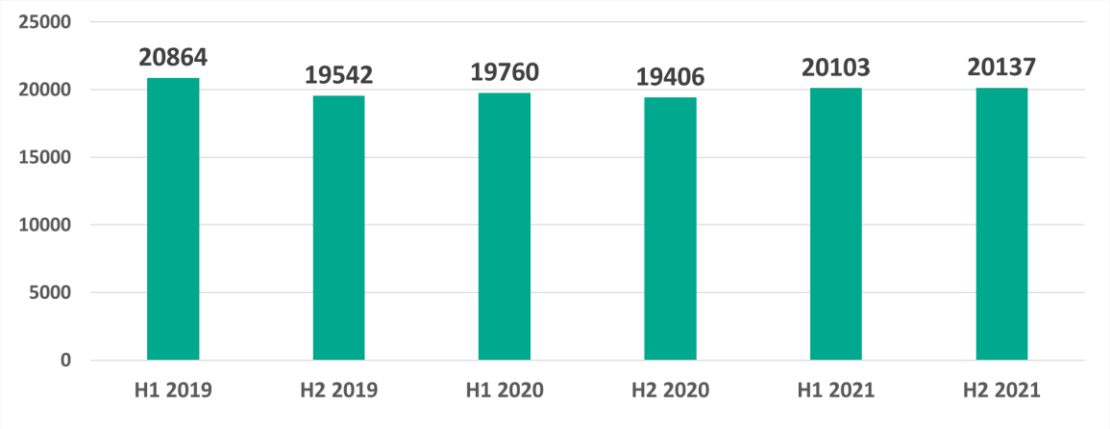
Разнообразие обнаруженного вредоносного ПО

Во втором полугодии 2021 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 20 тысяч модификаций вредоносного ПО из 5230 различных семейств.

Количество семейств вредоносного ПО, заблокированного на компьютерах АСУ



Количество модификаций 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.

Результаты нашего анализа дали следующие оценки процента компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий:

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.

Ресурсы из интернета из списка запрещённых

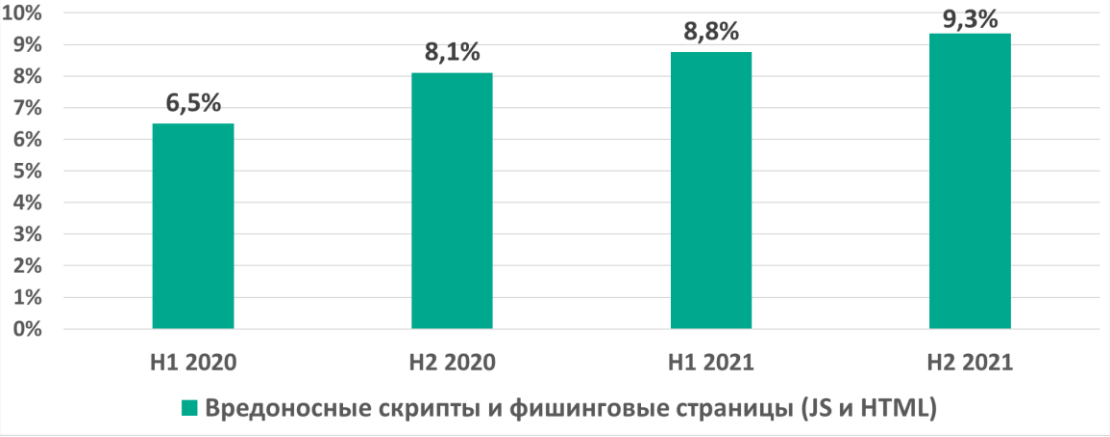
По проценту атакованных компьютеров АСУ по-прежнему лидируют ресурсы из интернета из списка запрещённых, значительная часть которых используется для распространения вредоносных скриптов и фишинговых страниц (HTML). Наиболее заметное изменение показателя — уменьшение на 3,9 п.п. — отмечено именно в этой категории.

Проактивное блокирование вредоносных скриптов, встраиваемых в расширения для веб-браузеров, а также удаление со множества легитимных сайтов загрузчиков вредоносных скриптов (в том числе недобросовестных/небезопасных рекламных модулей) в значительной степени способствовало снижению показателя заблокированных ресурсов в интернете из списка запрещенных. Многие такие ресурсы и связанные с ними вредоносные скрипты были в значительной мере распространены на территории России и в странах СНГ.

