kaspersky

Ландшафт угроз для систем промышленной автоматизации. Статистика

Первое полугодие 2022

Kaspersky ICS CERT

08.09.2022 Version 1.0

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].

Цифры полугодия

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты:

- 31,8% — процент компьютеров АСУ в мире, на которых хотя бы раз в первом полугодии 2022 года были заблокированы вредоносные объекты.
- На 1,7 п.п. упал процент с января по март — минимум первого полугодия пришелся на март впервые за пять лет наблюдений.
- 41,5% — Африка, первое полугодие 2022 — максимальный процент среди всех регионов.
- 12,8% — Северная Европа, первое полугодие 2022 — минимальный процент среди всех регионов. И максимальный в регионе процент за полугодие за период первое полугодие 2020 — первое полугодие 2022.
- 43,2% — Тайвань, первое полугодие 2022. После неожиданного роста на 8 п.п. Тайвань по проценту за первое полугодие обогнал континентальный Китай (41,4%).
- 6,8% — Люксембург, первое полугодие 2022 — минимальный процент среди стран.

[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.

Разнообразие вредоносного ПО:

- 7219 — количество семейств вредоносных программ, заблокированных на компьютерах АСУ.
- 8,6% — процент компьютеров АСУ, на которых были заблокированы программы-шпионы. Среди отраслей по этому показателю лидирует Автоматизация зданий (12,9%).
- 2,8% — процент компьютеров АСУ, на которых были заблокированы майнеры (исполняемые файлы для ОС Windows) в производственном секторе.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели:

- 0,65% — мир, первое полугодие 2022 года — самый высокий процент полугодия за период первое полугодие 2020 — первое полугодие 2022.
- 0,27% — мир, февраль 2022 — самый высокий показатель месяца за период с января 2020 по июнь 2022.
- 1% — отрасль Автоматизация зданий, первое полугодие 2022, лидирует среди отраслей по проценту компьютеров АСУ, атакованных программами-вымогателями.
- 0,95% — Восточная Азия, первое полугодие 2022, лидирует среди регионов по проценту компьютеров АСУ, атакованных программами-вымогателями.
- 0,89% — Ближний Восток, первое полугодие 2022. Ближний Восток занял второе место в рейтинге регионов по программам-вымогателям. В этом регионе с 2020 года процент компьютеров АСУ, на которых за полугодие были заблокированы программы-вымогатели, вырос в 2,5 раза.
- 9 из 14 — количество регионов, в которых в первом полугодии 2022 года вырос процент компьютеров АСУ, на которых были заблокированы программы-вымогатели.

Источники угроз:

- 14,4% — процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки в отрасли Автоматизация зданий. Показатель этой отрасли в два раза больше, чем в среднем в мире (7%). Специалисты, занятые в сфере автоматизации зданий, активно пользуются интернет-ресурсами и почтой и могут оказаться «точкой входа» злоумышленников в инфраструктуру целевой организации.

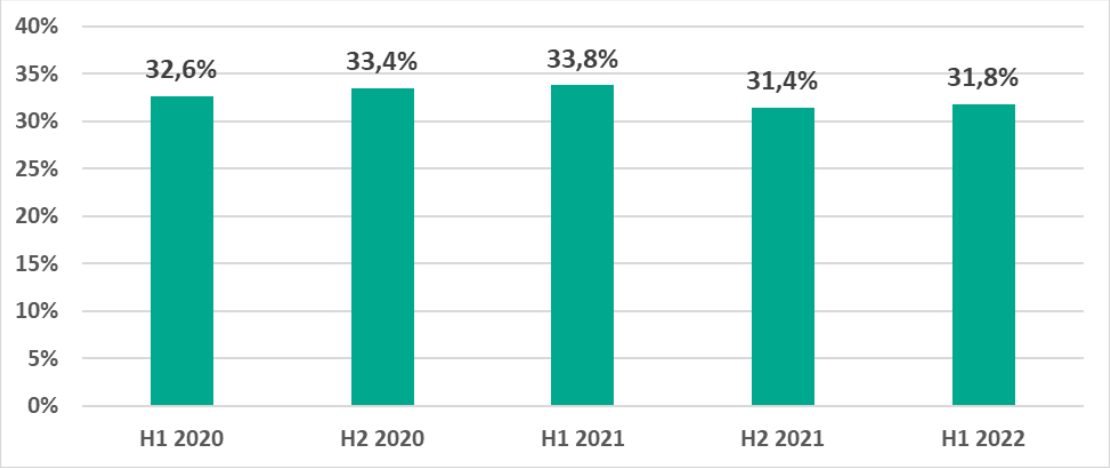
- 10,4% — процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, в отрасли Нефть и газ, — это в 3 раза больше, чем в среднем в мире (3,5%).
- 1,2% — процент компьютеров АСУ в отрасли Нефть и газ, на которых было заблокировано вредоносное ПО в сетевых папках, — это в два раза больше, чем в среднем в мире (0,6%).

Мир, общая статистика

Процент компьютеров, на которых были заблокированы вредоносные объекты

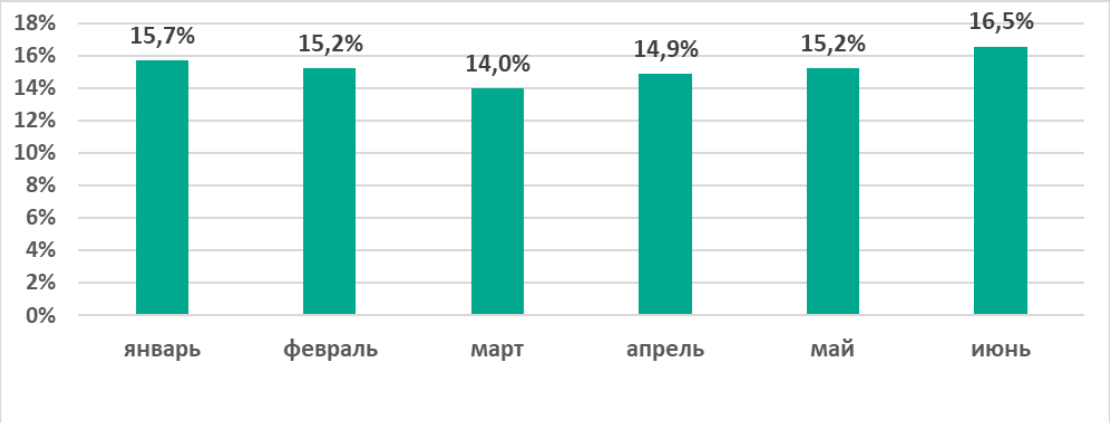
В первом полугодии 2022 года вредоносные объекты были заблокированы на 31,8% компьютеров АСУ.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



В течение первых шести месяцев года наибольший процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался в июне, наименьший — в марте.

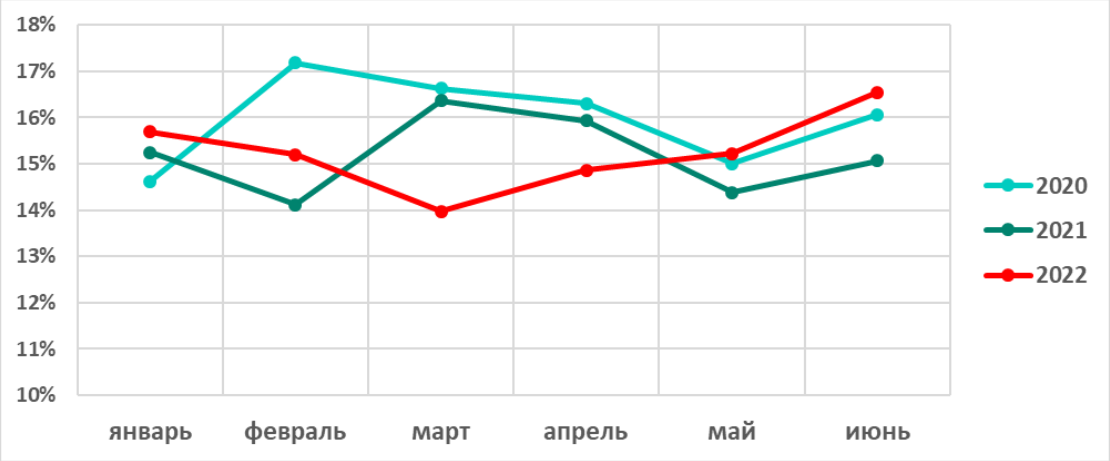
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — июнь 2022



Отметим, что за последние пять лет минимум первого полугодия впервые пришелся на март. Обычно минимумы в месячной статистике связаны с периодами отпусков и праздничных дней — в частности, в летние месяцы, а также в декабре и январе. Это, вероятно, связано со снижением активности пользователей, и, как следствие, снижением процента компьютеров, на которых было заблокировано вредоносное ПО.

Мы полагаем, что отклонение, наблюдаемое нами в марте, также связано со снижением пользовательской активности, но уже по причине нарушения цепочек поставок, оно также может быть обусловлено всплеском случаев заражения COVID в январе и марте 2022 года.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — июнь 2020, 2021, 2022

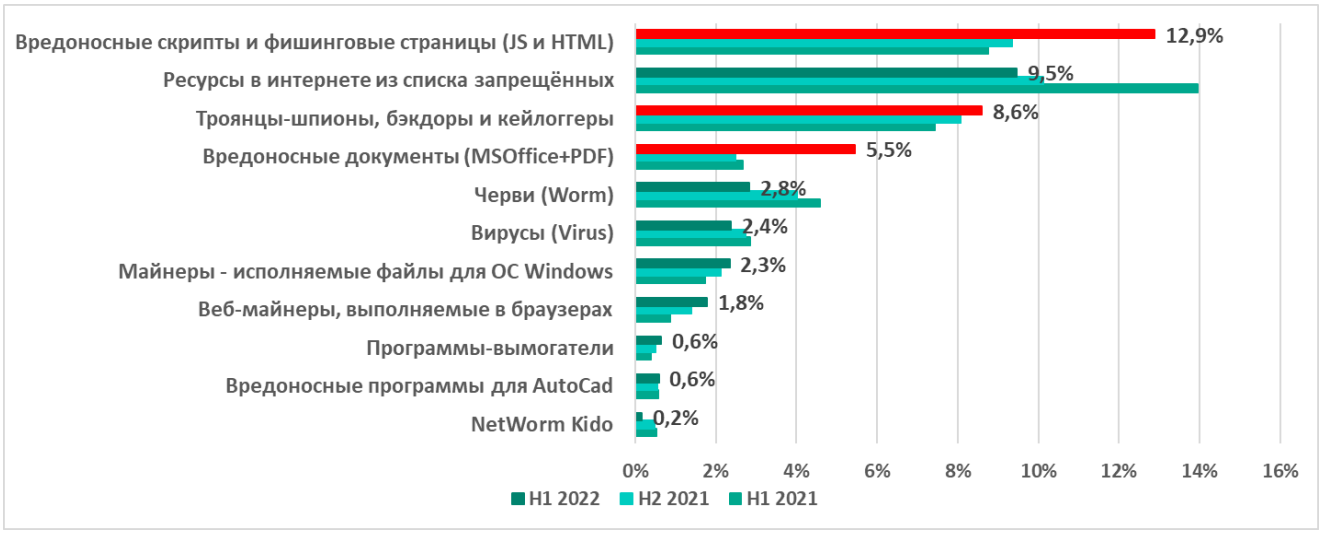


Разнообразие обнаруженного вредоносного ПО

В первом полугодии 2022 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 102 тысяч модификаций вредоносного ПО из 7219 различных семейств.

