Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Австралия и Новая Зеландия

Второй квартал 2025 года

19.09.2025

Версия 1.0

Австралия и Новая Зеландия

Основные проблемы кибербезопасности в регионе

Один из наиболее благополучных с точки зрения кибербезопасности регионов. По доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, во втором квартале 2025 года Австралия и Новая Зеландия занимает 11-е место в рейтинге регионов.

При этом по показателям некоторых источников и категорий угроз регион в соответствующих рейтингах занимает более высокие позиции:

- угрозы из почтовых клиентов — седьмое место;
- вредоносные скрипты и фишинговые страницы — шестое место;
- программы-вымогатели — седьмое место;
- вредоносные документы — восьмое место.

Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для скрытого майнинга криптовалюты, программ-вымогателей). Они распространяются как в интернете, так и в письмах, рассылаемых по электронной почте.

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и используют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

Во втором квартале 2025 года Австралия и Новая Зеландия — один из двух регионов, где доля компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, не уменьшилась.

Также это один из двух регионов, где за квартал вырос показатель шпионских программ. Австралия и Новая Зеландия занимает второе место по росту за квартал доли компьютеров АСУ, на которых блокируются программы-вымогатели. Этот показатель в регионе растет третий квартал подряд.

Относительно высокие показатели угроз, распространяющихся через почтовые клиенты (фишинг), а также вредоносных скриптов могут быть признаками доступности технологических систем в регионе для продвинутых категорий злоумышленников.

Особенности стран

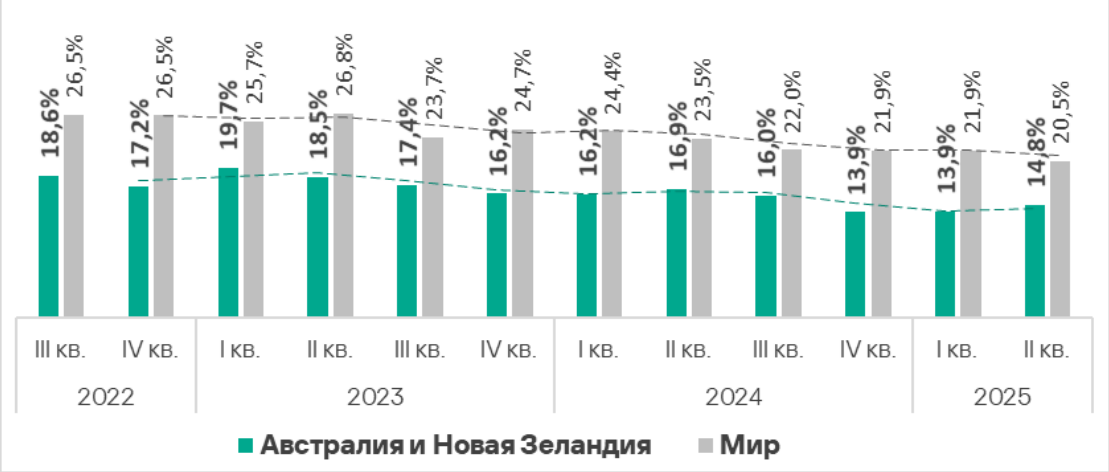
В Новой Зеландии доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, выше, чем в Австралии, в 1,3 раза. Также в Новой Зеландии выше показатели категорий угроз, которые распространяются в интернете.

В Австралии доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, превышает соответствующий показатель Новой Зеландии в 3,1 раза. Также выше в Австралии показатели категорий угроз, которые распространяются преимущественно через почту.

