kaspersky

Ландшафт угроз для систем промышленной автоматизации

Первое полугодие 2021

Kaspersky ICS CERT

09.09.2021 Version 1.0

Цифры полугодия

Процент атакованных компьютеров АСУ

1. В первом полугодии 2021 года **процент атакованных компьютеров АСУ** составил **33,8%** — на 0,4 п.п. больше, чем во втором полугодии 2020.

   В разных странах этот показатель варьирует от 58,4% в Алжире до 6,8% в Израиле.

   Среди регионов лидируют Африка (46,1%), Юго-Восточная (44,1%), Восточная (43,1%) и Центральная Азия (42,1%).

2. **Наибольшее увеличение процента атакованных компьютеров АСУ** за полугодие было отмечено:
   - более чем на 10 п.п. — в Беларуси (50,4%) и на Украине (33,1%);
   - на 7,4 п.п — в Чехии (20,2%) и Словакии (24,3%);
   - на 6,5 п.п. — в Гонконге (20,8%);
   - на 6 п.п. — в Австралии (23%) и в Камеруне (45,2%).

   Основной вклад в этот рост внесли угрозы из интернета.

3. **Во всех исследованных индустриях** процент компьютеров АСУ, на которых были заблокированы угрозы, уменьшился. Наиболее заметно — на 7,5 п.п. и 6,3 п.п. — соответственно в Нефтегазовой отрасли (36,5%) и Автоматизации зданий (40,3%).

Основные источники угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, съемные носители и электронная почта.

1. **Угрозы из интернета** заблокированы на 18,2% компьютеров АСУ (+1,5 п.п.)

   Наибольший рост этого показателя в первом полугодии отмечен в Беларуси (+12,2 п.п.), Украине (+ 8 п.п.) и в России (+6,7 п.п.).

   Россия (27,6%) возглавила соответствующий рейтинг регионов, Беларусь (32,8%) — рейтинг стран.

2. **При подключении съемных носителей** угрозы заблокированы на 5,2% компьютеров АСУ (-0,2 п.п.). Этот показатель понемногу снижается со второй половины 2019 года.

   Среди регионов по этому показателю с заметным отрывом лидирует Африка (15,6%), среди стран — Алжир (24%).

В регионах Азии процент компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, за полугодие уменьшился.

3. **Вредоносные почтовые вложения** заблокированы на 3,4% компьютеров АСУ (-0,6 п.п.).

   Среди регионов по этому показателю лидирует Южная Европа (6,4%), среди стран — Бангладеш (8,8%).

   Единственный регион, где этот показатель за полугодие вырос — Австралия и Новая Зеландия (+1,3 п.п.).

Разнообразие вредоносного ПО

Защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 20,1 тысяч модификаций вредоносного ПО из 5150 различных семейств.

1. Основную угрозу представляют **ресурсы из интернета из списка запрещённых** (заблокированы на 14% компьютеров АСУ).

   На различных медиаресурсах и сайтах с пиратским контентом злоумышленники используют вредоносные скрипты, которые перенаправляют пользователей на сайты, распространяющие шпионское ПО и/или программы для скрытого майнинга криптовалюты. Процент компьютеров, на которых были заблокированы такие угрозы, растет с 2020 года.

2. **Вредоносные скрипты и перенаправления (JS и HTML)** — были заблокированы на 8,8% компьютеров АСУ (+0,7 п.п.).

   Процент компьютеров, на которых блокировались вредоносные скрипты-загрузчики, используемые для загрузки шпионского ПО, заметно вырос в Австралии и Новой Зеландии (+3,8 п.п) и в России (+4,4 п.п.).

3. **Шпионское ПО (бэкдоры, троянцы-шпионы и кейлоггеры)** — были заблокированы на 7,4% компьютеров АСУ (+ 0,4 п.п.).

   Самым высоким это показатель был в Восточной Азии (14,3%), Африке (13,4%) и Юго-Восточной Азии (11,2%).

4. **Вредоносные программы-вымогатели** были заблокированы на 0,40% компьютеров АСУ (-0,1 п.п.).

   Выше всего этот показатель — в Восточной Азии (0,82%).

   В странах Ближнего Востока вырос процент компьютеров, на которых блокировались черви (+0,4 п.п) и шифровальщики (+0.3 п.п.).

Россия

В России процент компьютеров АСУ, где были заблокированы:

- **Все угрозы** — увеличился на 4,8 п.п. до **39,4%.** В рейтинге регионов Россия оказалась на пятом месте после Африки, Юго-Восточной, Восточной и Центральной Азии.
- **Угрозы из интернета** — вырос на 6,7 п.п. С показателем **27,6%** Россия заняла первое место среди регионов в соответствующем рейтинге.
- **Угрозы при подключении съемных носителей** — увеличился на 0,3 п.п. до **2,9%.**
- **Угрозы в почтовых вложениях** — уменьшился на 0,4 п.п. С показателем **1,2%** Россия среди регионов оказалась в самом конце соответствующего рейтинга.
- **Программы-шпионы** (Spyware) — составил **5,6%.**
- **Вредоносные программы-вымогатели** — остался без изменений (**0,33%**).
- **Среди исследованных индустрий** наибольший процент атакованных компьютеров АСУ отмечен в машиностроении (**53,7%**); наименьший — в нефтегазовой отрасли (**38,8%**).

Общая статистика по миру

В разделе 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 телеметрия содержит только те типы и категории информации, 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].

[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.

Методика подготовки статистики

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:

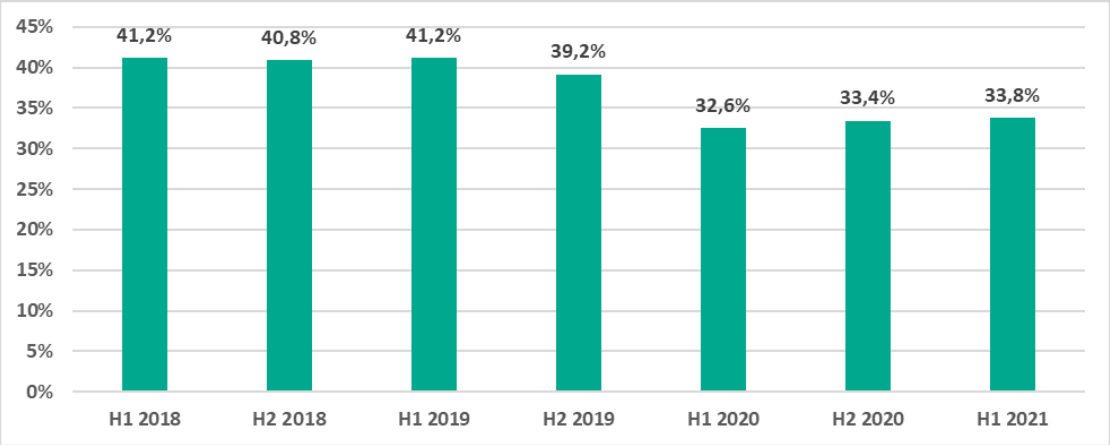
- серверы управления и сбора данных (SCADA);
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human Machine Interface (HMI);
- компьютеры, используемые для администрирования технологических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

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.

Процент компьютеров, на которых были заблокированы вредоносные объекты

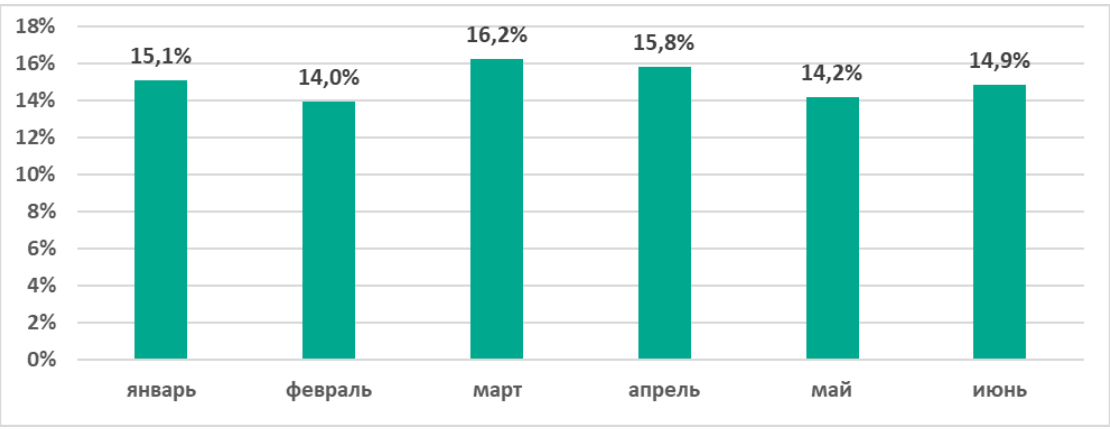
В первом полугодии 2021 года процент атакованных компьютеров АСУ составил 33,8% — на 0,4 п.п. больше, чем в H2 2020.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