Вредоносные скрипты и фишинговые страницы (JS и HTML)

На втором месте — вредоносные скрипты и фишинговые страницы (JS и HTML), распространяемые как через интернет, так и посредством фишинговых рассылок (в том числе внутри офисных документов и/или архивов). Процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, неуклонно растет год к году и с начала 2020 вырос в 1,4 раза.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

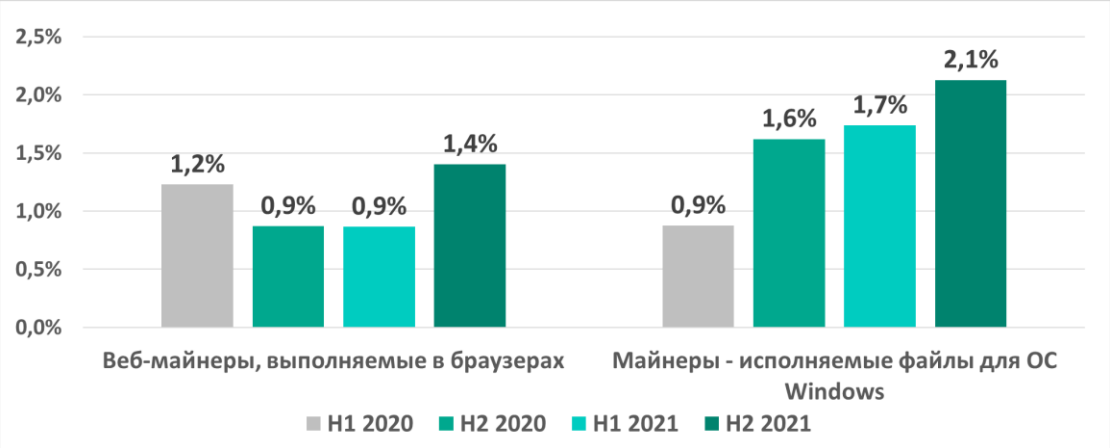


Вредоносные скрипты используются злоумышленниками для выполнения большого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО и/или программ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

Майнеры

Характерно, что с ростом активности использования злоумышленниками скриптов растет и активность использования майнеров. Процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, — с начала 2020 года увеличился более чем вдвое. Во втором полугодии 2021 вырос и показатель веб-майнеров.

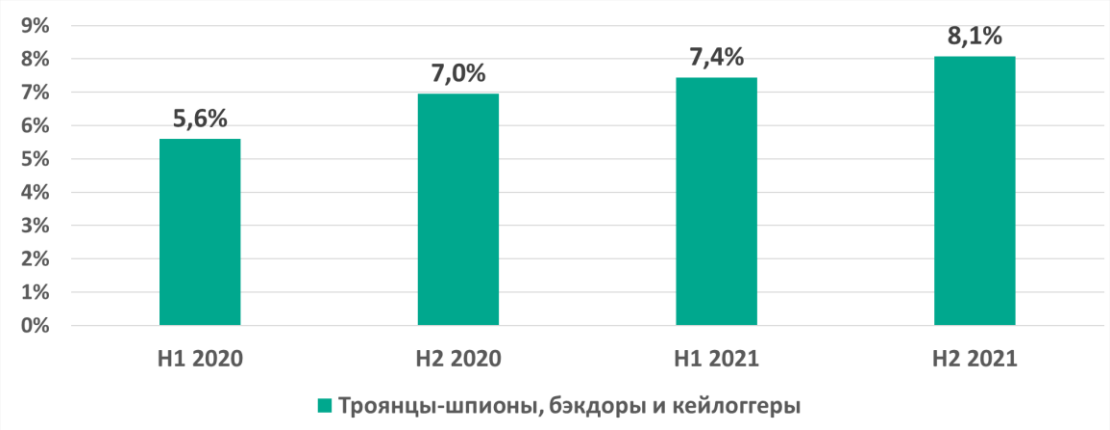
Процент компьютеров АСУ, на которых были заблокированы майнеры



Шпионское ПО

Шпионское ПО (троянцы-шпионы, бэкдоры и кейлоггеры) занимают третье место. Такие угрозы нацелены на предоставление скрытого удаленного доступа к системе и/или краже данных, в том числе данных аутентификации. Процент компьютеров АСУ, на которых блокируется шпионское ПО, с первого полугодия 2020 вырос в 1,4 раза.

Процент компьютеров АСУ, на которых было заблокировано шпионское ПО



В 2021 году эксперты Kaspersky ICS CERT выявили множество атак на компьютеры АСУ с применением шпионского ПО. Около 20% всех образцов шпионского ПО, заблокированных на компьютерах АСУ по всему миру, использовались в атаках с ограниченным охватом и коротким временем жизни каждого вредоносного образца. Программы-шпионы в этой кампании

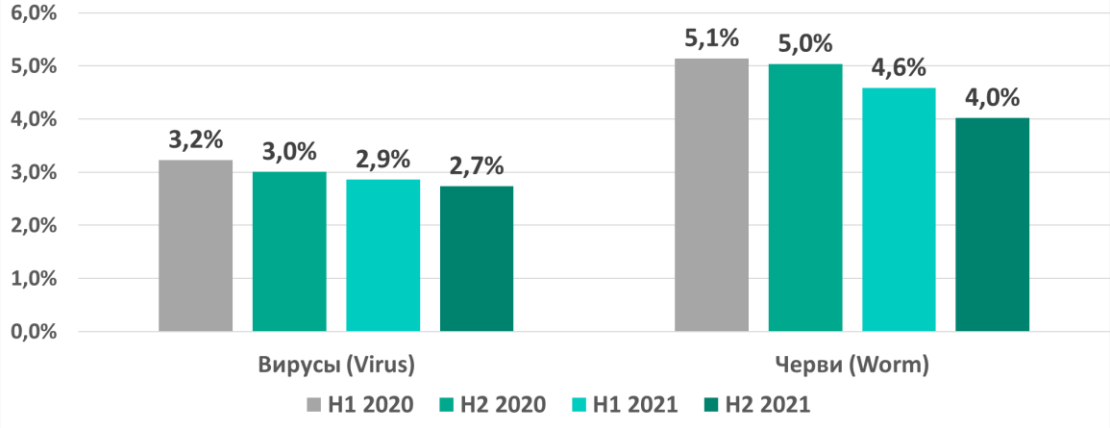
были вполне «обычными» — из числа тех, что активно используются злоумышленниками и в более массовых атаках.