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.

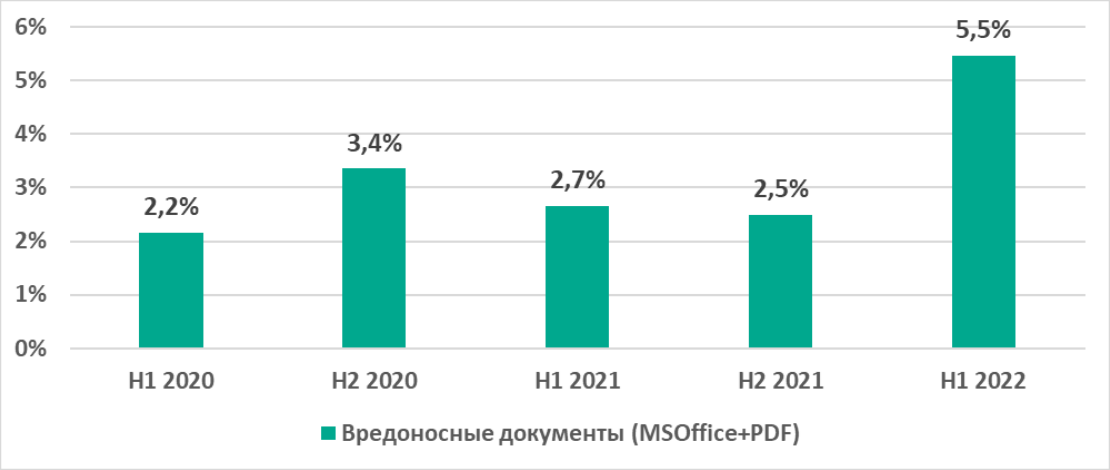
В первом полугодии 2022 года наиболее значительно увеличился процент компьютеров АСУ, на которых были заблокированы:

- **Вредоносные скрипты и фишинговые страницы (JS и HTML)** — на 3,5 п.п.
- **Вредоносные документы** — на 3,0 п.п.
- **Шпионское ПО** — троянцы-шпионы, бэкдоры и кейлоггеры — на 0,5 п.п.

Вредоносные скрипты и фишинговые страницы распространяются как в интернете, так и в письмах, рассылаемых в электронной почте.

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях. Такие методы активно используются для первичного заражения компьютеров.

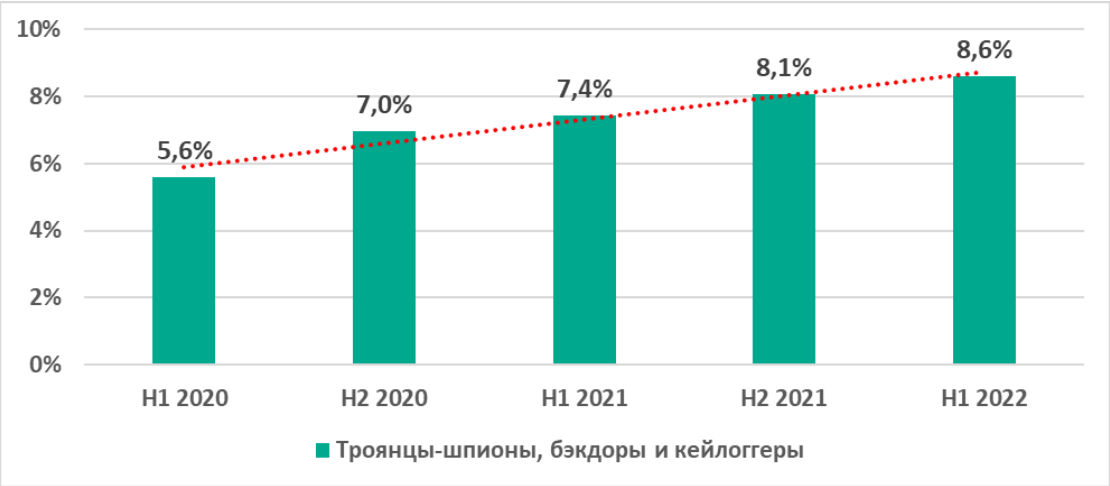
Процент компьютеров АСУ, на которых были заблокированы вредоносные документы (MSOffice+ PDF)



На следующем этапе на зараженные компьютеры чаще всего загружаются **шпионские программы**, которые используются для кражи конфиденциальной информации, получения удаленного доступа к зараженным компьютерам и загрузки целевого вредоносного ПО, в том числе — **программ-вымогателей** (о них мы расскажем подробнее — см. ниже).

Процент компьютеров АСУ, на которых блокируются программы-шпионы, растет с 2020 года.

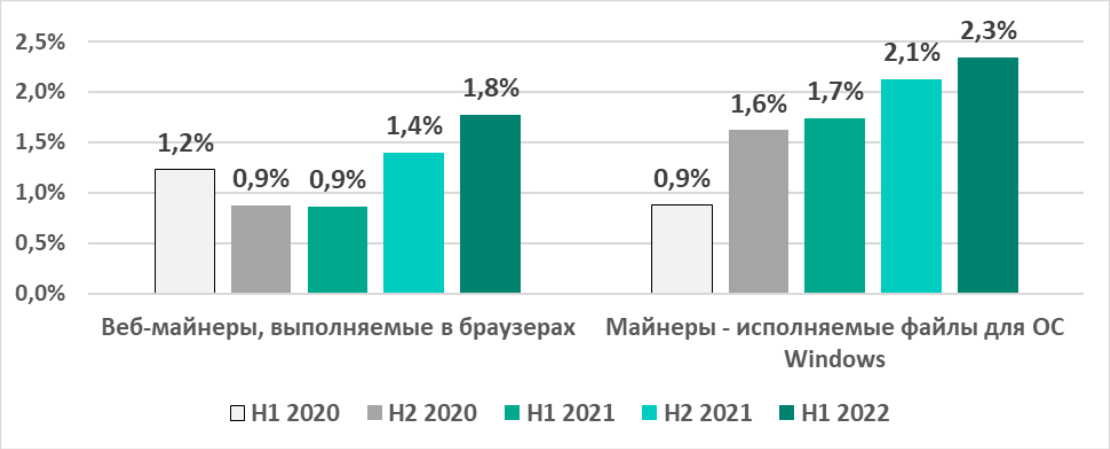
Процент компьютеров АСУ, на которых были заблокированы программы-шпионы



Продолжился постепенный рост процента компьютеров АСУ, на которых были заблокированы вредоносные программы для скрытого майнинга криптовалюты:

- **Веб майнеры, исполняемые в браузерах,** — на 0,4 п.п.
- **Майнеры - исполняемые файлы для ОС Windows** — на 0,2 п.п.

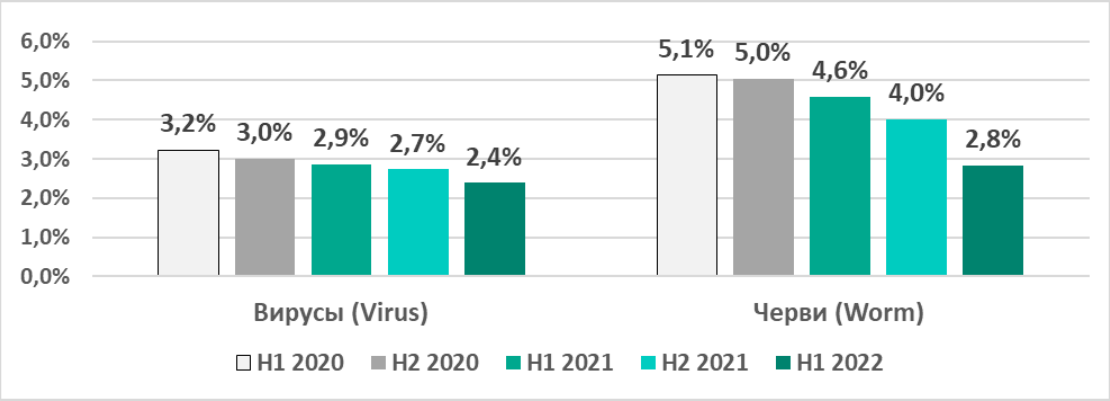
Процент компьютеров АСУ, на которых были заблокированы вредоносные программы для скрытого майнинга криптовалюты



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

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).

Среди распространяющихся вирусов и червей довольно много старых (например, таких как Kido/Conficker). Несмотря на то, что их командные серверы уже отключены, 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.

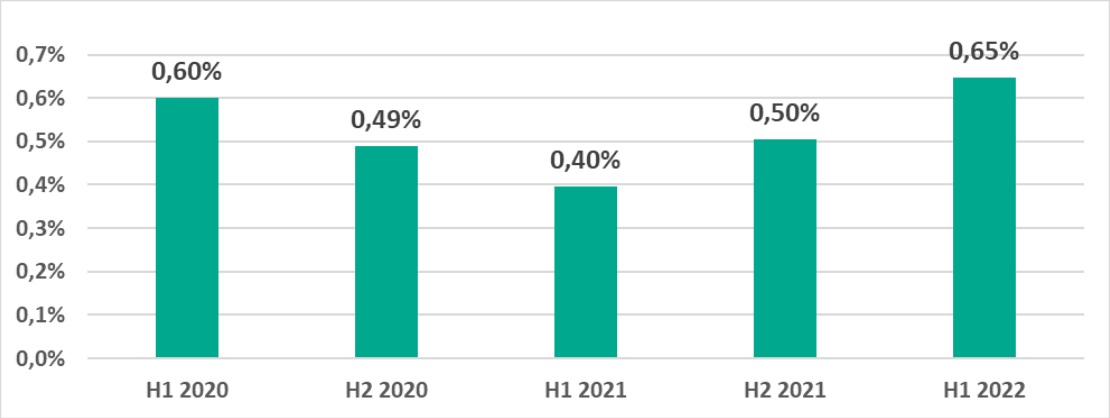
Вместе с тем, в сетях АСУ встречаются и новые версии червей, используемые злоумышленниками для распространения в сети шпионского ПО, программ-вымогателей и майнеров. Чаще всего для распространения по сети эти черви используют эксплойты для исправленных производителями, но еще актуальных в технологических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

Уменьшение процента компьютеров АСУ, на которых блокируется такое вредоносное ПО, обусловлено, в том числе, и более тщательной проверкой съемных носителей — процент компьютеров АСУ, на которых было заблокировано вредоносное ПО при присоединении съемных носителей, уменьшается уже несколько полугодий подряд.