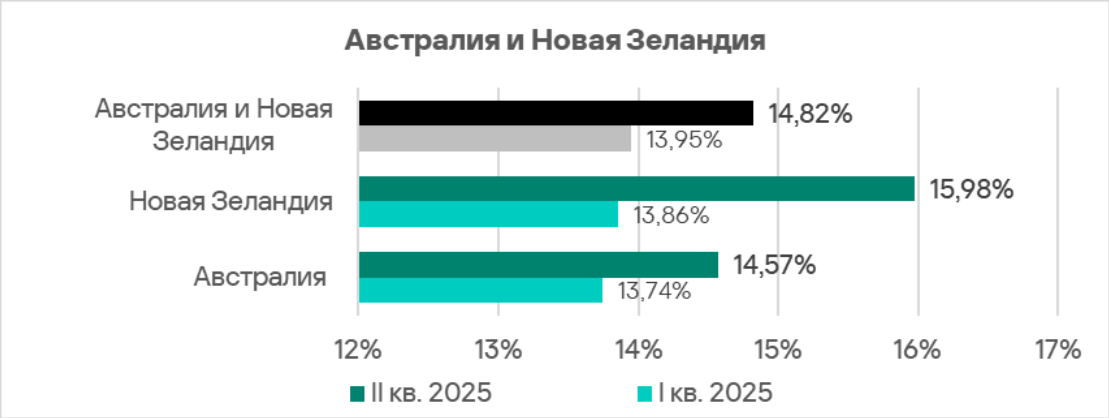
Статистика по всем угрозам

Австралия и Новая Зеландия занимают 11-е место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Значение показателя — 14,8% — существенно ниже среднемирового, но в 1,3 раза выше, чем в Северной Европе, которая замыкает этот рейтинг.

Австралия и Новая Зеландия — один из двух регионов, где доля компьютеров АСУ, на которых блокировались вредоносные объекты, во втором квартале 2025 года выросла. По росту показателя регион лидирует.



Показатель региона в целом во многом зависит от ситуации в Австралии. Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в этой стране меньше, чем в Новой Зеландии.

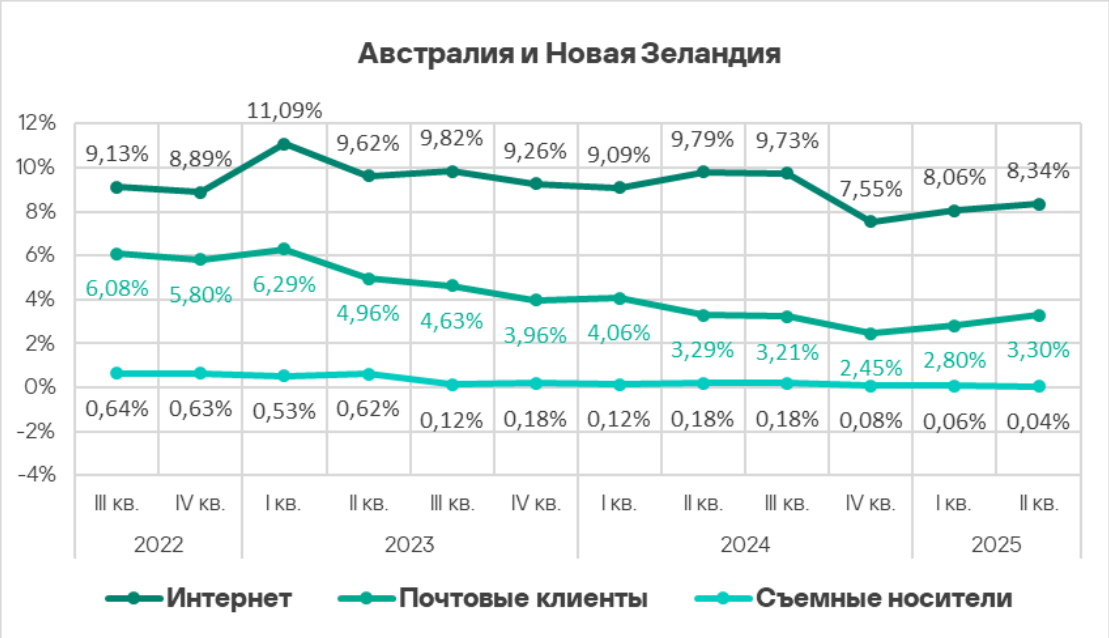


Источники угроз

Показатели всех источников угроз, кроме почтовых клиентов, в Австралии и Новой Зеландии ниже среднемировых. Доля компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах, в регионе в 1,1 раза выше среднемирового показателя.