Вредоносное ПО во многих случаях распространялось от одного промышленного предприятия к другому через фишинговые письма, замаскированные под корреспонденцию организаций-жертв. Недавно мы опубликовали результаты исследования TTP этих атак и значительной части вредоносной экосистемы — от используемых MaaS-платформ и инфраструктур тестирования и отладки до форумов и SM-платформ, коммуникации злоумышленников и онлайн-площадок по продаже украденных ими данных аутентификации для скрытого удаленного доступа на компьютеры различных промышленных организаций.

Вирусы и черви

Вирусы и черви по-прежнему на четвертом и пятом местах. Хорошая новость — процент компьютеров АСУ, на которых блокируется такое вредоносное ПО, постепенно уменьшается.

Процент компьютеров АСУ, на которых были заблокированы вирусы и черви



В сетях АСУ продолжают доживать свой век вирусы и черви, распространяющиеся через сетевые папки, съемные носители, зараженные файлы (в том числе бэкапы) и сетевые атаки на безнадежно устаревшее ПО (например, Radmin2). Старые вирусы, такие как Virut и Sality, а также старые черви, такие как Kido/Conficker, не являются по-настоящему активными (их командные серверы данным давно 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.

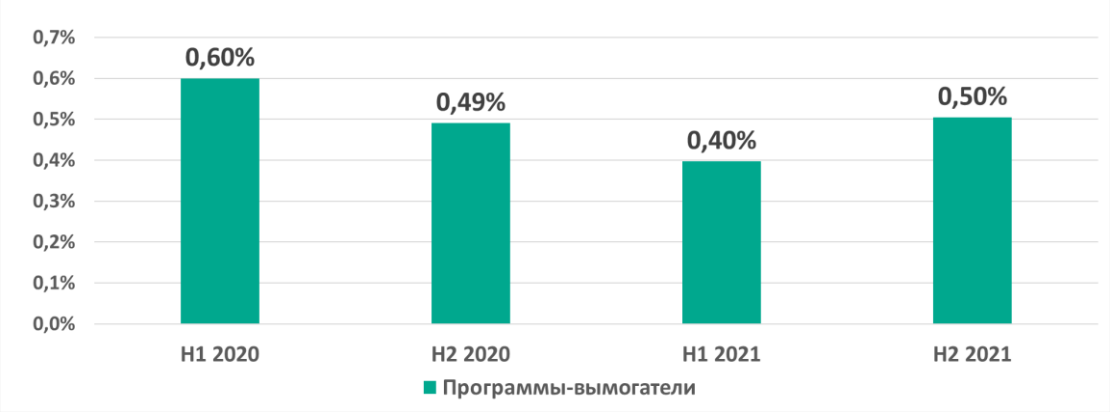
Вместе с тем, в сетях АСУ встречаются и новые версии червей, используемые злоумышленниками для распространения в сети шпионского ПО, программ-вымогателей и майнеров. Чаще всего для распространения по сети эти черви используют эксплойты для исправленных производителями,

но еще актуальных в технологических сетях уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

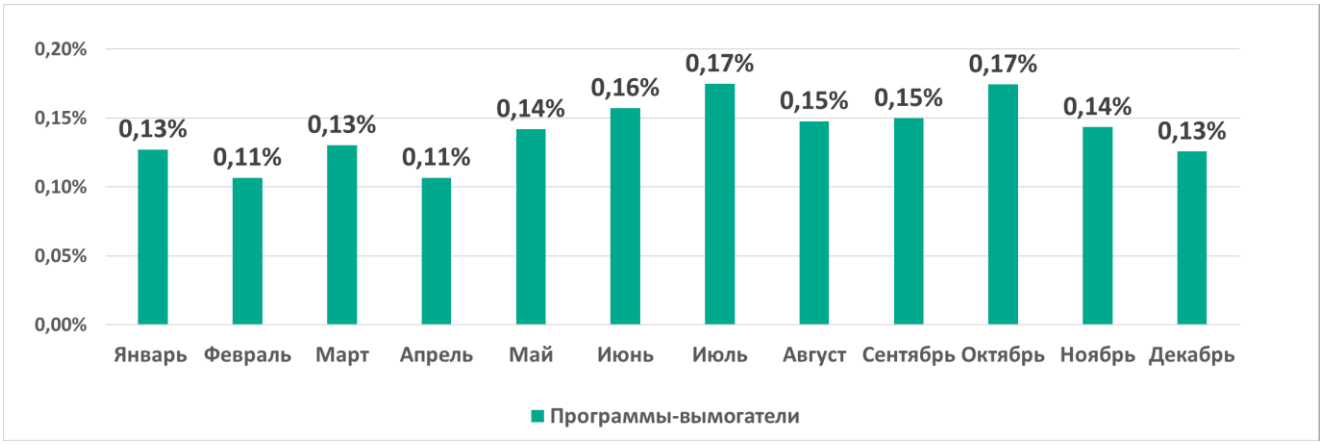
Программы-вымогатели

Во втором полугодии 2021 года вредоносные программы-вымогатели были заблокированы на 0,50% компьютеров АСУ.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели