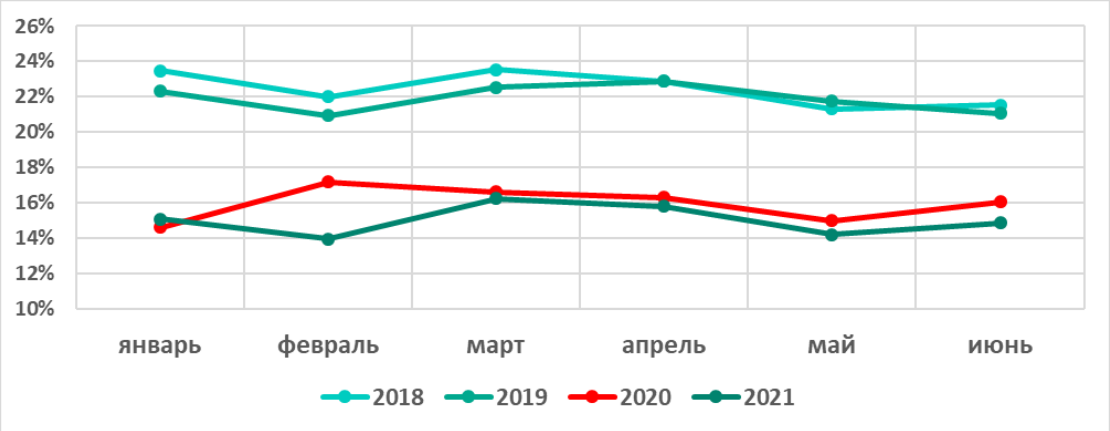
Наименьший процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался в феврале, наибольший — в марте.

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



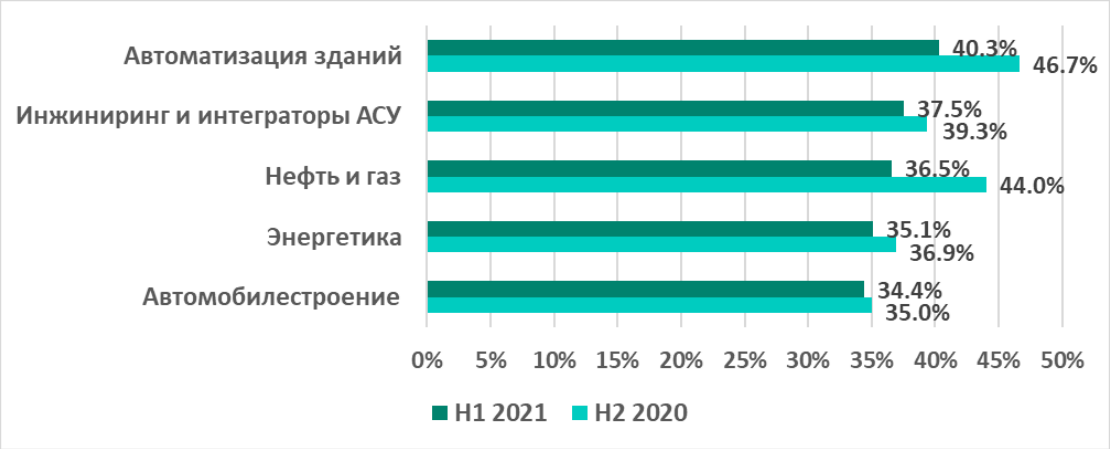
Отметим, что динамика показателя по месяцам за первые шесть месяцев 2021 соответствует 2020 году — за исключением данных за февраль.
В феврале 2020 был отмечен рост процента атакованных компьютеров АСУ, не характерный для предыдущих лет.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам первого полугодия 2018 – 2021 годов



Некоторые индустрии

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



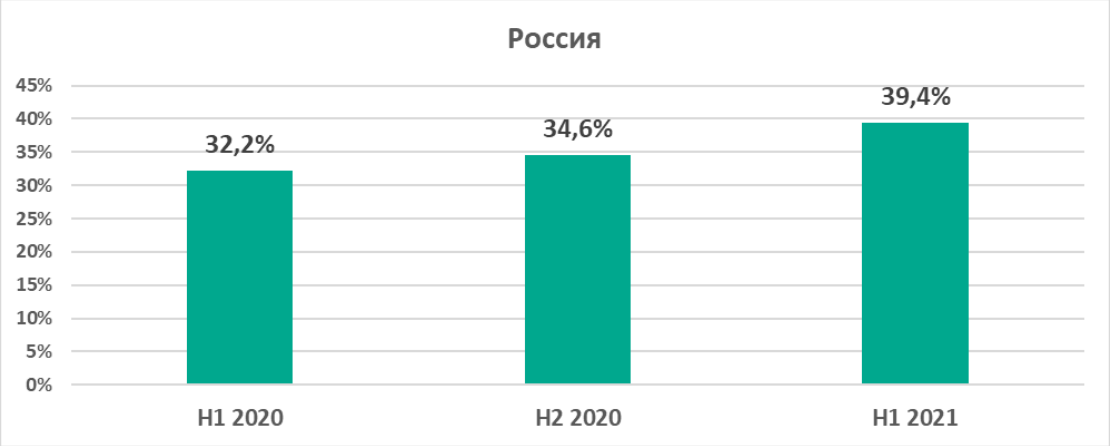
В первом полугодии 2021 года показатели всех исследуемых индустрий уменьшились. Особенно заметно — в Нефтегазовой отрасли (-7,5 п.п.) и Автоматизации зданий (-6,4 п.п.).

Компьютеры, используемые в системах автоматизации зданий, часто имеют такую же поверхность атаки, что и обычные корпоративные системы, более широкую по сравнению с компьютерами АСУ. Они могут быть подключены к корпоративной сети и иметь доступ к различным сервисам, таким как интернет, корпоративная почта, контроллер домена и пр. Нередко системы автоматизации зданий принадлежат подрядной организации и, даже имея доступ к корпоративной сети компании, не всегда находятся в ведении корпоративной службы информационной безопасности.

Россия

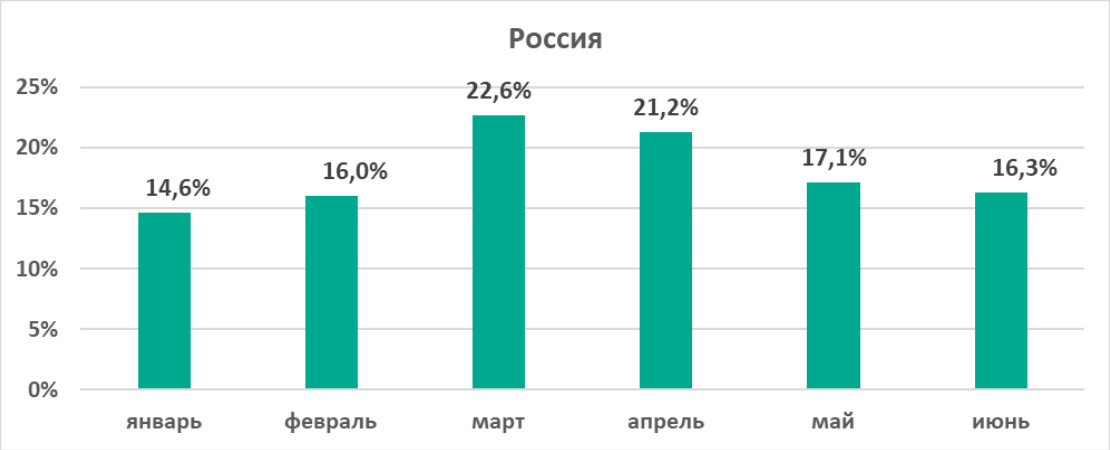
В России в течение первого полугодия 2021 года хотя бы один раз вредоносные объекты были заблокированы на 39,4% компьютеров АСУ. Это на 4,8 п.п. больше, чем во втором полугодии 2020 года, а по сравнению с первым полугодием 2020 показатель вырос на 7,2 п.п

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



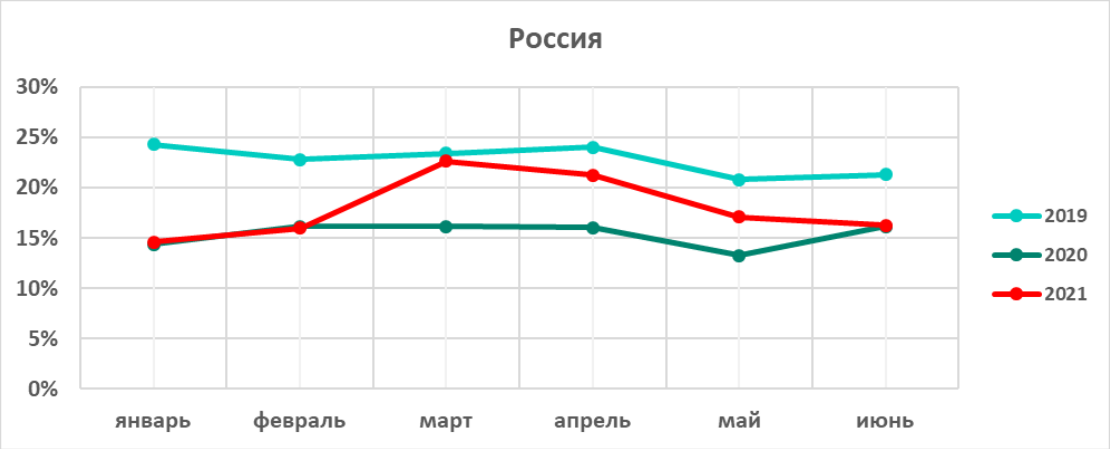
Самый высокий показатель был отмечен в марте (22,6%), самый низкий — в январе (14,6%).