Программы — вымогатели

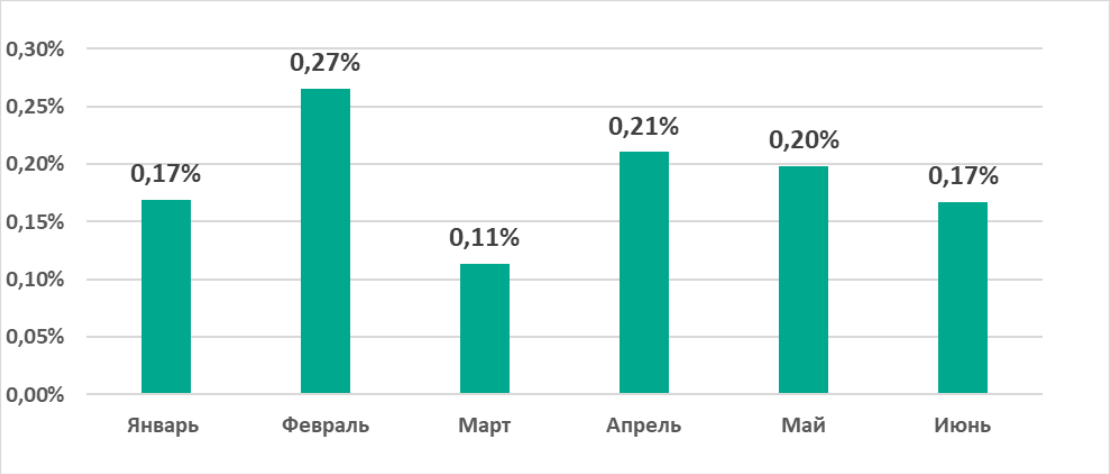
В первом полугодии 2022 года вредоносные программы-вымогатели были заблокированы на 0,65% компьютеров АСУ. Это самый высокий процент за полугодие за период первое полугодие 2020 года — первое полугодие 2022 года.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели



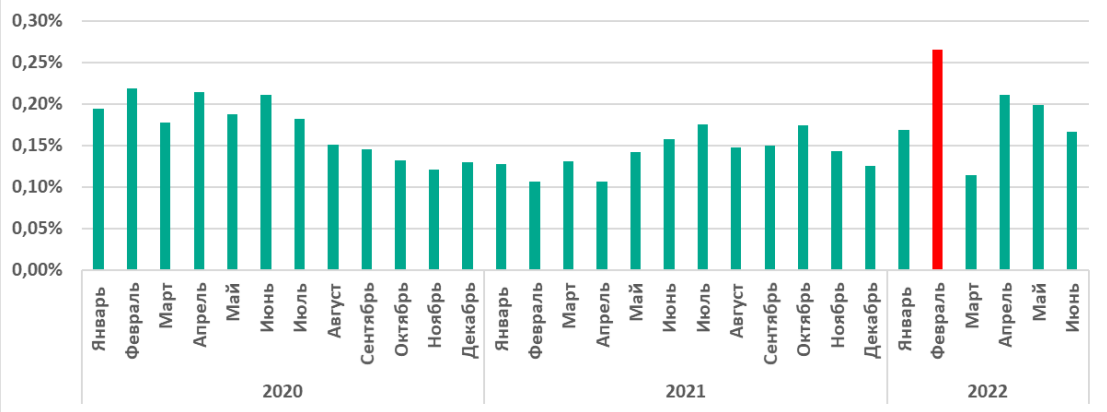
Наибольшее значение процента компьютеров АСУ, на которых были заблокированы программы-вымогатели, было отмечено в феврале, наименьшее — в марте.

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



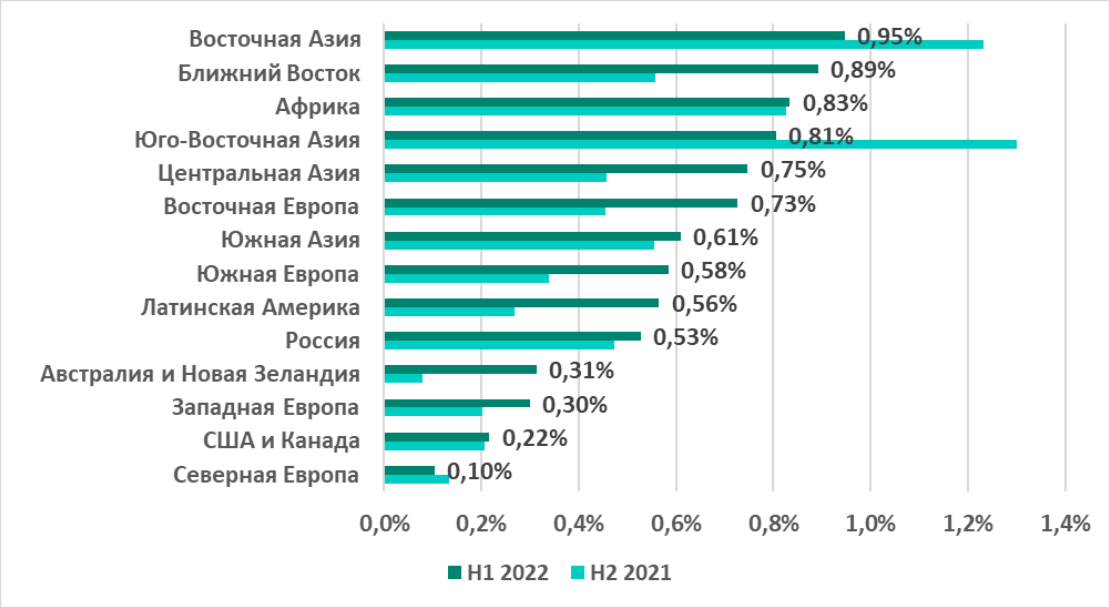
Показатель февраля оказался рекордным для двух с половиной лет наблюдений.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь 2020 — июнь 2022



В первом полугодии 2022 года процент атакованных вымогателями компьютеров АСУ увеличился в 9 регионах мира.

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



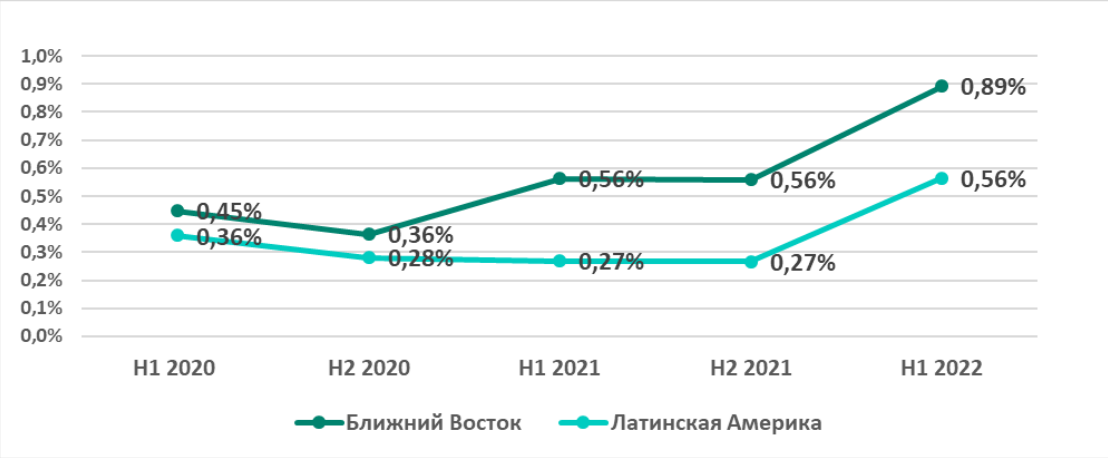
Наиболее значительно этот показатель вырос на Ближнем Востоке и в Латинской Америке.

Изменение в регионах мира процента компьютеров АСУ, на которых были заблокированы программы-вымогатели

На Ближнем Востоке с 2020 года процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, постепенно вырос в 2,5 раза.

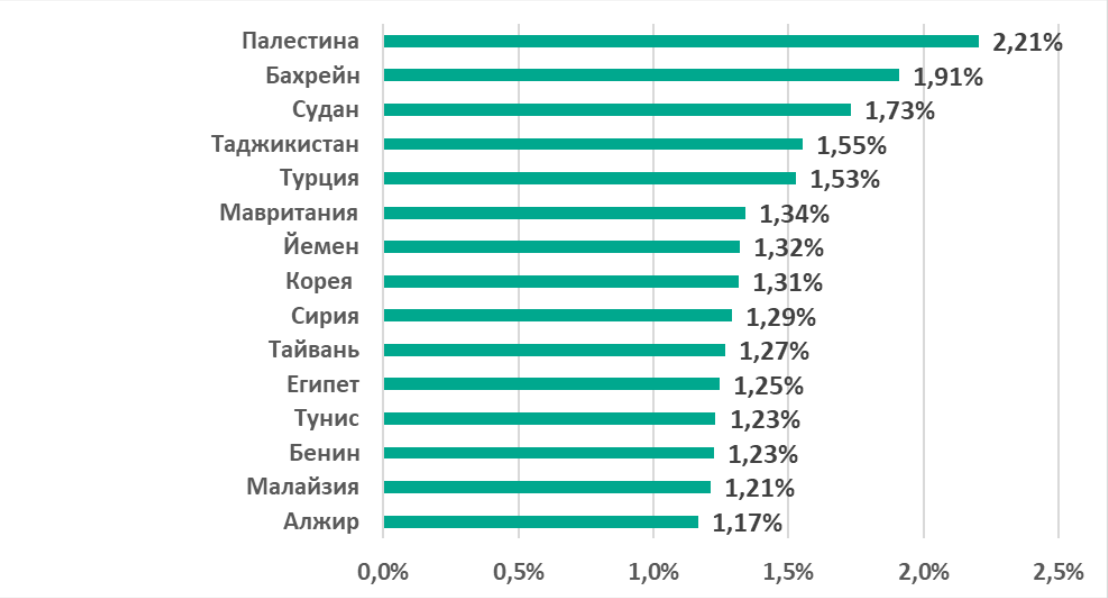
В Латинской Америке он уменьшался вплоть до конца 2021 года, а в первом полугодии 2022 увеличился по сравнению с предыдущим полугодием вдвое.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, на Ближнем Востоке и в Латинской Америке



В числе 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы программы-вымогатели, лидирует Палестина.