Вредоносные объекты в регионе распространяются преимущественно через интернет и почту. В рейтинге по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, Австралия и Новая Зеландия занимают предпоследнее место.

Во втором квартале 2025 года из всех источников угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась у интернета и почтовых клиентов. По росту показателя угроз из интернета Австралия и Новая Зеландия находятся на втором месте среди регионов.

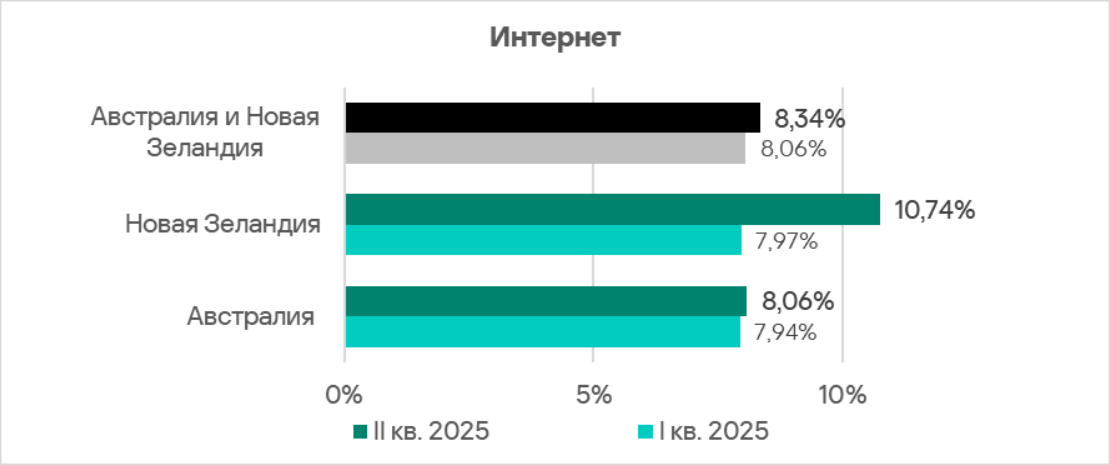


Интернет

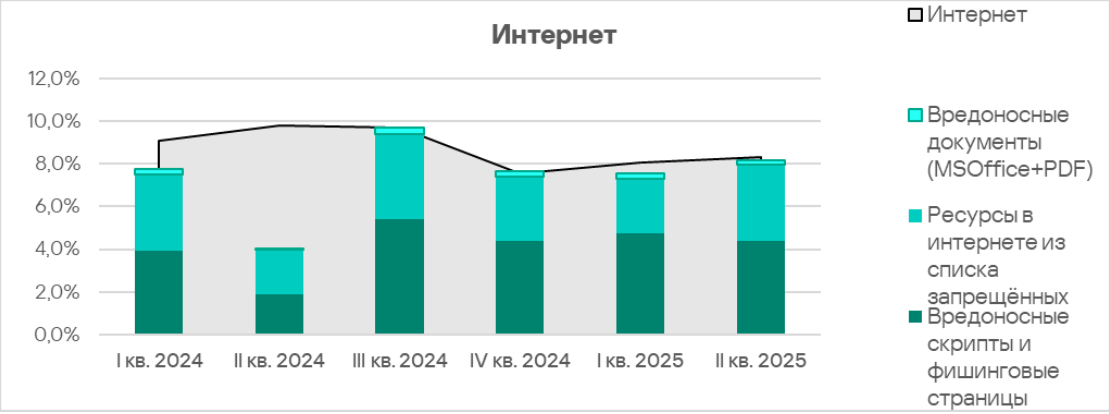
По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, регион Австралия и Новая Зеландия занимает 10-е место с показателем 8,34%. Это выше минимального показателя регионов — у Восточной Азии — в 1,3 раза.

После падения в конце 2024 года показатель в Австралии и Новой Зеландии растет второй квартал подряд, однако пока он меньше тех значений, которые были у него до снижения.