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



В весенние месяцы процент атакованных компьютеров АСУ в России был значительно выше, чем в аналогичный период прошлого года. Динамика показателя от месяца к месяцу отличается и от 2020, и от 2019 годов.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам первого полугодия 2019 – 2021 годов



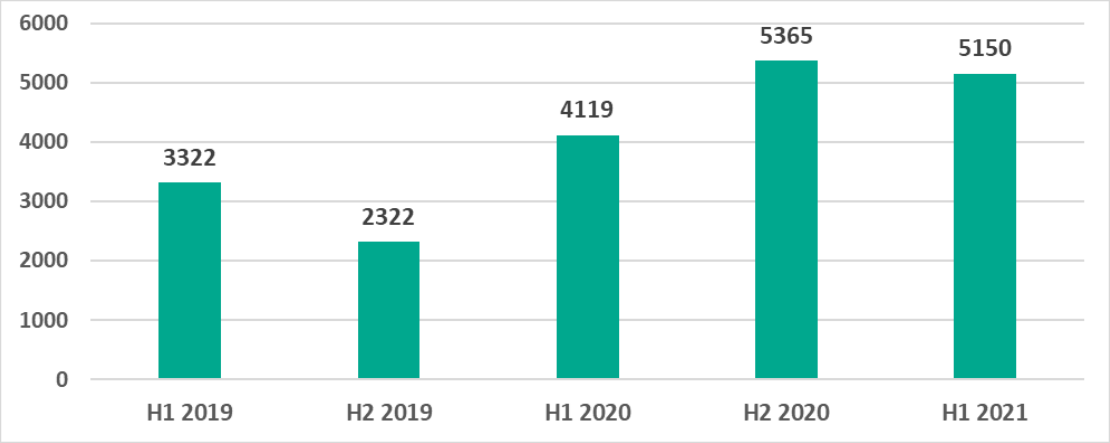
Показатели по всем исследованным индустриям в России выше, чем в среднем по миру.

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

Разнообразие обнаруженного вредоносного ПО

В первом полугодии 2021 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 20 тысяч модификаций вредоносного ПО из 5150 различных семейств.

Количество семейств вредоносного ПО, заблокированного на компьютерах АСУ

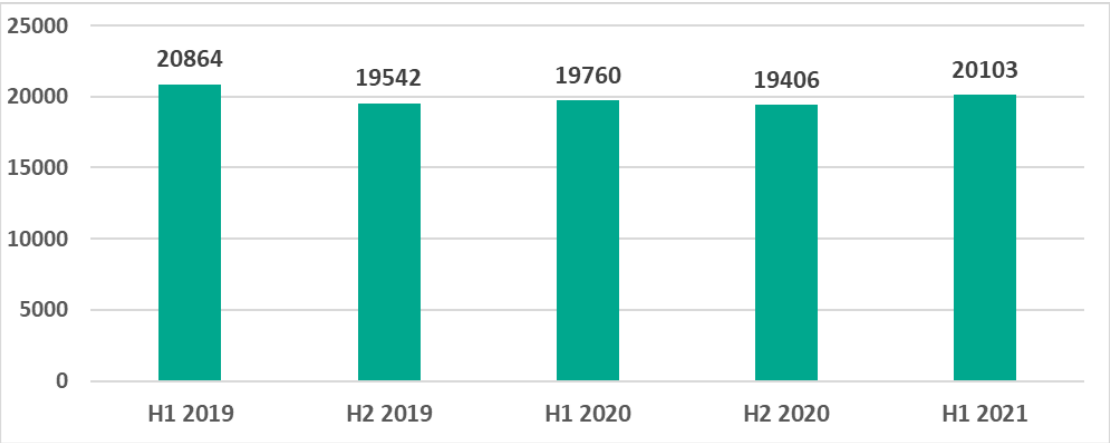


По сравнению с предыдущим полугодием количество семейств вредоносного ПО немного уменьшилось, в то же время число модификаций превысило показатели, зафиксированные в предыдущие полтора года.

Этот факт, а также анализ образцов вредоносного ПО явно указывает на устоявшуюся практику использования злоумышленниками популярных семейств вредоносного (в особенности шпионского) ПО, которые предлагаются по модели MaaS (вредоносное ПО как сервис). Вместо создания «своих» уникальных зловредов атакующие используют готовые и модифицированные под их нужды вредоносные программы, что не требует наличия у них навыков разработки ПО.

Увеличение количества уникальных образцов вредоносного ПО также связано с тем, что злоумышленники массово пользуются сервисами для обфускации вредоносного ПО, чтобы избежать его детектирования.

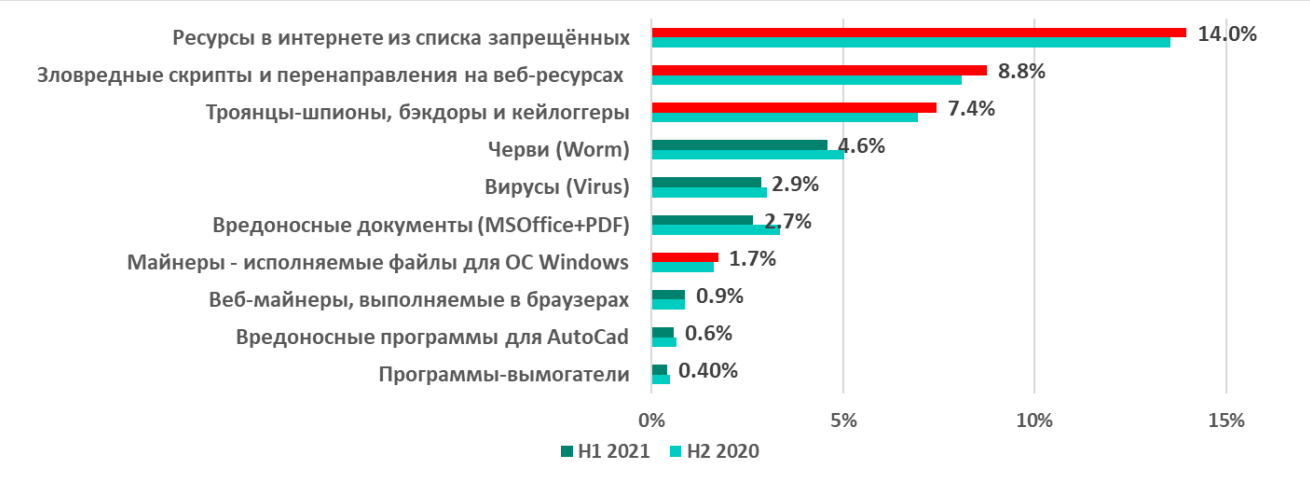
Количество модификаций вредоносного ПО, заблокированного на компьютерах АСУ



Категории вредоносных объектов

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям. Для того чтобы дать лучшее представление о типах заблокированных угроз, мы выполнили их детальную классификацию.

Результаты нашего детального 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.

Краткое описание каждого типа угроз представлено в отдельном документе.