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

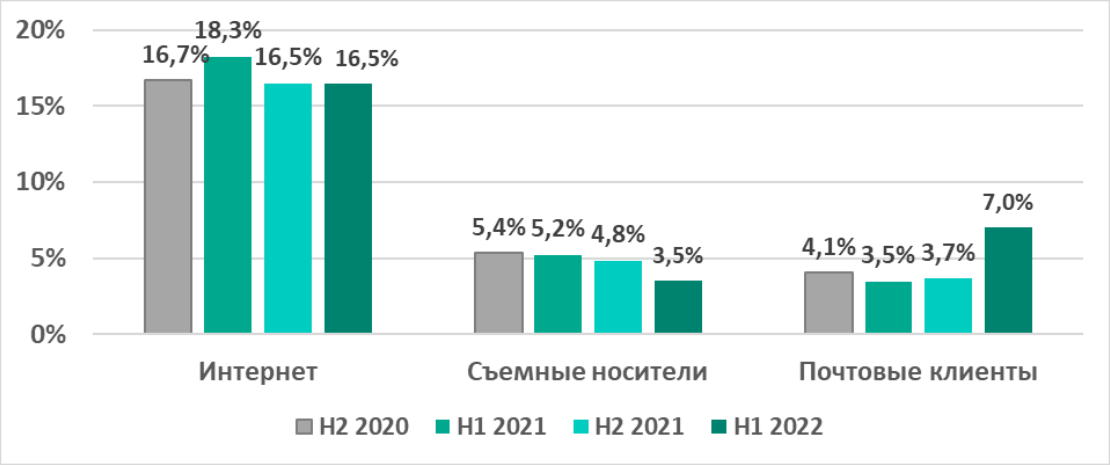


Этот рейтинг каждое полугодие обновляется, но три страны — Алжир, Египет и Турция — остались в нем с прошлого полугодия.

Источники угроз

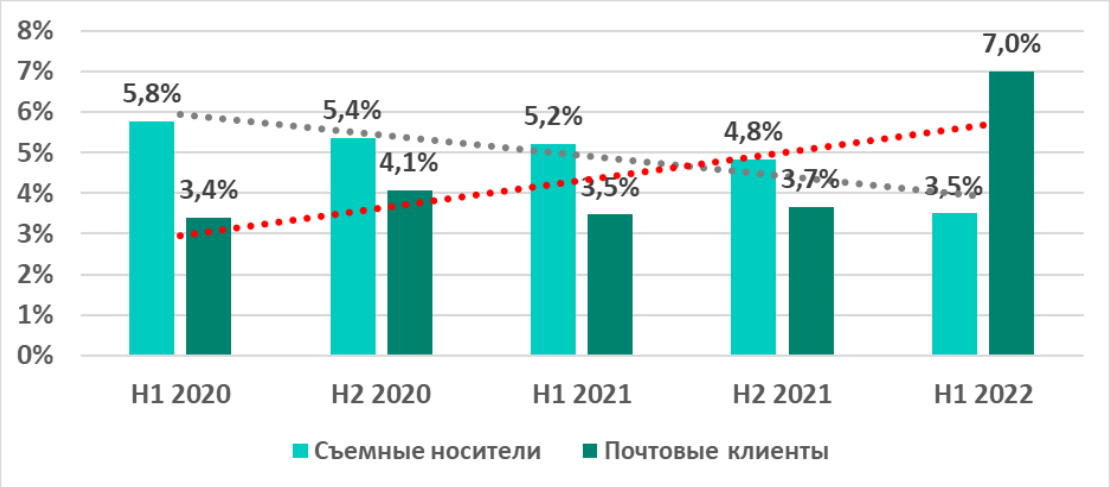
Основными источниками угроз для компьютеров в технологической инфраструктуре организаций являются интернет, съемные носители и электронная почта.

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



В первом полугодии 2022 продолжил уменьшаться процент компьютеров АСУ, на которых вредоносное ПО было заблокировано при подключении съемных носителей.

Процент компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей и вредоносные почтовые вложения и фишинговые ссылки



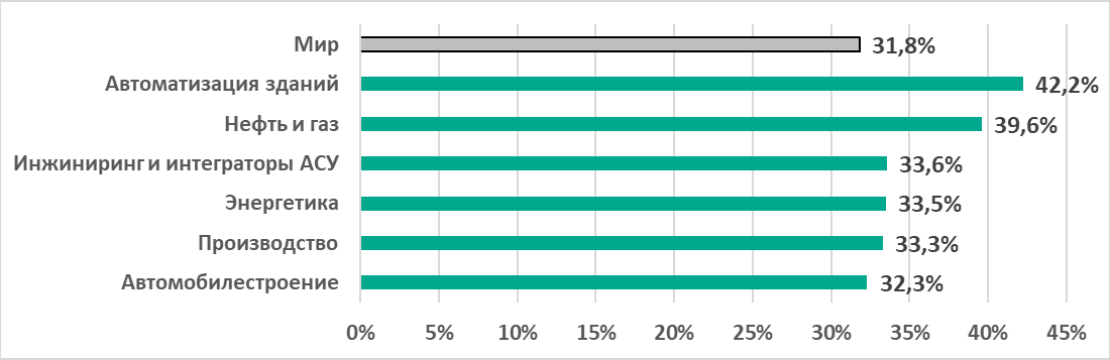
В то же время мы наблюдаем устойчивый рост процента компьютеров АСУ, на которых были заблокированы почтовые вложения и фишинговые ссылки. Заметная разница между вторым полугодием 2021 и первым полугодием 2022 года обусловлена, в частности, увеличением количества машин АСУ, которые поставляют нам анонимную статистику. Значительная часть «новых» машин — компьютеры инженеров АСУ и системы автоматизации зданий, на которых активно используются почтовые клиенты (см. статистику по индустриям ниже). Вклад таких машин в общий прирост процента компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и/или фишинговые ссылки, составил 2–2,5 п.п., в то время как остальные компьютеры АСУ обеспечили прирост порядка 1 п.п.

Некоторые отрасли

Мы выбрали несколько отраслей, чтобы посмотреть, как отличается ситуация в разных индустриях.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, во всех выбранных нами для исследования отраслях больше, чем в среднем по миру.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях, первое полугодие 2022

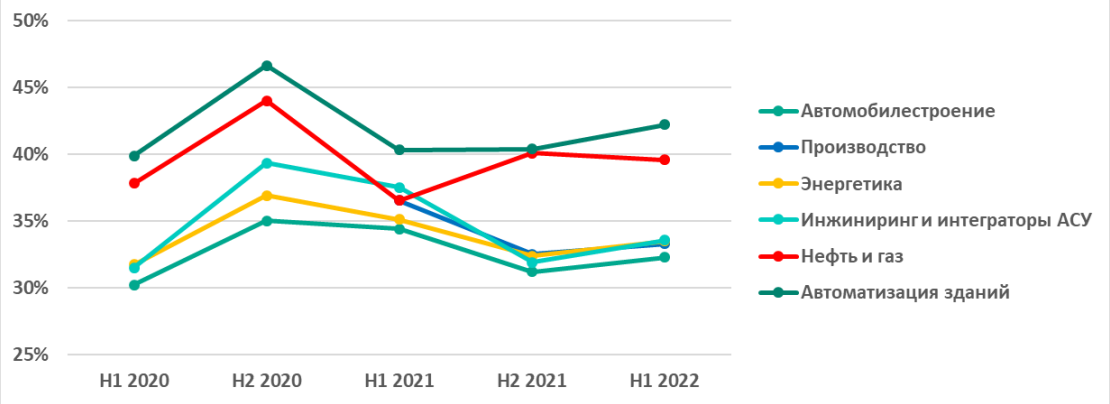


Две отрасли — Автоматизация зданий и Нефть и газ — лидируют с отрывом от отрасли на третьем месте в 8,6 п.п. и 6 п.п. соответственно.

Показатели отраслей Инжиниринг и интеграторы АСУ, Энергетика и Производство отличаются на десятые доли процентных пунктов.

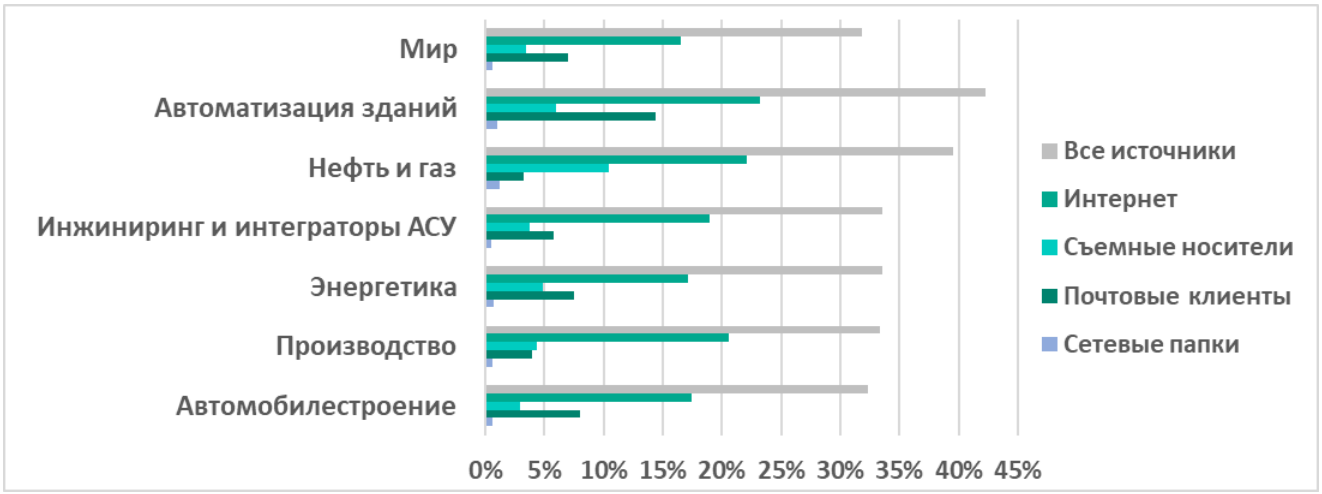
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, во всех исследуемых отраслях уменьшался в 2021 году. Исключением стала нефтегазовая отрасль, в которой во втором полугодии 2021 года процент вырос. А в первом полугодии 2022 эта отрасль стала единственной из исследуемых, где процент немного уменьшился — во всех остальных отраслях зафиксирован небольшой рост.

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



Несмотря на рост процента атакованных компьютеров АСУ, по итогам первого полугодия 2022 года во всех исследуемых отраслях он меньше показателей второго полугодия 2020 года.

Интернет, почта и съемные носители — основные источники угроз для компьютеров АСУ во всех отраслях.



Процент компьютеров АСУ, на которых было заблокировано вредоносное ПО из разных источников, в некоторых отраслях, первое полугодие 2022

Автоматизация зданий

Автоматизация зданий занимает первое место в рейтинге выбранных отраслей по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты (42,2%).

Эта отрасль — самая «беспокойная» из исследуемых, она лидирует и в большинстве рейтингов отраслей по вредоносному ПО различных типов, и по некоторым источникам угроз.