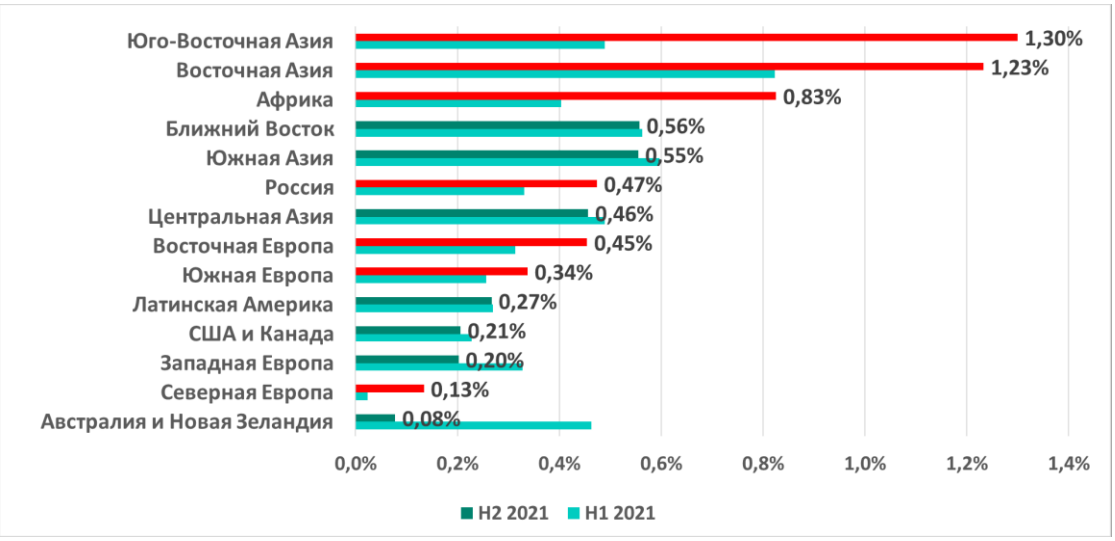
Наибольшие значения процента компьютеров АСУ, на которых были заблокированы программы-вымогатели, в течение 2021 года были отмечены в июле и октябре (0,17%), наименьшие — в феврале и в апреле (0,11%).



Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь — декабрь 2021

Во втором полугодии 2021 процент атакованных вымогателями компьютеров АСУ вырос в половине регионов мира. Наиболее значительно — в Юго-Восточной и Восточной Азии и в Африке, которые и возглавили рейтинг регионов по этому показателю.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2021



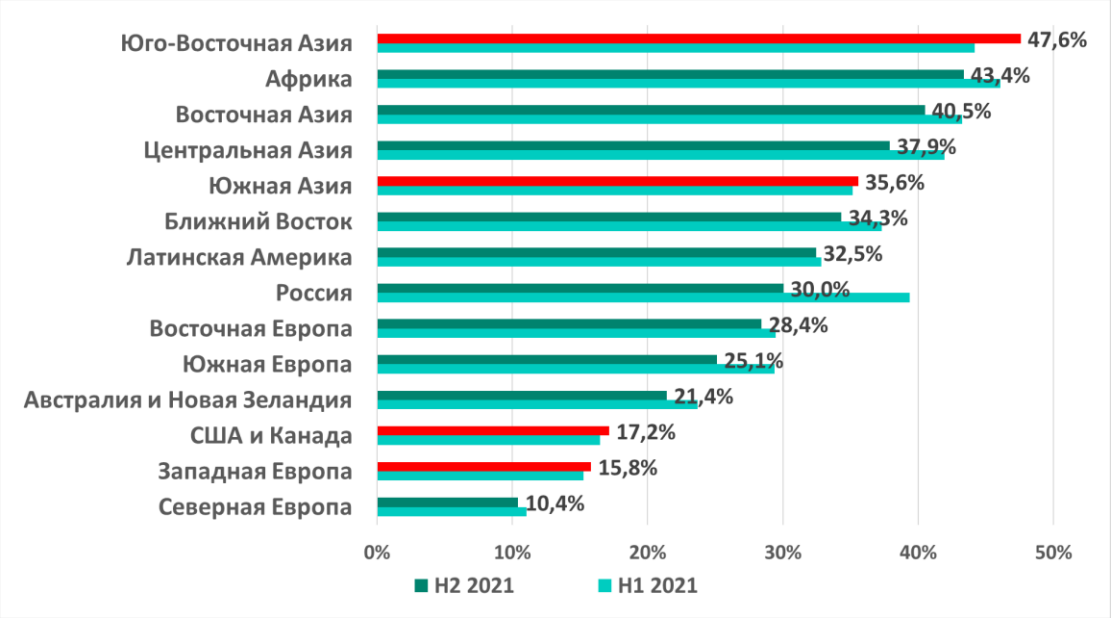
В России процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, за полугодие вырос с 0,33% до 0,47%.