Доля компьютеров АСУ, на которых блокируются угрозы из интернета, в Новой Зеландии выше, чем в Австралии, в 1,3 раза.



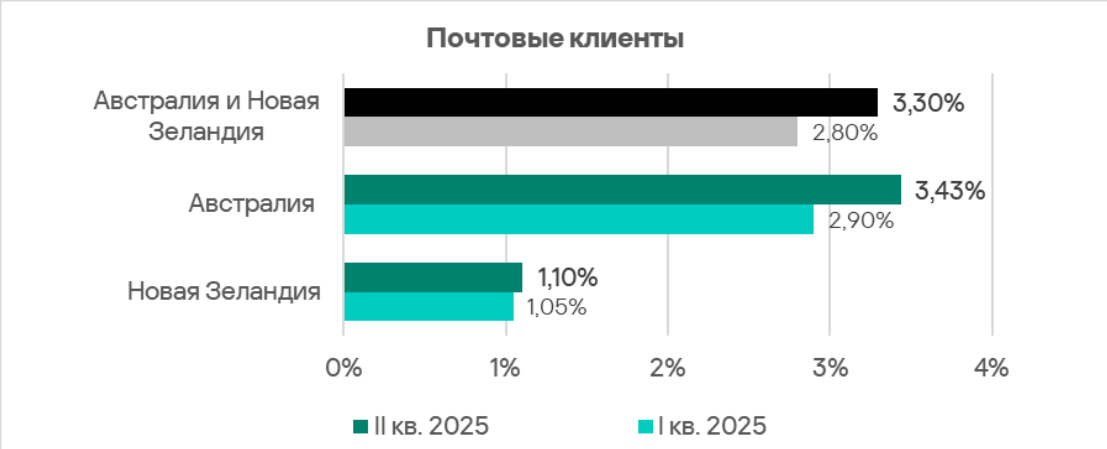
Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных.



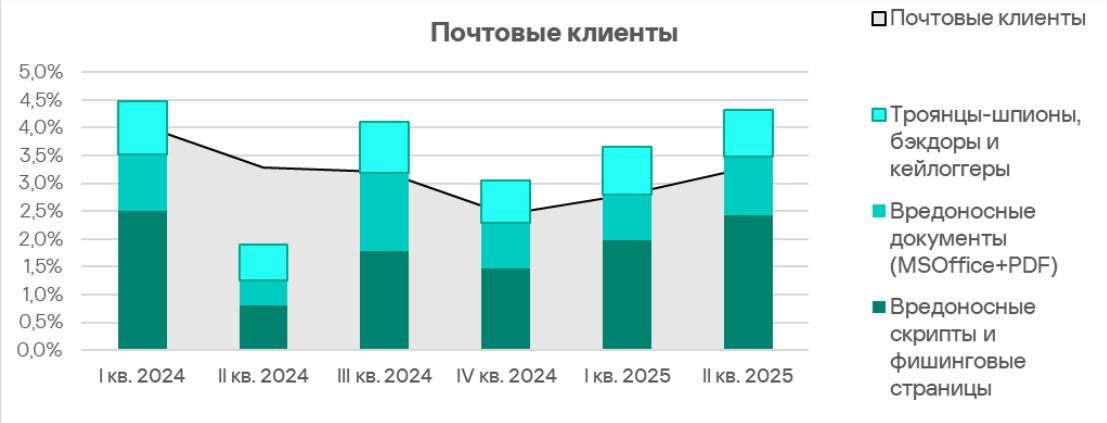
Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, во втором квартале 2025 года Австралия и Новая Зеландия занимают седьмое место с показателем 3,30%. Это в 4,1 раза больше, чем в России, которая замыкает соответствующий рейтинг.