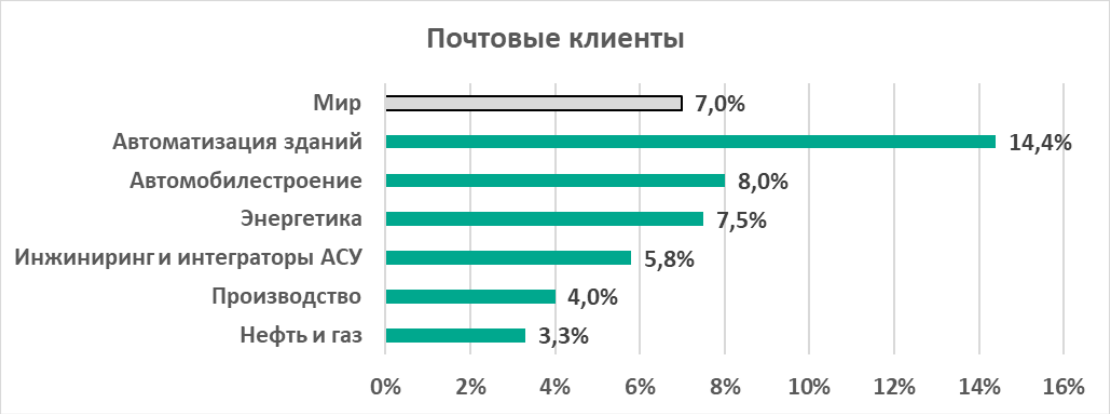
Как видно на графиках ниже, занятые в сфере автоматизации зданий специалисты активнее других пользуются интернет-ресурсами и почтой. Соответственно, они могут оказаться более доступной для злоумышленников «точкой входа» в инфраструктуру целевой организации. А учитывая тот факт, что функция мониторинга и управления системами автоматизации зданий часто выносится за рамки организационной структуры предприятия и получается, например, в виде сервиса, оказываемого третьей стороной, скомпрометированный компьютер инженера или оператора систем автоматизации зданий может легко открыть дорогу злоумышленникам сразу во много организаций.

Автоматизация зданий занимает первое место в рейтингах по проценту компьютеров АСУ, на которых были заблокированы:

- Вредоносные объекты из интернета

- Угрозы, распространяемые в интернете:
  - ресурсы в интернете из списка запрещённых (11,5%),
  - вредоносные скрипты и фишинговые страницы (17,7%).

- Вредоносные почтовые вложения и фишинговые ссылки. Автоматизация зданий лидирует с большим отрывом от остальных отраслей, при этом процент в этой отрасли вдвое превышает аналогичный показатель в среднем по миру.

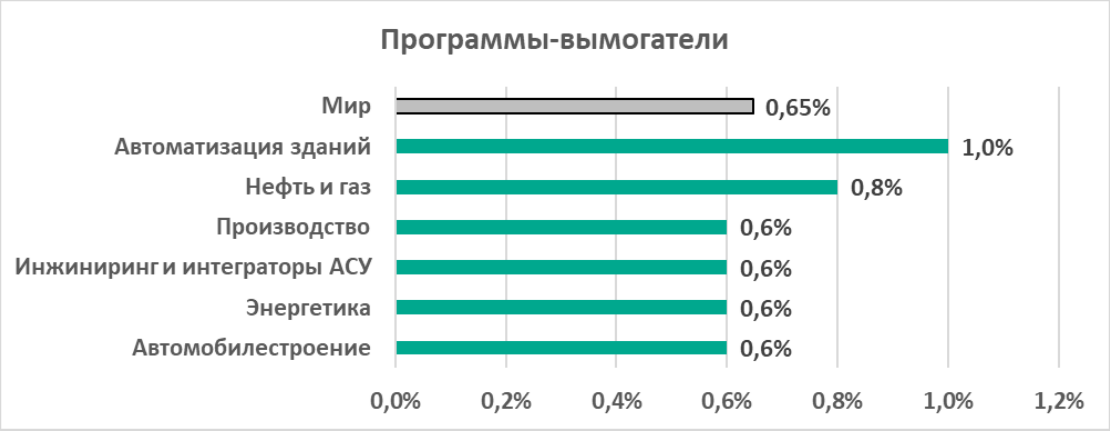


- Вредоносные документы офисных форматов, которые чаще всего распространяются в фишинговых письмах. Процент отрасли

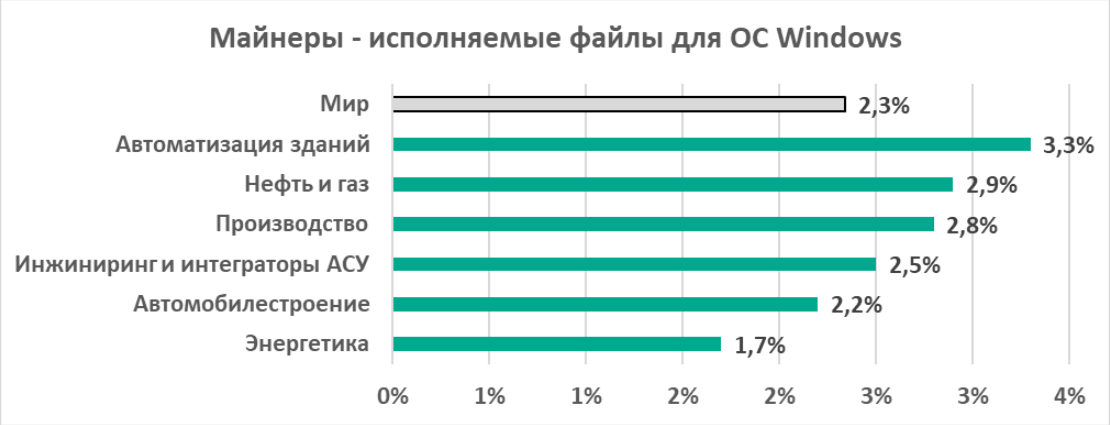
Автоматизация зданий и в этом рейтинге ожидаемо превышает средний по миру почти вдвое.

- Шпионское ПО — наиболее частая вредоносная нагрузка фишинговых рассылок — также обнаруживается на б*о*льшем проценте компьютеров, чем в остальных отраслях.

- Программы-вымогатели



- Вредоносные программы для скрытого майнинга криптовалюты



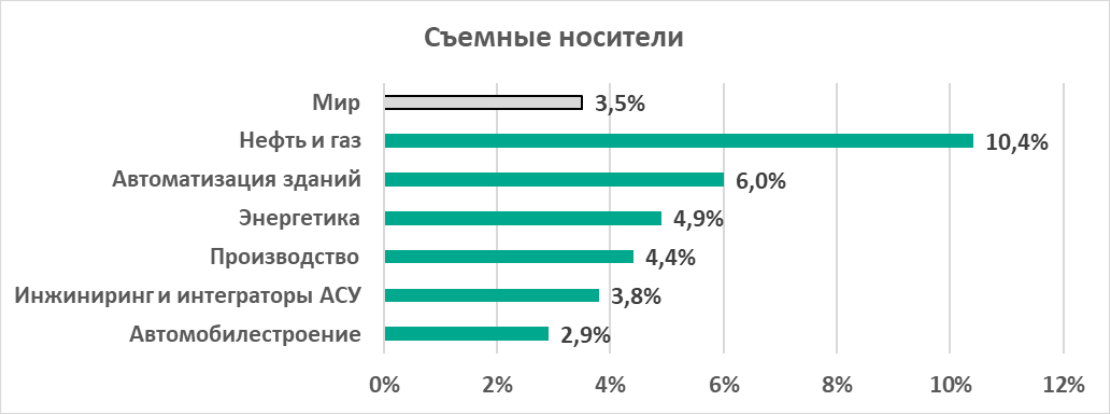
Нефть и газ

Нефть и газ занимает **второе место** в рейтингах выбранных отраслей по проценту компьютеров АСУ, на которых были заблокированы:

- все вредоносные объекты (39,6%),
- программы-вымогатели (0,8%),
- майнеры — исполняемые файлы для ОС Windows (2,9%) (см. графики выше).

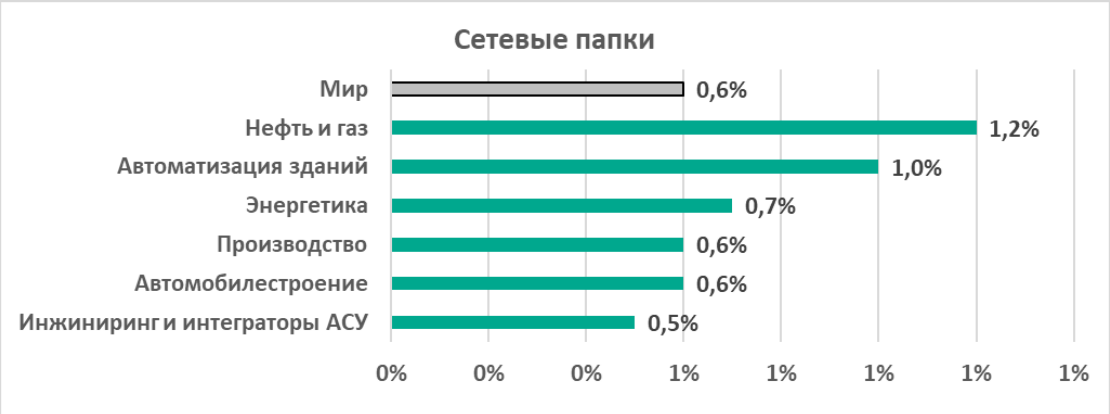
В свою очередь, нефть и газ лидирует в рейтингах по компьютерам АСУ, на которых было заблокировано вредоносное ПО:

- При подключении съемных носителей.

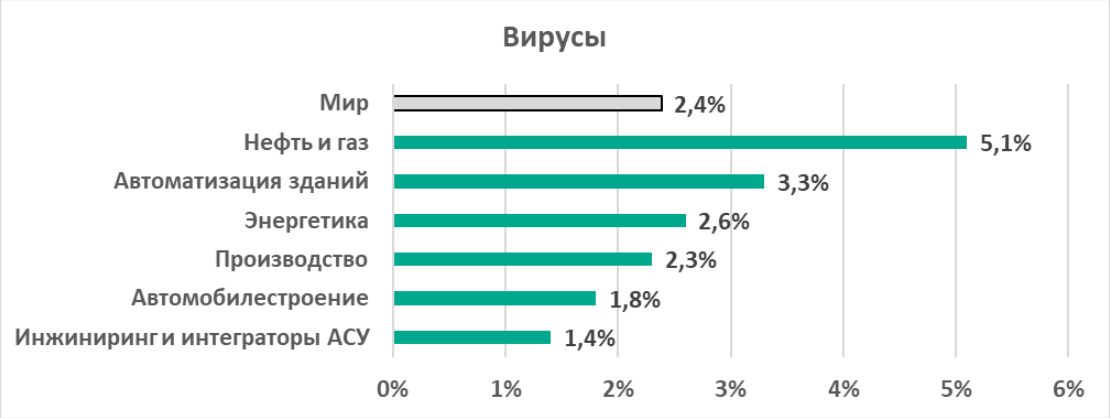


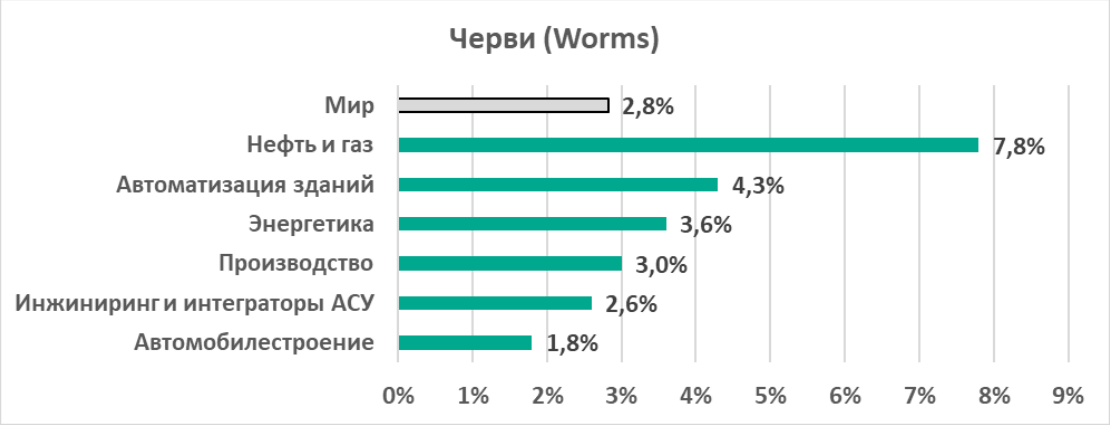
По нашему мнению, столь высокий процент компьютеров, на которых вредоносное ПО блокируется при подключении съемных носителей, может быть обусловлен, прежде всего, спецификой отрасли. Большое количество территориально распределённых предприятий, часто с плохими каналами связи между удалёнными системами и объектами, вынуждает при выполнении задач обслуживания активнее, чем на предприятиях других отраслей, пользоваться съёмными носителями.