География

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты: география

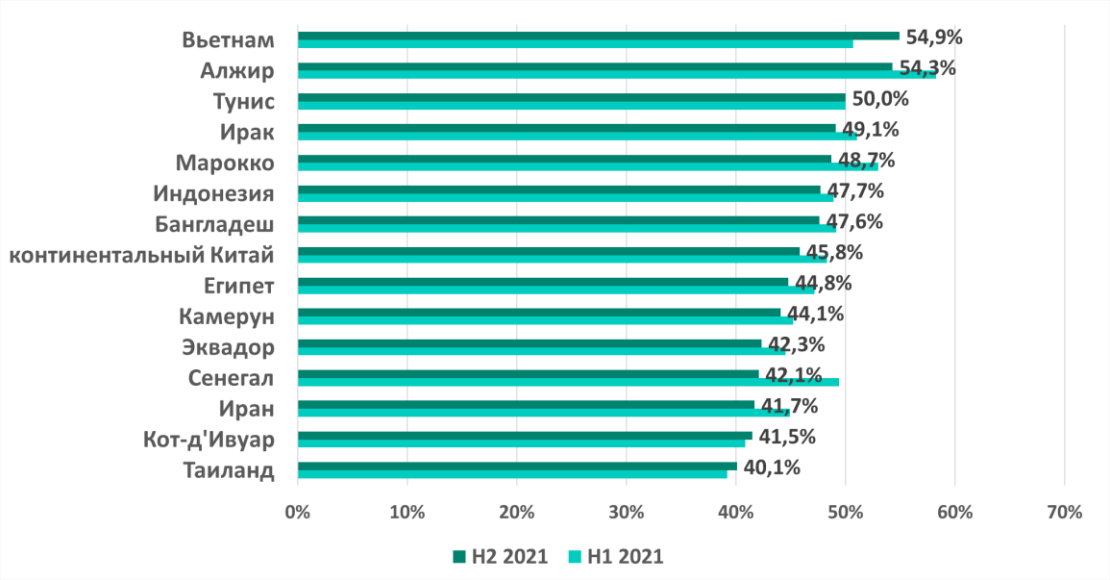
В рейтинге регионов мира по доле компьютеров АСУ, на которых была предотвращена вредоносная активность, лидируют Юго-Восточная Азия, Африка, Восточная и Центральная Азия.

Рейтинг регионов мира по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2021

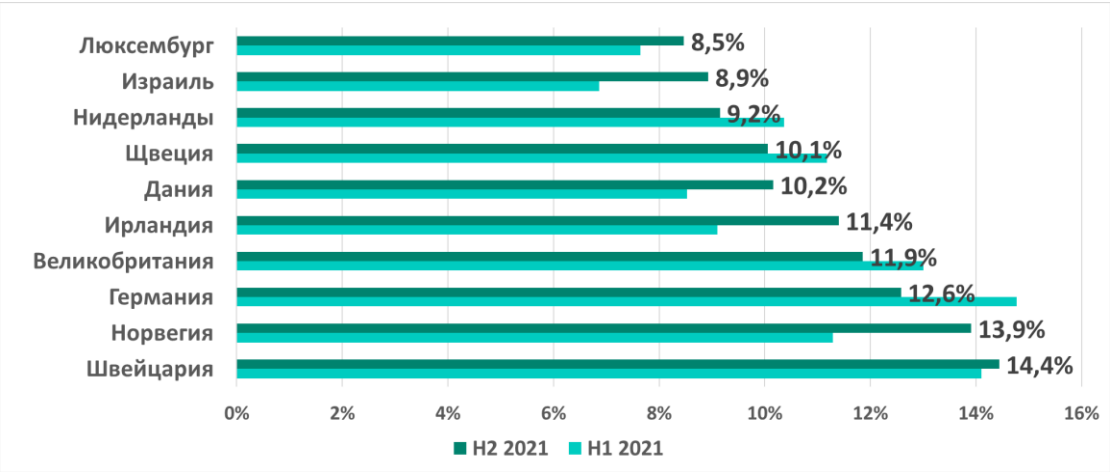


Наибольшее увеличение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, зафиксировано в Юго-Восточной Азии (+ 3,4 п.п.).