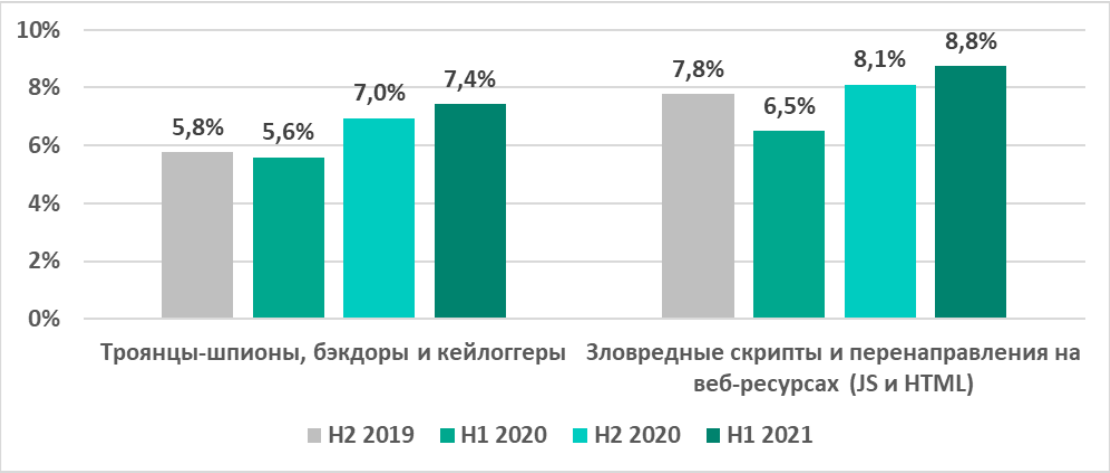
В первом полугодии 2021 года вырос процент компьютеров АСУ, на которых были заблокированы:

- **Угрозы из интернета** — занесенные в список запрещённых веб-ресурсы, задействованные в распространении или управлении вредоносным ПО, — на 0,5 п.п.
- **Зловредные скрипты и перенаправления на веб-ресурсах** (JS и HTML) — на 0,7 п.п.
- **Шпионское ПО** — троянцы-шпионы, бэкдоры и кейлоггеры — на 0,4 п.п.
- **Майнеры** — исполняемые файлы для ОС Windows — на 0,12 п.п.

Вредоносные скрипты используются злоумышленниками на различных медиаресурсах и сайтах с пиратским контентом для перенаправления пользователей на сайты, распространяющие шпионское ПО и/или программы для скрытого майнинга криптовалюты.

Отметим, что показатели шпионского ПО и вредоносных скриптов и перенаправлений растут уже второе полугодие подряд.

Процент компьютеров АСУ, на которых было заблокированы вредоносные объекты

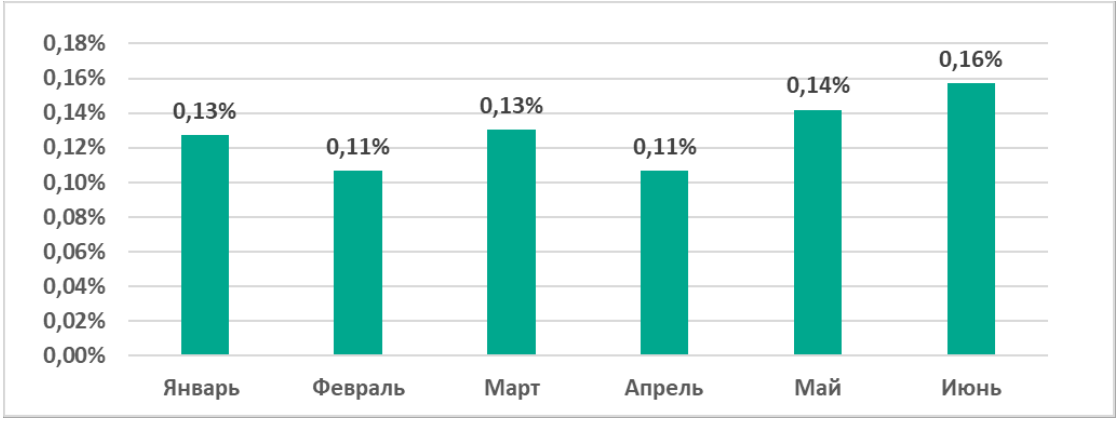


Программы — вымогатели

В первом полугодии 2021 года вредоносные программы-вымогатели были заблокированы на 0,40% компьютеров АСУ. Это на 0,09 п.п. меньше, чем в предыдущем полугодии.

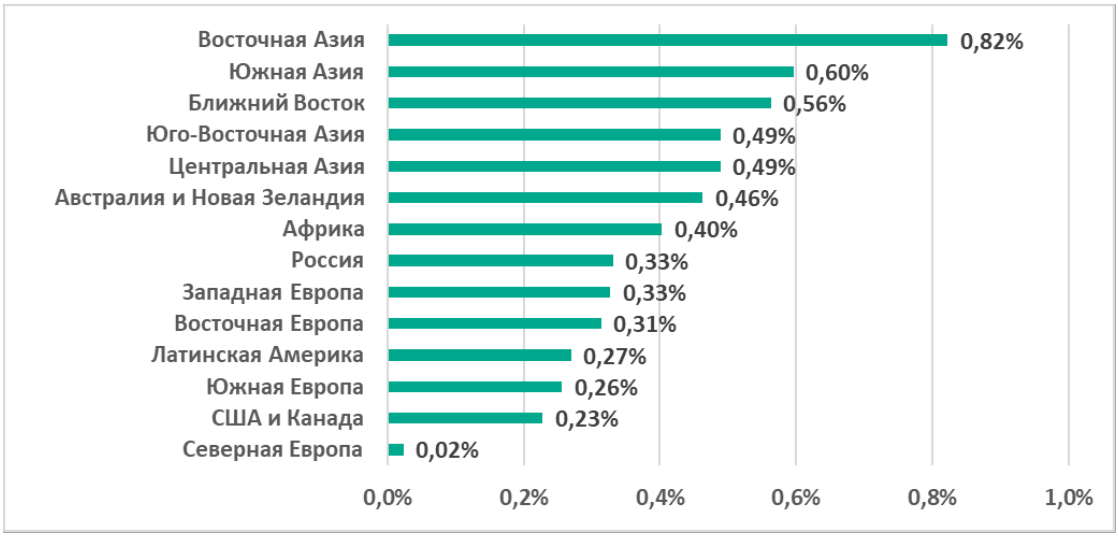
Наибольшее значение процента компьютеров АСУ, на которых были заблокированы программы-вымогатели, было отмечено в июне (0,16%), наименьшие — в феврале и в апреле (0,11%).

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



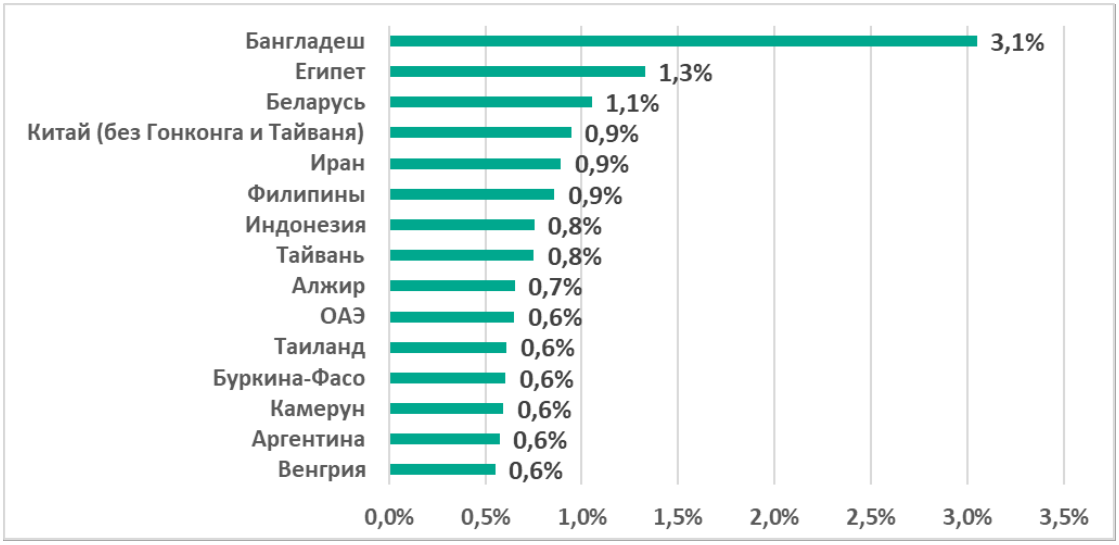
В рейтинге регионов по проценту атакованных вымогателями компьютеров АСУ лидируют регионы Азии и Ближний Восток.