- В сетевых папках.



- Вирусы и черви.





То, что отрасль Нефть и газ лидирует по проценту компьютеров АСУ, атакованных вирусами и червями, не удивительно — ведь это вредоносное ПО распространяется в сетях АСУ преимущественно через съемные носители и сетевые папки.

Производство

Производственная отрасль занимает **третье место** в рейтингах выбранных отраслей по проценту компьютеров АСУ, на которых были заблокированы:

- угрозы из интернета (20,6%),
- майнеры — исполняемые файлы для ОС Windows (2,8%).

Второе место досталось этой отрасли в рейтинге по веб-майнерам, исполняемым в браузерах (2,4%) (см. графики выше).

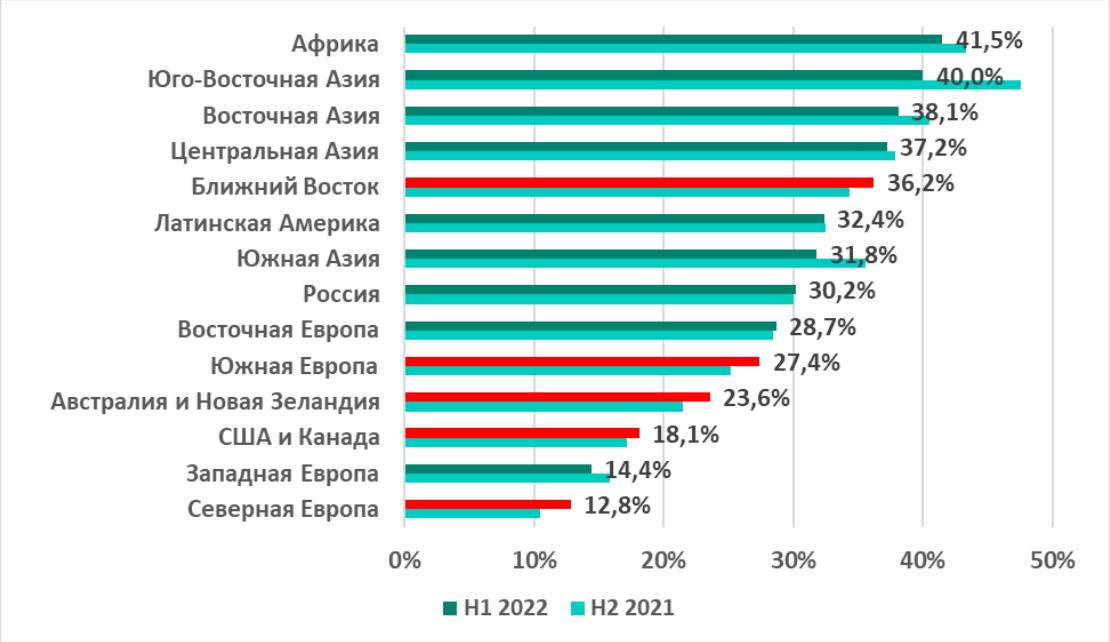
Регионы и страны

На карте ниже для каждой страны отражен процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по отношению к общему количеству таких компьютеров в стране.

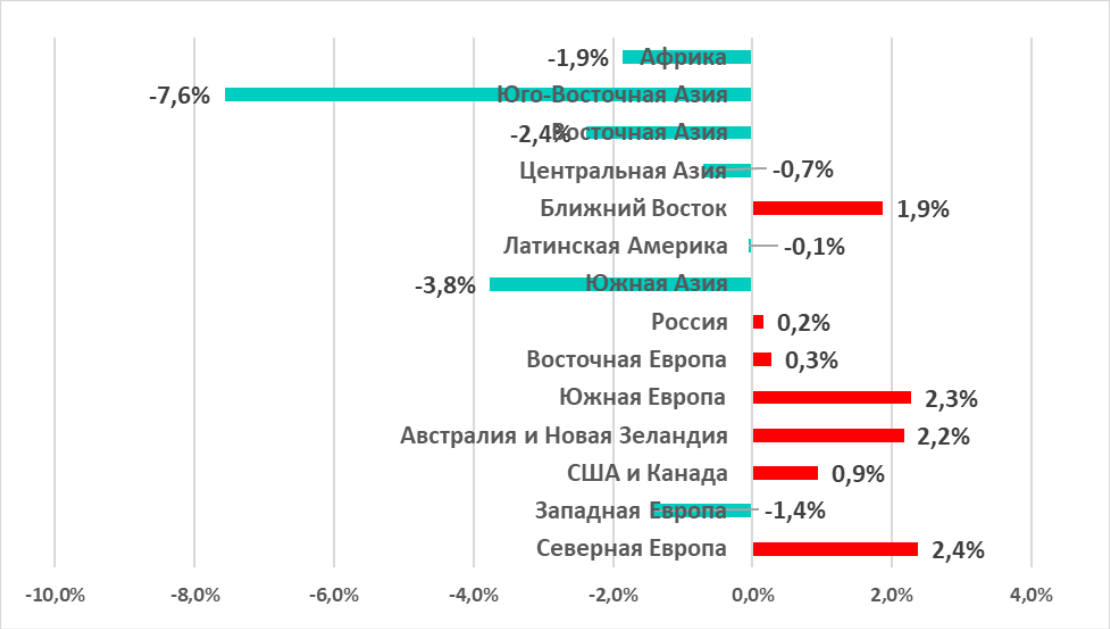
Регионы

В рейтинге регионов мира по доле компьютеров 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



Изменение в первом полугодии 2022 года процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионах мира



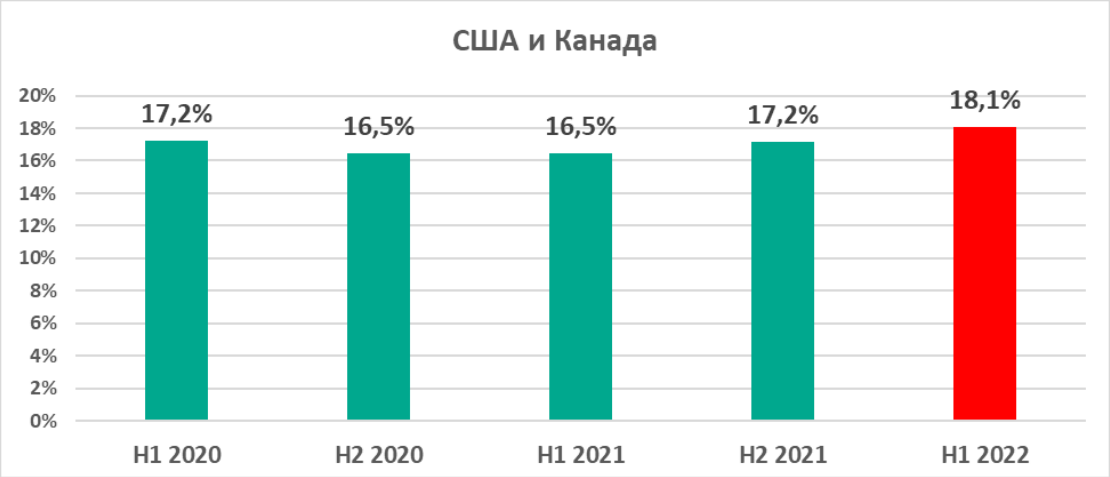
Как видно на графиках, в первом полугодии 2022 процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, вырос в 7 из 14 регионов. Все они, за исключением Ближнего Востока, находятся в нижней части рейтинга, то есть относятся к более благополучным по этому показателю. Единственный благополучный регион, в котором показатель снизился, — Западная Европа.

В то же время в регионах, занимающих первые семь позиций в рейтинге по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты (то есть менее благополучных по этому признаку), процент уменьшился. Исключением в этом случае стал упомянутый выше Ближний Восток.

В США и Канаде, а также в Северной Европе отмечен максимальный за два с половиной года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Северной Европе

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в США и Канаде



Страны

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты, первое полугодие 2022

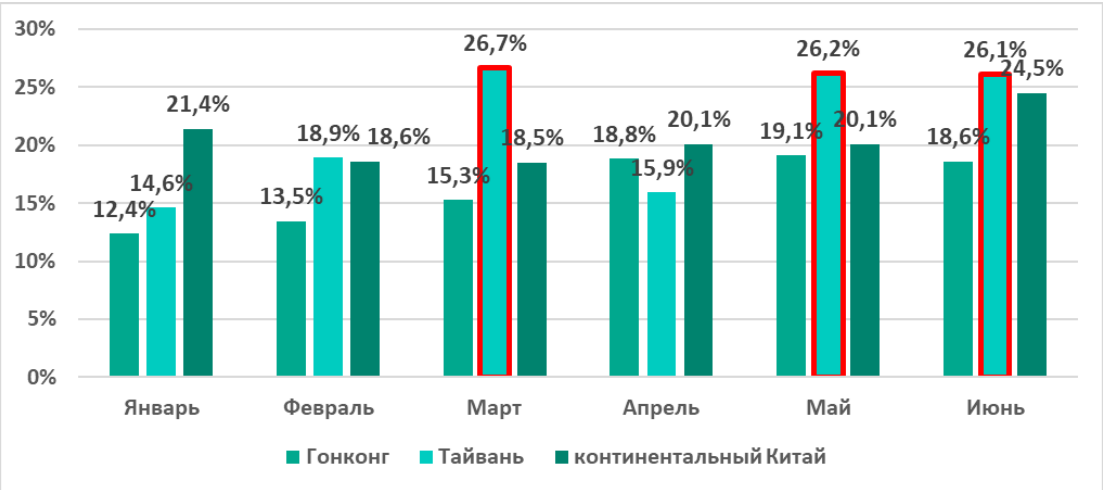
В тройку стран и территорий, где отмечено самое значительное за первое полугодие 2022 года увеличение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, вошли Южная Африка (+ 11,5 п.п.), Дания (+ 9,4 п.п.) и Тайвань (+ 8,0 п.п.). В первом полугодии 2022 года у них был максимальный показатель за период первое полугодие 2020 — первое полугодие 2022.