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2021



10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2021

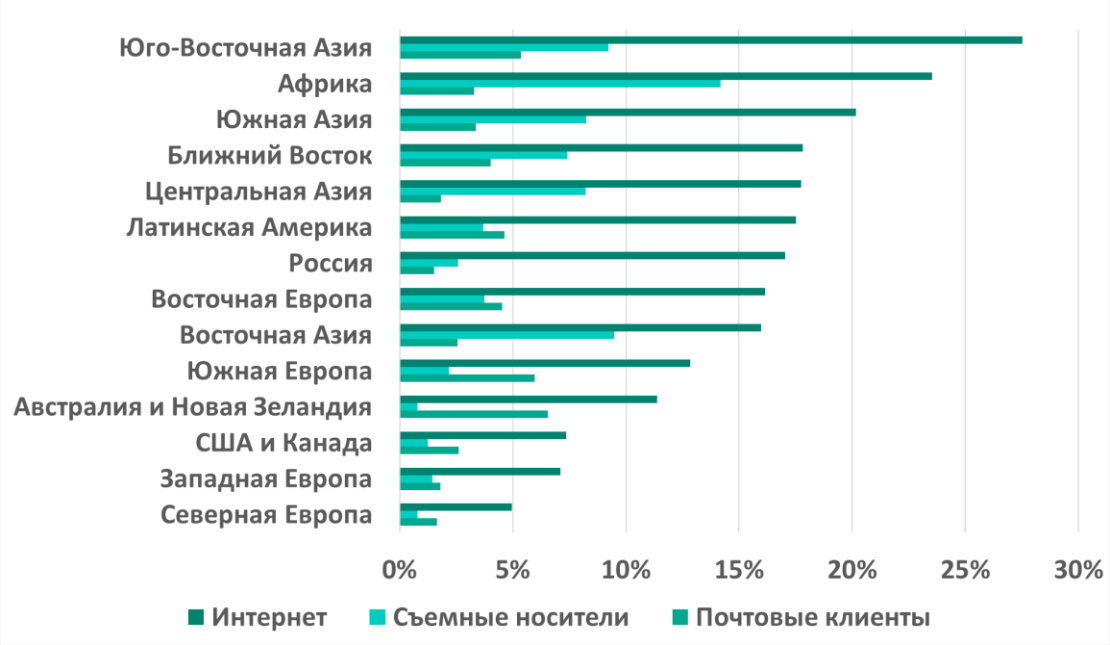


Наименьший показатель во втором полугодии 2021 был отмечен в Люксембурге.

Самое значительное увеличение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, было отмечено на Филиппинах (+ 5,1 п.п.), в Перу (+ 5,0 п.п.) и в Аргентине (+ 4,9 п.п.).

Основные источники угроз: данные по регионам и странам

Основные источники угроз, заблокированных на компьютерах АСУ в регионах мира во втором полугодии 2021



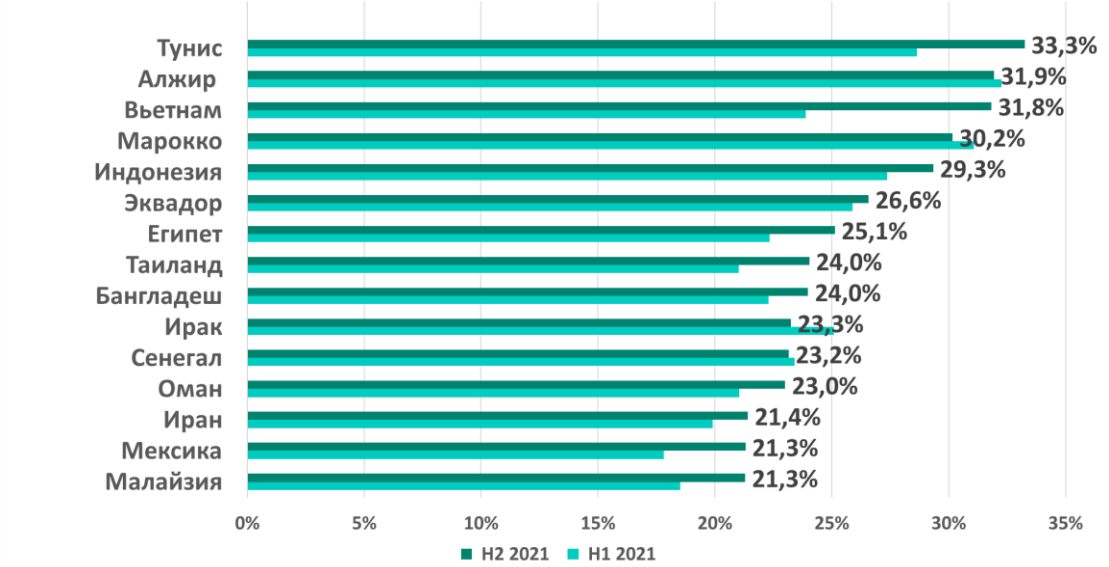
Интернет

Процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, во втором полугодии 2021 увеличился в четырех регионах мира, наиболее значительно — в Юго-Восточной Азии (+5,6 п.п.) и в Южной Азии (+3,3 п.п.).