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



В числе 15 стран с наибольшим процентом компьютеров АСУ, на которых были заблокированы программы-вымогатели, две европейские страны — Беларусь и Венгрия.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы программы-вымогатели, первое полугодие 2021



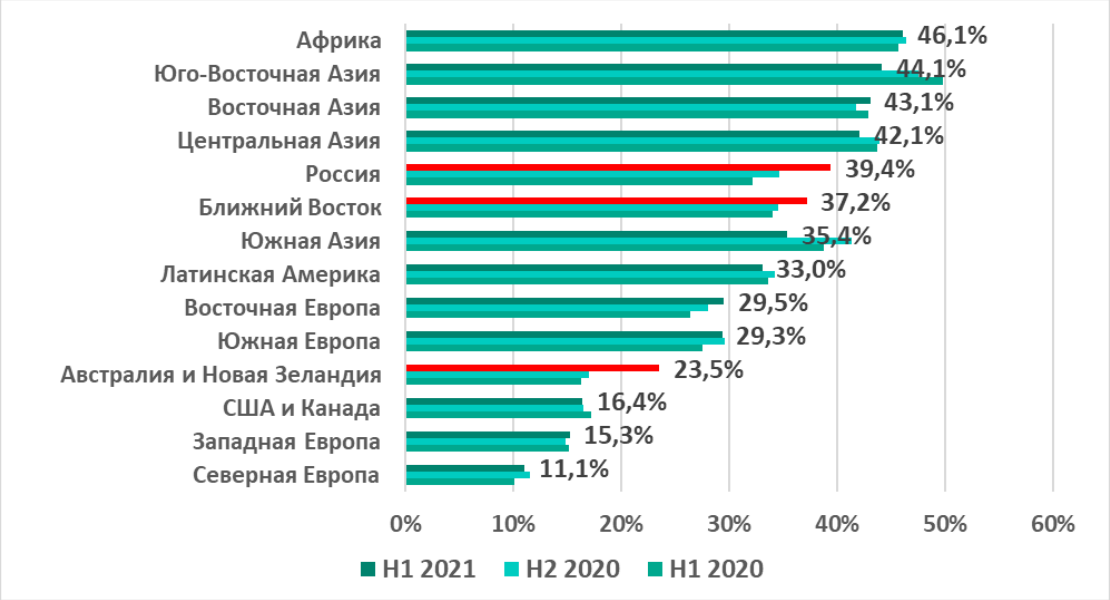
В России процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, за полугодие не изменился и составил 0,33%.

География

Регионы

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

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



Наибольшее увеличение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, зафиксировано:

1. **на 6,5 п.п. — в Австралии и Новой Зеландии;**
2. **на 4,8 п.п. — в России**, которая за год поднялась в этом рейтинге с 8-го на 5-е место;
3. **на 2,6 п.п.** — на Ближнем Востоке.

Столь значительный рост показателя **в Австралии и Новой Зеландии** связан с изменением в этом регионе основного способа распространения шпионского ПО. В предыдущие периоды основным вектором распространения были фишинговые письма, содержащие во вложении шпионское ПО или его загрузчик. В H1 2021 для загрузки шпионского ПО значительно чаще использовались вредоносные скрипты-загрузчики, преимущественно распространяемые в интернете. Процент компьютеров АСУ, на которых были заблокированы такие вредоносные объекты, вырос в Австралии и Новой Зеландии на 3,8 п.п.

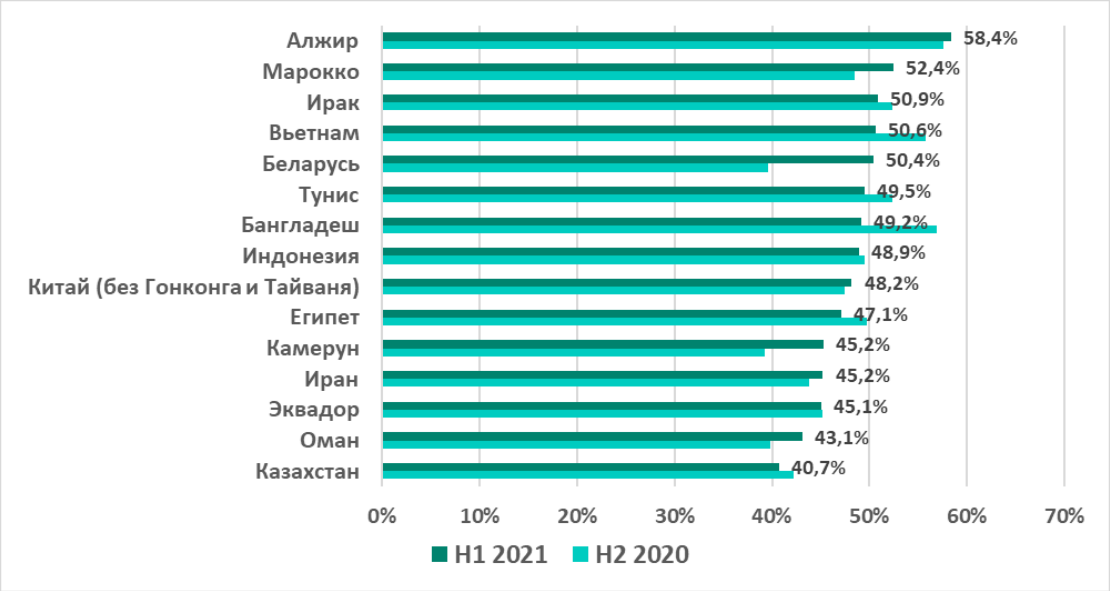
Аналогичный тренд актуален для **России** (+4,4 п.п.).

На **Ближнем Востоке** ситуация иная — там наблюдается рост процента компьютеров АСУ, на которых блокировались черви (+0,4 п.п.) и

шифровальщики (+0,3 п.п.), а вредоносные скрипты-загрузчики стали блокироваться реже
(-0.3 п.п).

Страны

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

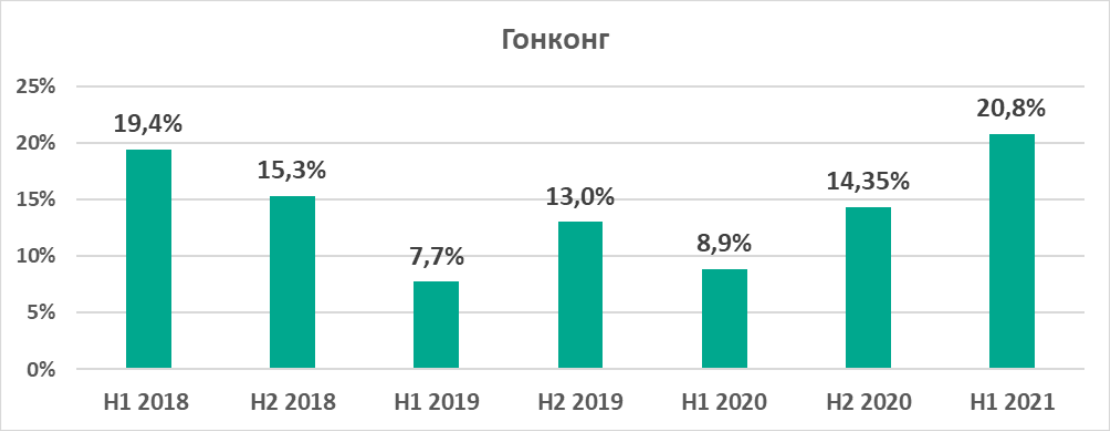


Наибольшее увеличение процента атакованных компьютеров АСУ было отмечено:

1. Более чем на **10 п.п. — в Беларуси и Украине**. В результате Беларусь оказалась на пятом месте в рейтинге стран по этому показателю.
2. На **7,4 пп — в Чехии и Словакии**. Чехия выбыла из рейтинга наиболее благополучных стран.
3. На **6,5 п.п. — в Гонконге и на 6 п.п. в Австралии**. Эти страны также выбыли из десятки наиболее благополучных.
4. На **6 п.п. — в Камеруне**. Эта страна попала в TOP15 по проценту атакованных компьютеров АСУ.

Отметим, что в Гонконге процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, превысил аналогичные показатели за предыдущие три года.