В 2021 году мы отмечали, что процент атакованных компьютеров АСУ относительно стабилен на Тайване, постепенно растет в Гонконге и уменьшается в материковом Китае. В Гонконге и материковом Китае в первой половине 2022 года тенденции сохранились, а на Тайване показатель вырос настолько, что по проценту атакованных компьютеров АСУ Тайвань даже обогнал континентальный Китай.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Гонконге, на Тайване и в континенталь-ном Китае

Особенно высоким процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, на Тайване был в марте, мае и июне.

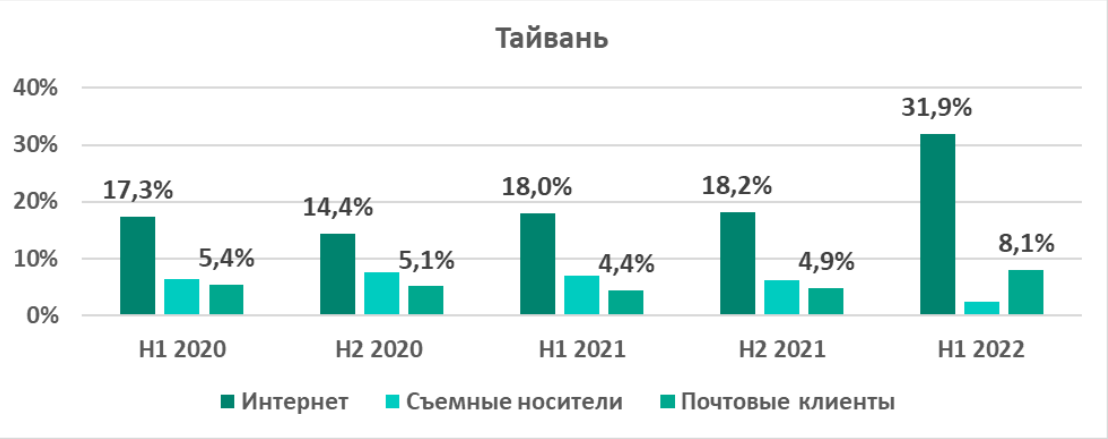
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Гонконге, на Тайване и в континенталь-ном Китае, январь — июнь 2022



В то же время по итогам первого полугодия 2022 года на Тайване вырос процент компьютеров АСУ, на которых были заблокированы угрозы из

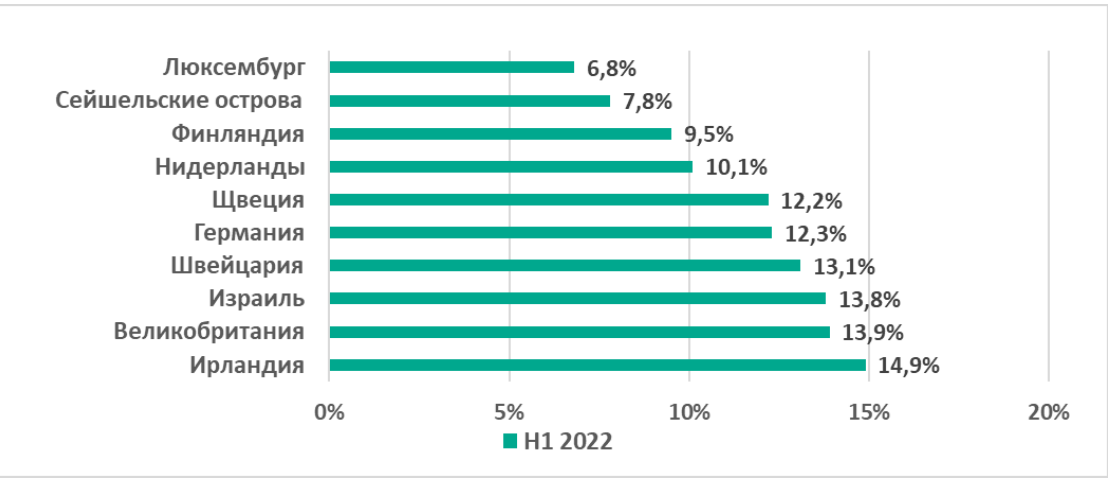
интернета (Тайвань даже занял первое место в рейтинге стран и территорий по этому показателю). Этот рост во многом обусловлен тем, что на Тайване в этот период была агрессивная рекламная кампания, в ходе которой пользователи перенаправлялись на фишинговые ресурсы.

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



Как и во втором полугодии 2021 года, наименьший процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в первом полугодии 2022 года отмечен в Люксембурге.

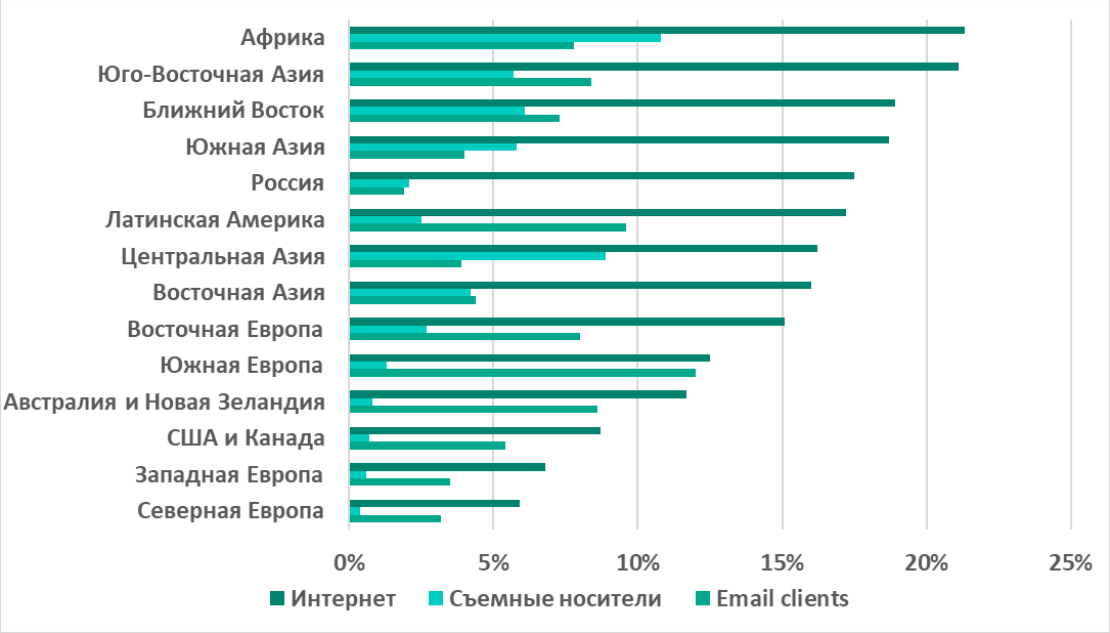
10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты, первое полугодие 2022



Самое значительное уменьшение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, — во Вьетнаме (-11,0 п.п.), в Ираке (-9,7 п.п.) и в Тунисе (-8,5 п.п.).

Основные источники угроз: география

Основные источники угроз, заблокированных на компьютерах АСУ, в регионах мира, первое полугодие 2022

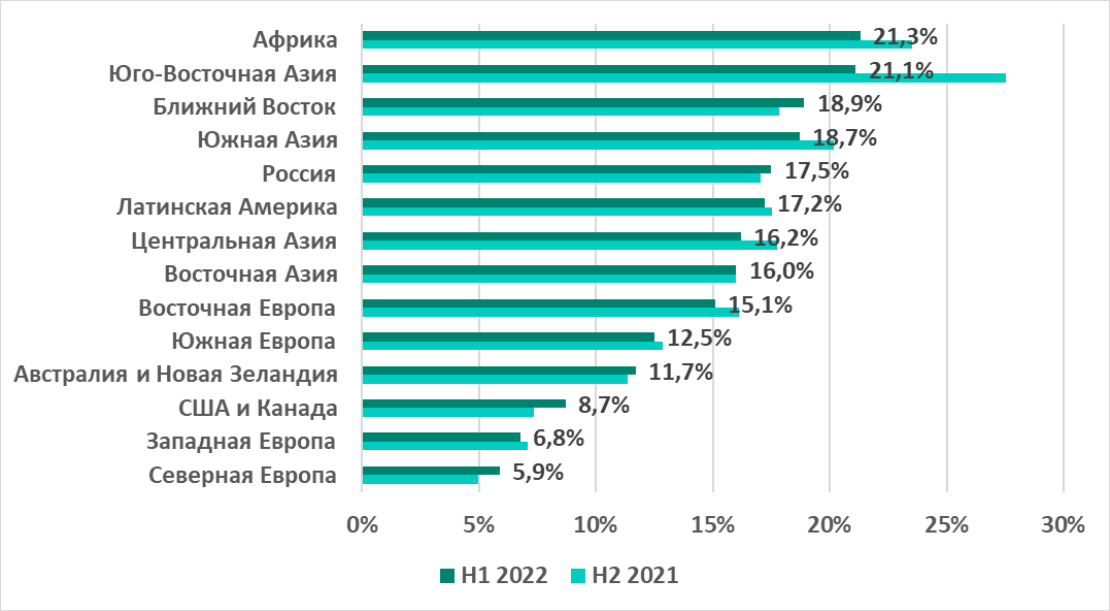


Отметим, что процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников, удается установить не во всех случаях.

Интернет

Процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, в первом полугодии 2022 года увеличился на Ближнем Востоке (+ 1,1 п.п.), в России (+ 0,5 п.п.), Северной Америке (+ 1,3 п.п.) и Северной Европе (+ 0,9 п.п.).

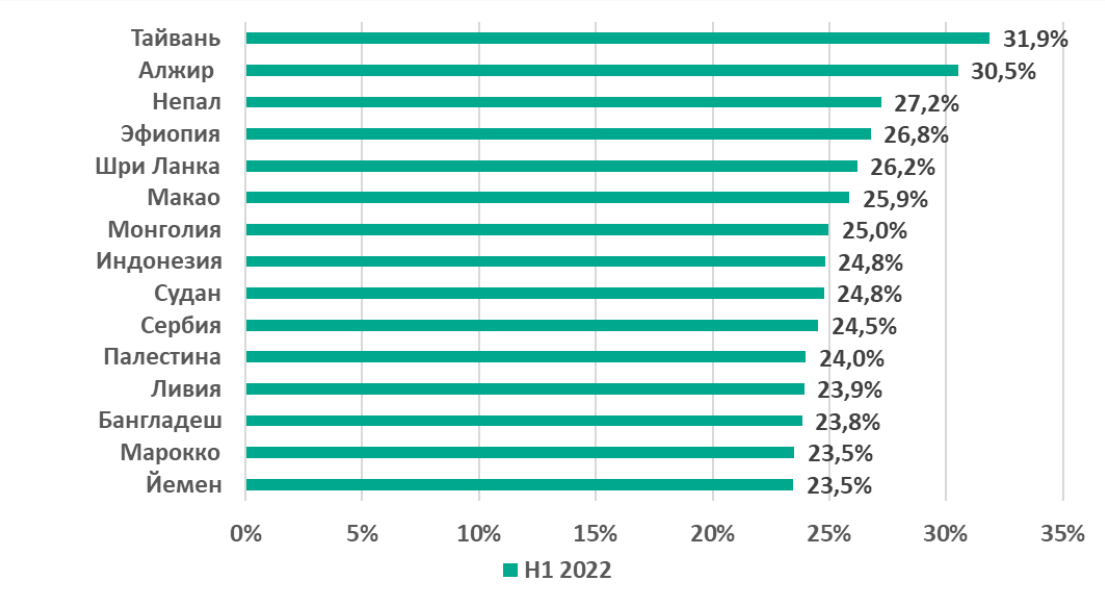
Процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, в регионах мира



Заметное уменьшение показателя отмечено в Юго-Восточной Азии (- 6,4 п.п.).