Рейтинг регионов мира по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета во втором полугодии 2021

Среди стран и территорий мира лидируют страны Азии, Африки и Ближнего Востока. В Топ 15 попала и одна латиноамериканская страна — Мексика.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы угрозы из интернета во втором полугодии 2021

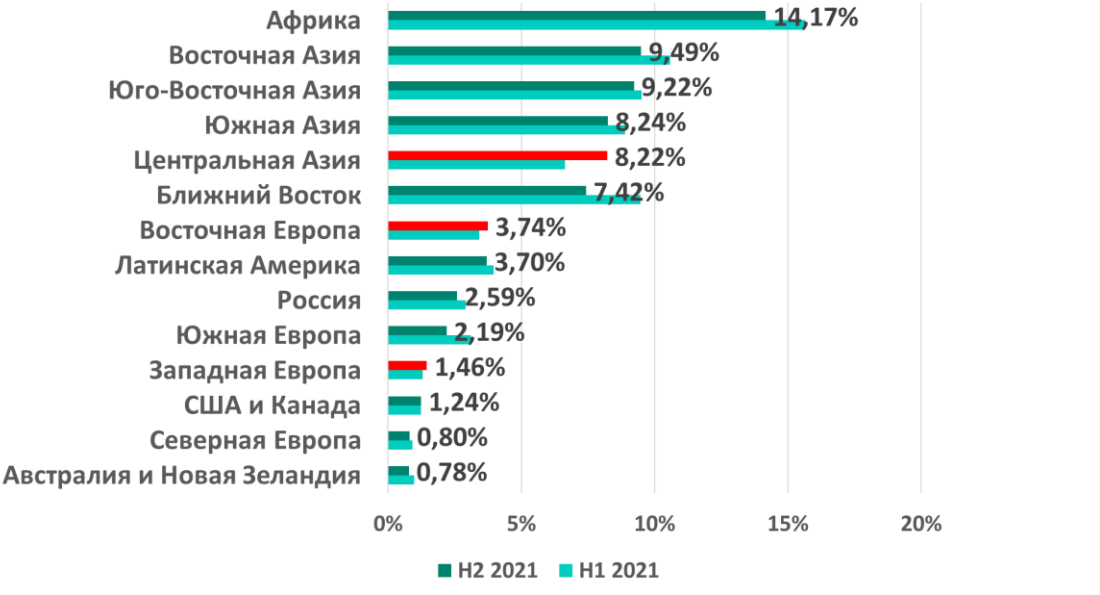


Наибольший прирост процента компьютеров АСУ, на которых были заблокированы вредоносные объекты из интернета, во втором полугодии 2021 отмечен во Вьетнаме (+7,9 п.п.).

Съемные носители

Рейтинг регионов по проценту компьютеров АСУ, на которых при подключении съемных носителей было заблокировано вредоносное ПО, традиционно возглавляют Африка, регионы Азии и Ближний Восток.

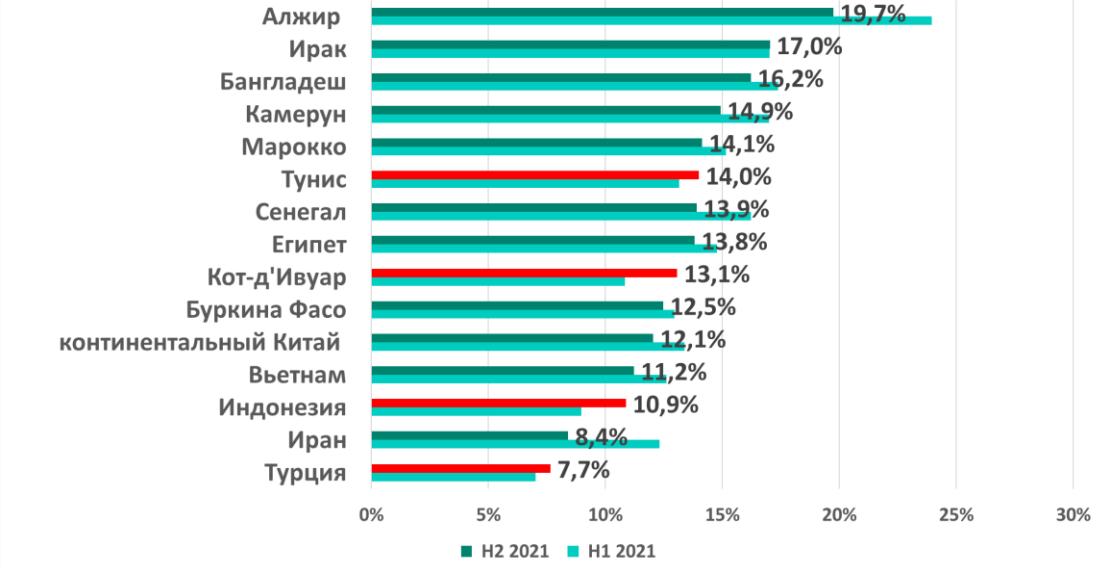
Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей во втором полугодии 2021



Во всех регионах, кроме Центральной Азии, Восточной и Западной Европы, данный показатель уменьшился.