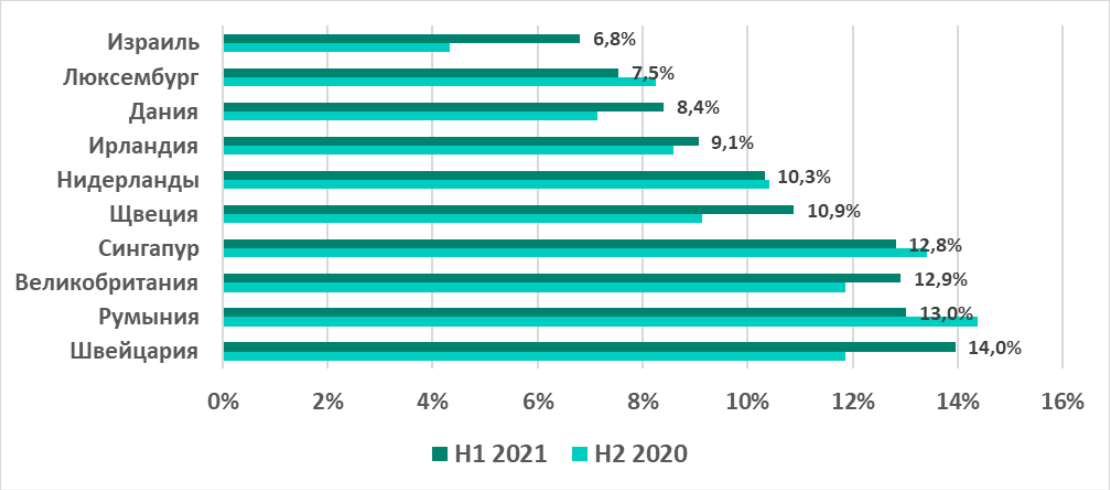
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в Гонконге



Наиболее значительное уменьшение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, было отмечено:

1. Более чем на 10 п.п. — на Филиппинах.
2. На 8,4 п.п — в Бангладеш.
3. Более чем на 7 п.п. — в Саудовской Аравии, Аргентине в Шри Ланке.

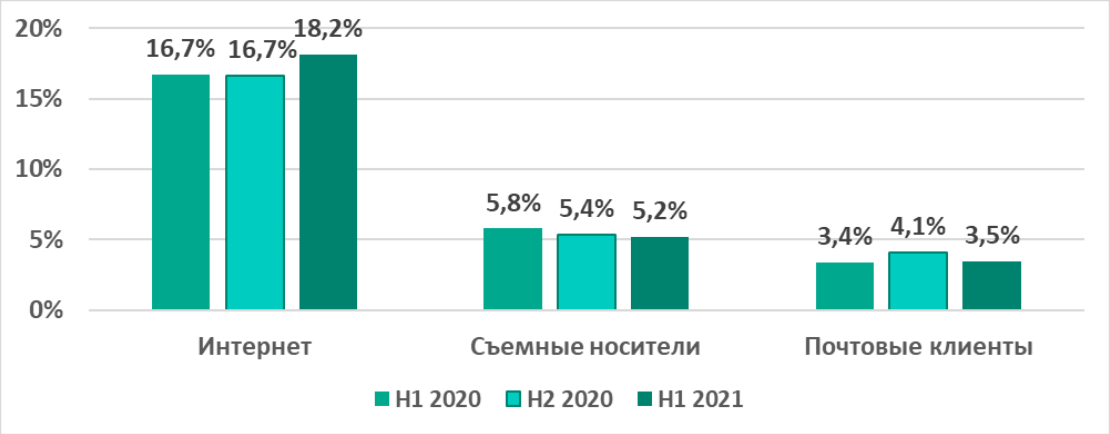
10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты в первом полугодии 2021



Источники угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций являются интернет, съемные носители и электронная почта.

Основные источники угроз, заблокированных на компьютерах АСУ*



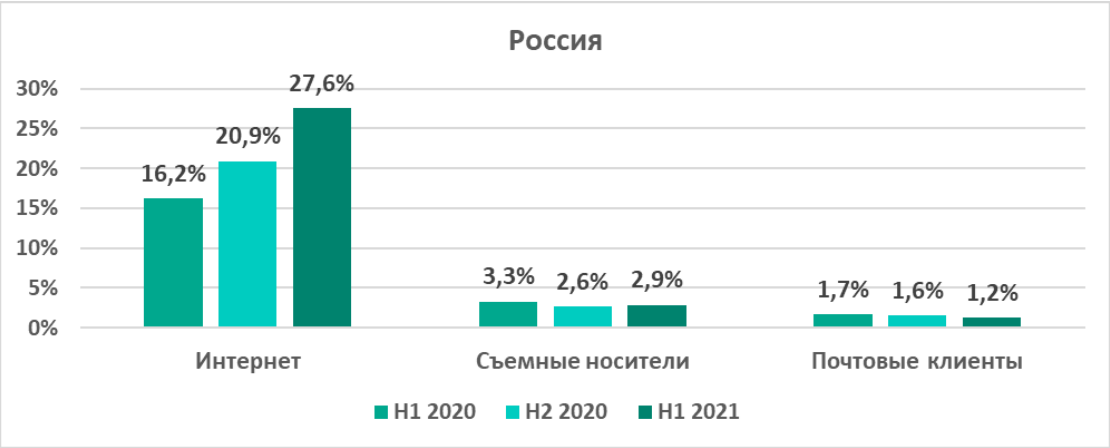
** Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников.*

В первом полугодии 2021 года процент компьютеров АСУ, где были заблокированы:

1. угрозы из интернета — увеличился на 1,5 п.п.;
2. угрозы при подключении съемных носителей — снижается уже год, в первом полугодии 2021 уменьшился на 0,2 п.п.
3. угрозы, распространяющиеся через почтовые клиенты, — уменьшился на 0,6 п.п.

В России процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, значительно увеличился — на 6,7 п.п.

Россия. Основные источники угроз, заблокированных на компьютерах АСУ*

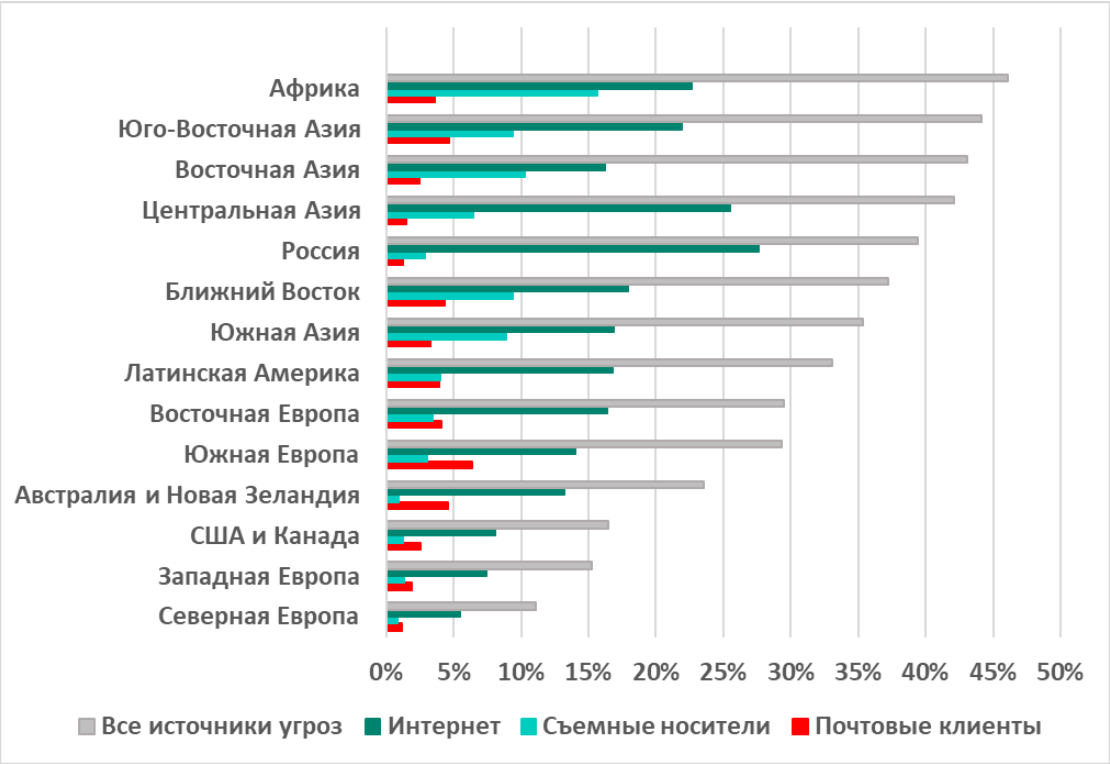


** Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников.*

Основные источники угроз: география

Основные источники угроз, заблокированных на компьютерах АСУ*, в регионах мира, первое полугодие 2021

** процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников, удается установить не во всех случаях*

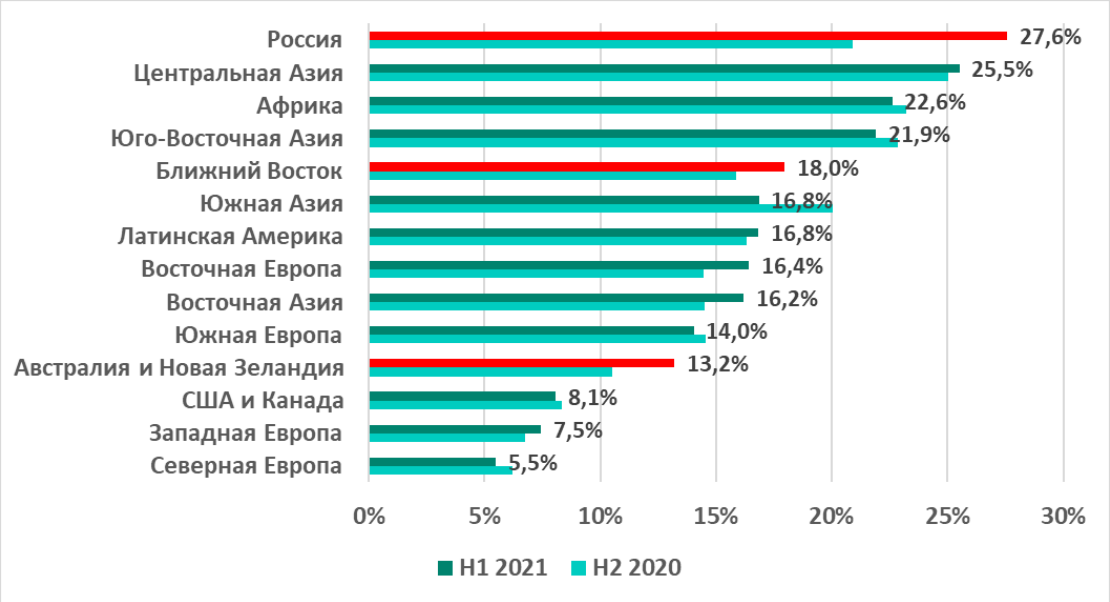


Как и прежде в наиболее благополучных регионах — в Европе, США и Канаде, Австралии и Новой Зеландии — показатели по вредоносным почтовым вложениям превышают показатели по съемным носителям.

Интернет

Основным источником угроз, которые блокируются на компьютерах АСУ, является интернет. По проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, все регионы можно разделить на три группы. Первая — регионы с показателем от 20 до 28%; вторая — от 13% до 18%, третья, наиболее благополучная — до 9%.

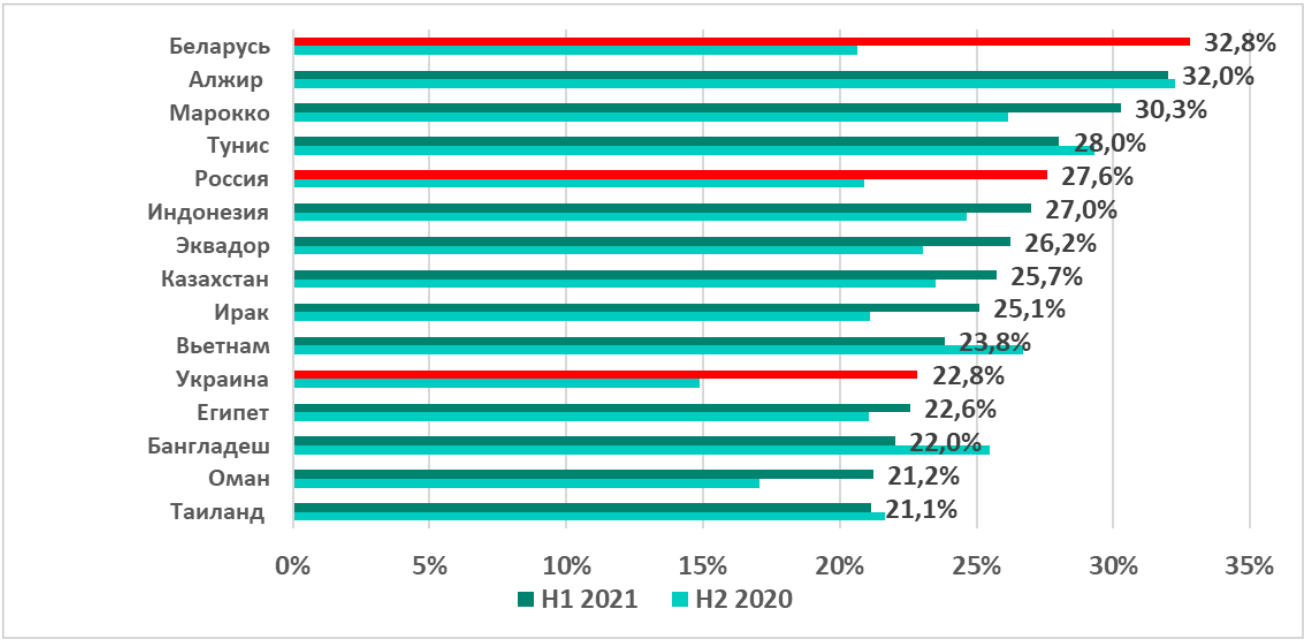
Процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, в регионах мира



В первом полугодии 2021 года процент компьютеров АСУ, где были заблокированы угрозы из интернета, наиболее значительно увеличился:

1. **на 6,7 п.п. — в России**, которая неожиданно заняла первое место среди всех регионов по этому показателю с 27,6%;
2. **на 2,7 п.п. — в Австралии и Новой Зеландии, в результате чего регион попал во вторую группу с показателем 13,2%;**
3. **на 2,1 п.п. — на ближнем Востоке.**

Заметное уменьшение показателя (**минус 3,2 п.п.**) отмечено **в Южной Азии.**



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

Самый значительный рост показателя за прошедшее полугодие был отмечен:

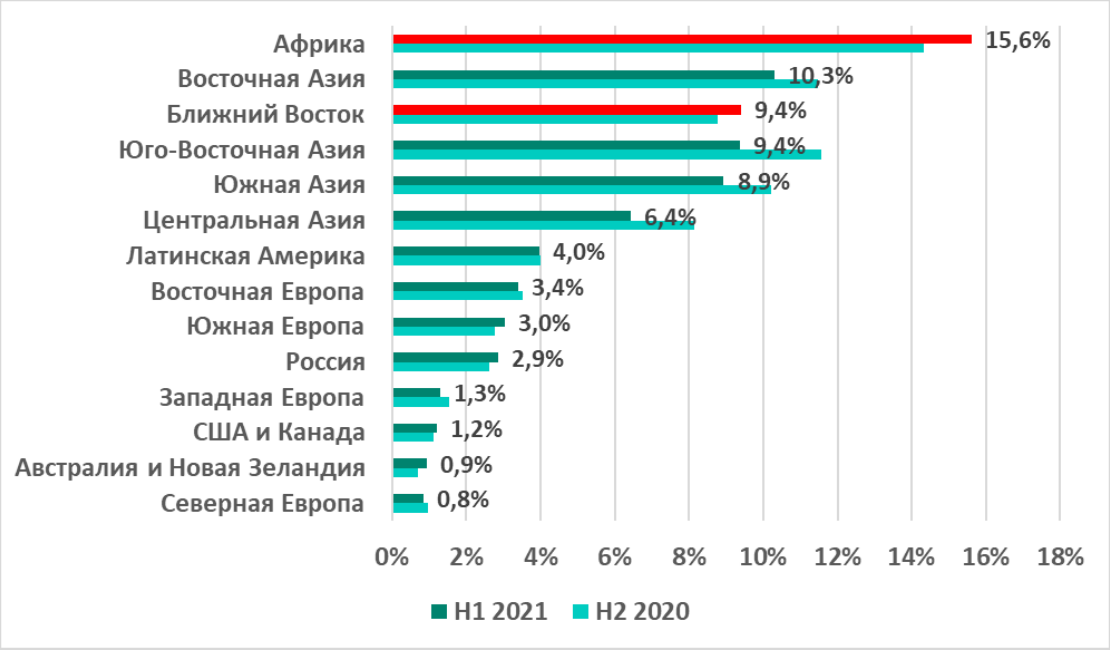
1. **рекордные 12,2 п.п. — в Беларуси**, которая в результате возглавила рейтинг;
2. **8 п.п. — на Украине;**
3. **6,7 п.п. — в России.**

Среди остальных стран в топ-15 нет ни одной европейской.

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.