Среди стран и территорий мира лидирует Тайвань. Мы уже писали выше, что в первом полугодии 2022 года на Тайване неожиданно на 8 п.п. вырос процент компьютеров АСУ, на которых были заблокированы вредоносные объекты. Очевидно, что основной вклад в рост показателя Тайваня внесли угрозы из интернета.

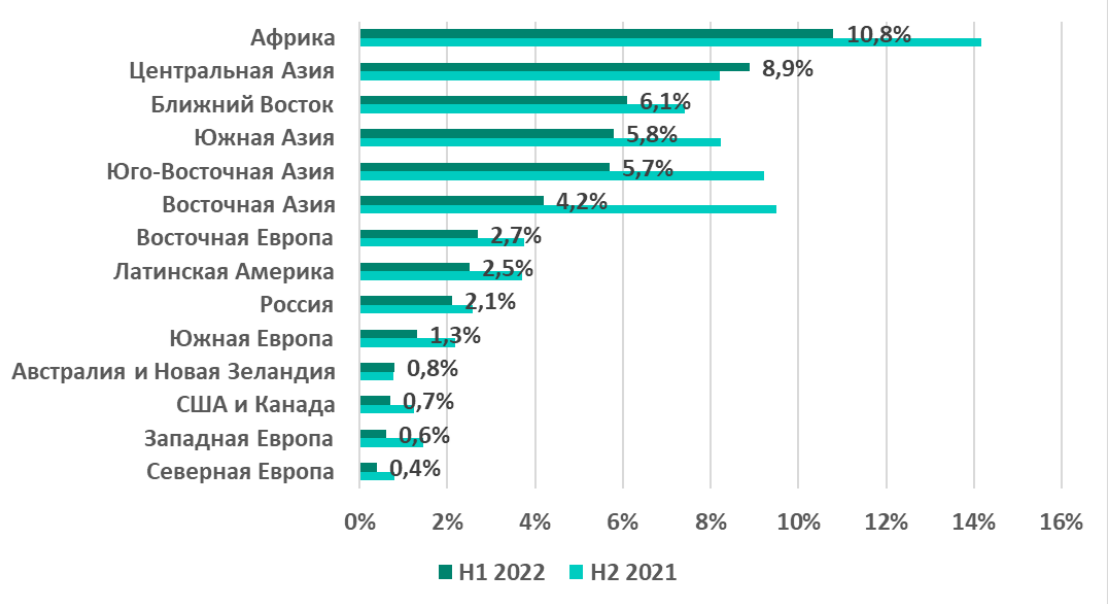
15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы угрозы из интернета, первое полугодие 2022



Съемные носители

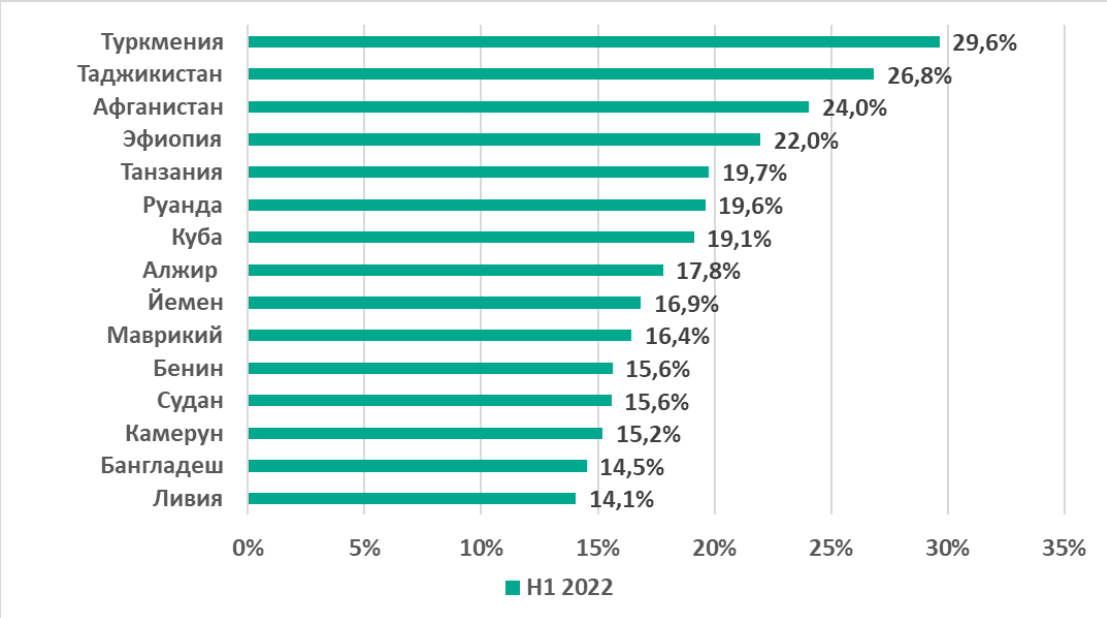
Процент компьютеров АСУ, на которых при подключении съемных носителей было заблокировано вредоносное ПО, уменьшился во всех регионах, кроме Центральной Азии и Австралии и Новой Зеландии.

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



Рейтинг стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, возглавили страны Центральной и Южной Азии.

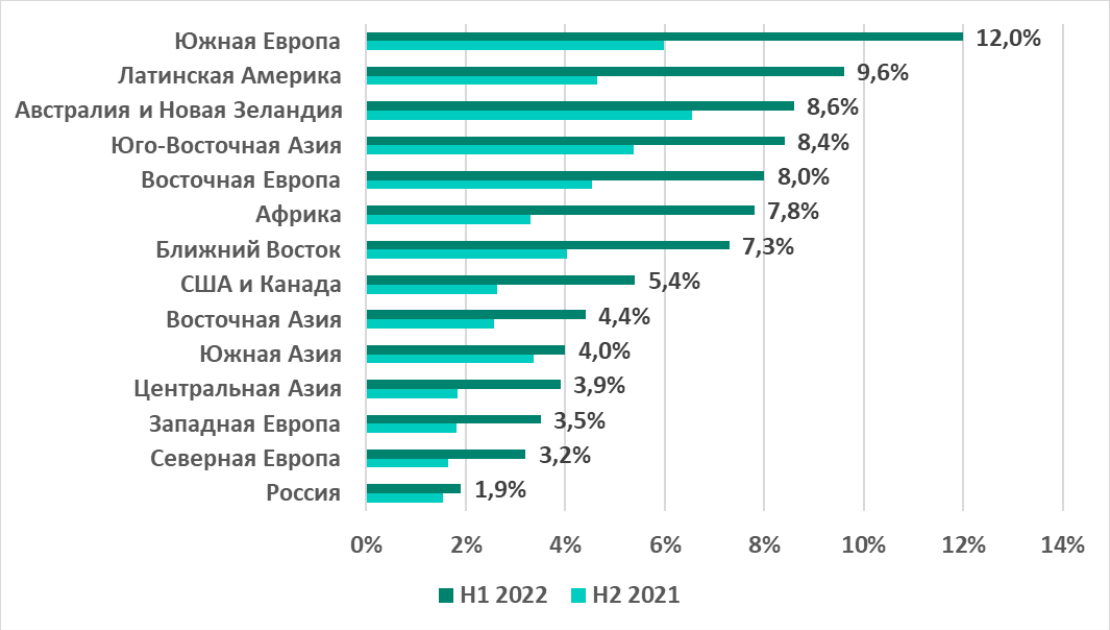
15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, первое полугодие 2022



Почтовые клиенты

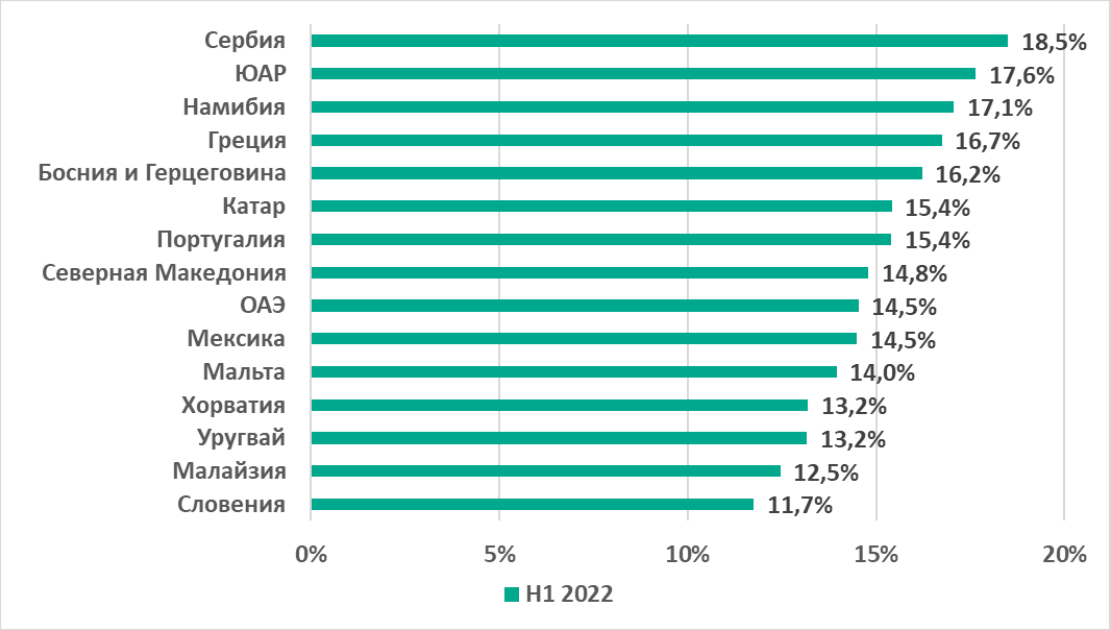
В первой половине 2022 года процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, увеличился во всех регионах. Самый большой рост был отмечен в Южной Европе (+ 6,0 п.п.), которая и возглавила рейтинг регионов по этому показателю.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, первое 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 из разных регионов.

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



Больше всего в этом рейтинге стран из Восточной и Южной Европы.

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 исследуемого периода (на графиках далее 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.

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