Среди 15 стран и территорий, лидирующих во втором полугодии 2021 года по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, показатель вырос только у четырех.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей во втором полугодии 2021

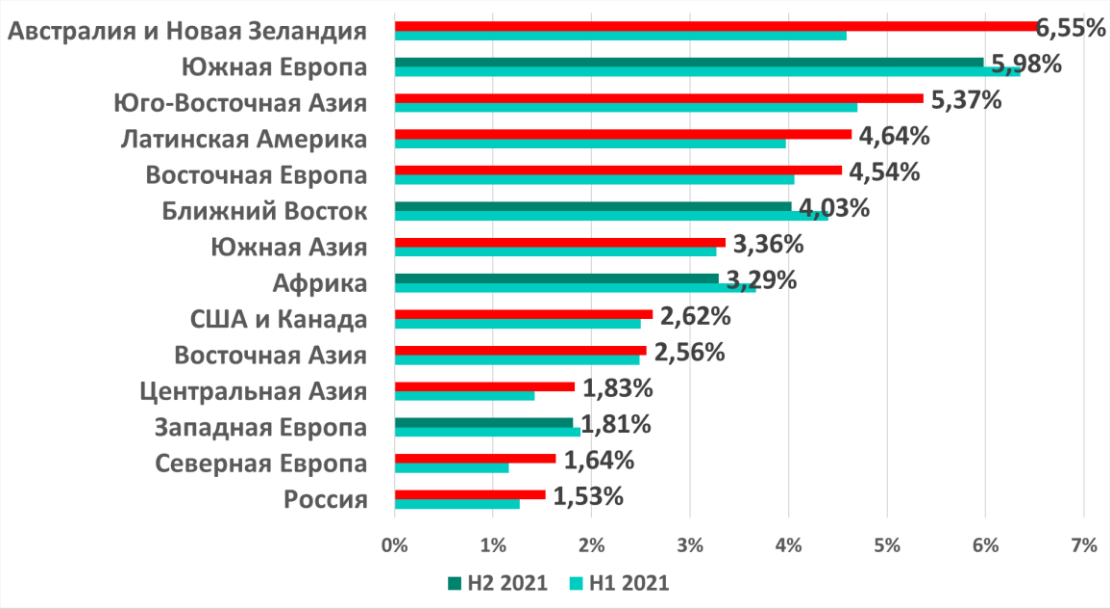


Почтовые клиенты

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, во втором полугодии 2021 неожиданно возглавила Австралия и Новая Зеландия, где был отмечен рост показателя с 4,55% до 6,55%.

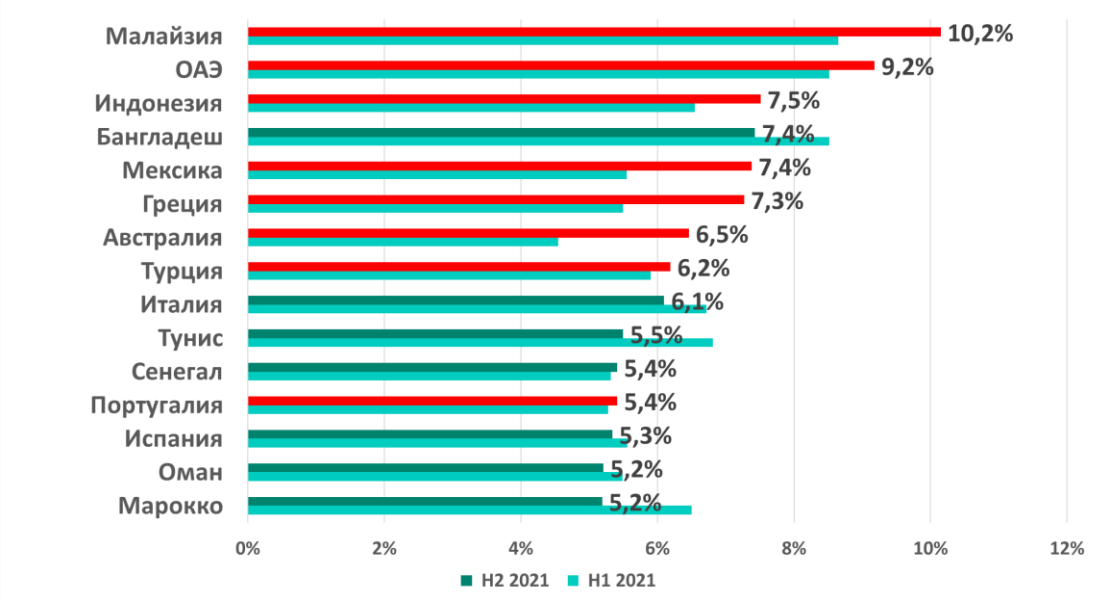
Напомним, что в первом полугодии 2021 единственным регионом, где увеличился данный показатель, был регион Австралия и Новая Зеландия (+1,3 п.п.). Во втором полугодии 2021 ситуация изменилась: показатель увеличился в десяти из четырнадцати регионов.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения во втором полугодии 2021



Среди 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, Австралия с 6,5% оказалась на седьмом месте. Лидирует Малайзия с рекордными 10,2%.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения во втором полугодии 2021



Как и в первом полугодии, в этот рейтинг попали европейские страны — Греция, Италия, Португалия и Испания.

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.

Атакованными мы считаем те компьютеры, на которых в течение отчетного периода 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 отчетного периода, по отношению ко всем компьютерам из нашей выборки, с которых в течение отчетного периода мы получали обезличенную информацию.

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