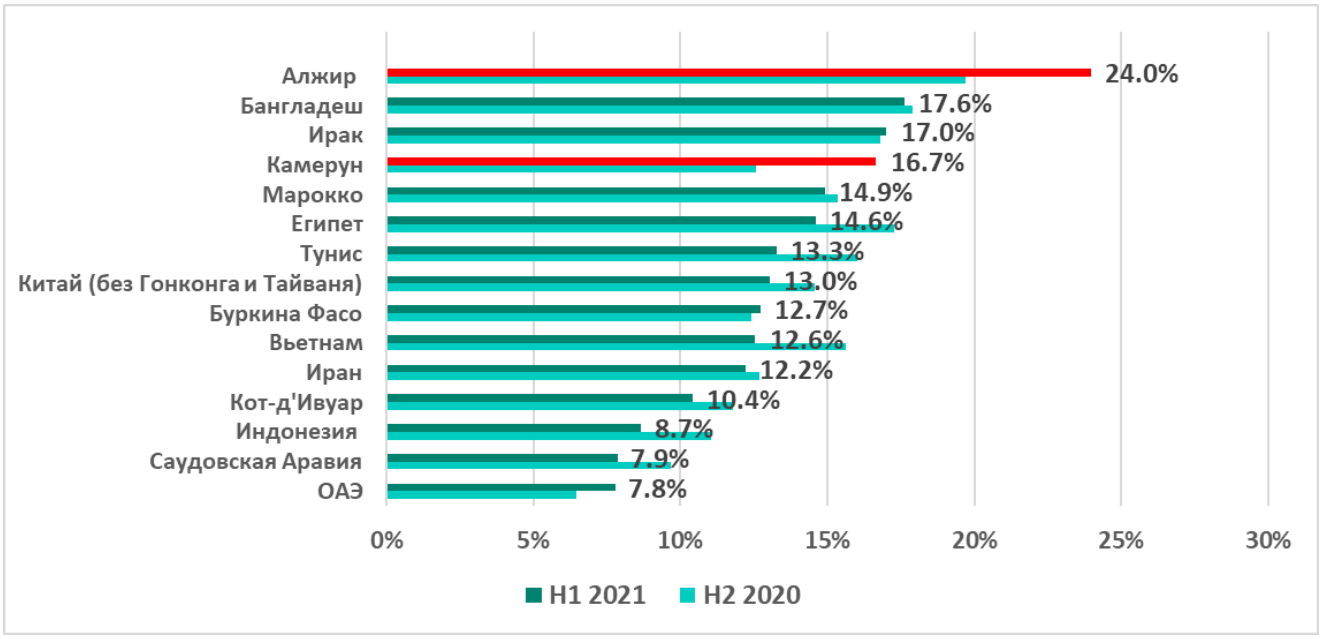
Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей в первом полугодии 2021



В Африке зафиксирован наибольший рост показателя — на 1,3 п.п.

Во всех регионах Азии данный показатель уменьшился на 1,2 — 2,2 п.п., а на Ближнем Востоке немного увеличился (на 0,6 п.п.). В результате Ближний Восток поднялся в этом рейтинге с пятого места на третье.

В первом полугодии 2021 года в список 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, традиционно не попали страны Европы, Северной Америки и Австралия.



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

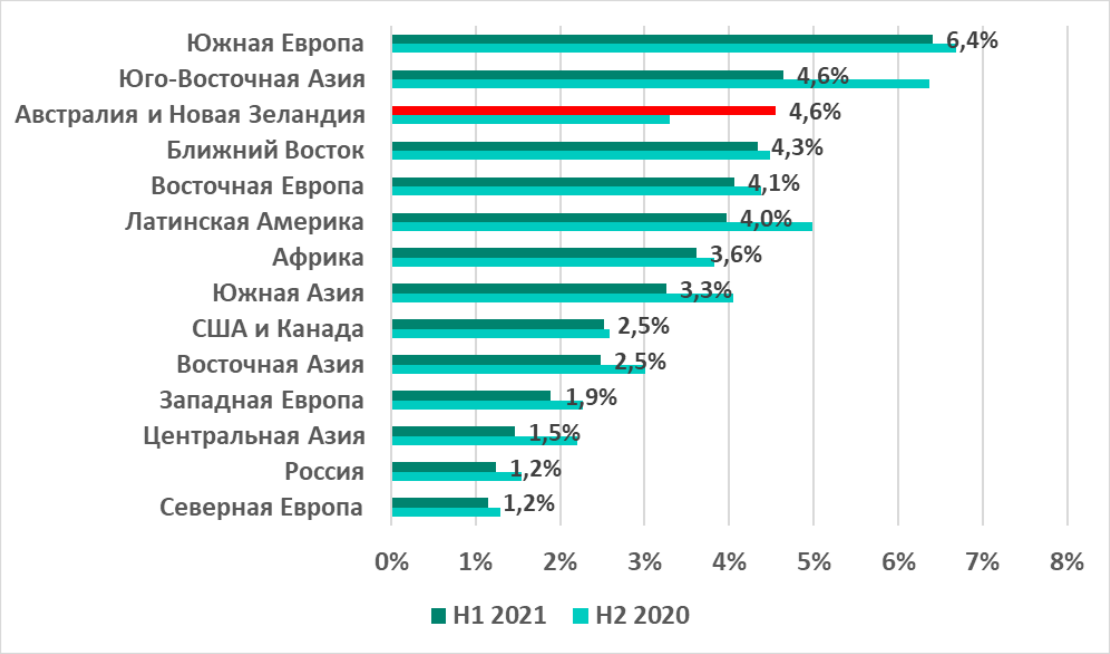
Наибольший рост показателя отмечен в Алжире и Камеруне — на 4,3 и 4,1 п.п. соответственно.

Почтовые клиенты

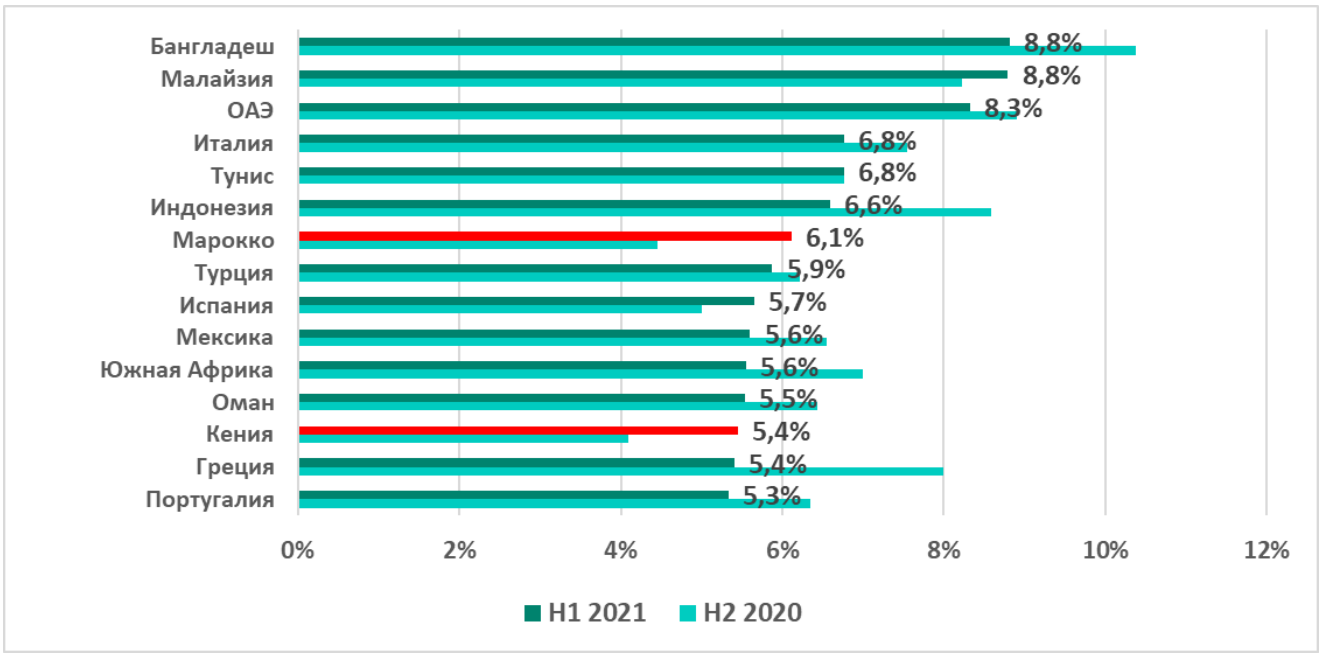
Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, как и в предыдущем полугодии, возглавили Южная Европа и Юго-Восточная Азия.

Во втором полугодии 2020 года в большинстве регионов был отмечен рост этого показателя. В первом полугодии 2021 года единственным регионом, где рост продолжился, стала Австралия и Новая Зеландия (+ 1,3 п.п.). Отметим, что в этом регионе процент компьютеров АСУ, на которых заблокированы вредоносные почтовые вложения, растет с первого полугодия 2020 года.

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



В число 15 стран с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, попали страны Южной Европы — Италия, Испания, Греция и Португалия.



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

Наиболее значительное увеличение этого показателя отмечено в Марокко и Кении — на 1,7 и 1,3 п.п. соответственно. В Греции показатель уменьшился на 2,6 п.п., и в результате страна опустилась в рейтинге с 5-го на 14-е место.

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