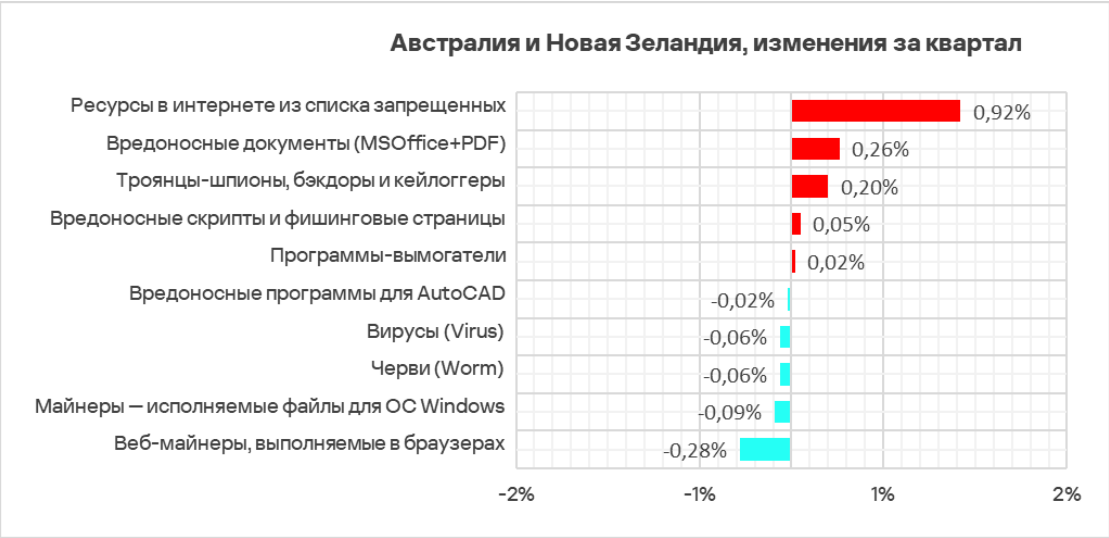
Показатель в Австралии в 3,1 раза больше, чем в Новой Зеландии.



Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ: вредоносные скрипты и фишинговые страницы, вредоносные документы и шпионское ПО.



Категории угроз



В регионе Австралия и Новая Зеландия среди категорий угроз показатель выше среднемирового, только у доли компьютеров АСУ, на которых блокировались вредоносные скрипты и фишинговые страницы, — в 1,1 раза.

Рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

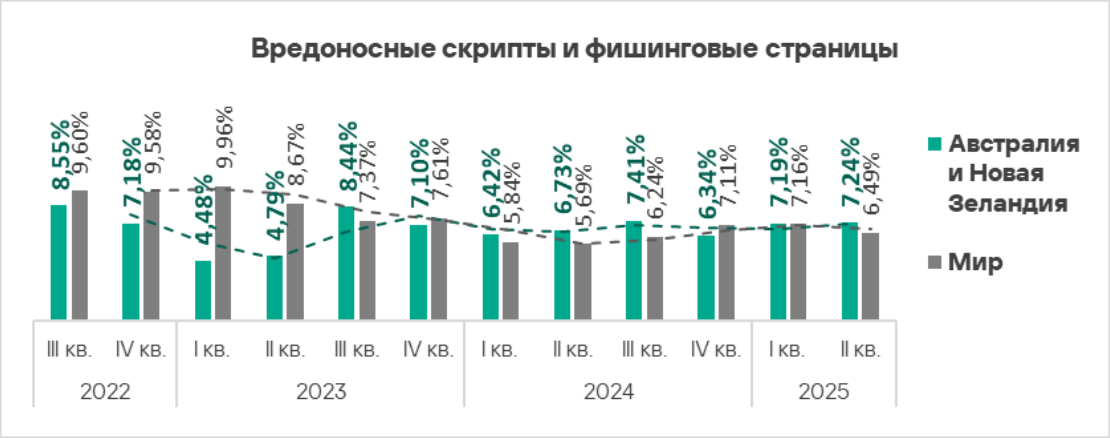
- вредоносные скрипты и фишинговые страницы;
- ресурсы в интернете из списка запрещенных — в 1,3 раза;

- вредоносные документы — 1,2 раза;
- шпионские программы — в 1,1 раза;
- программы-вымогатели — в 1,2 раза.

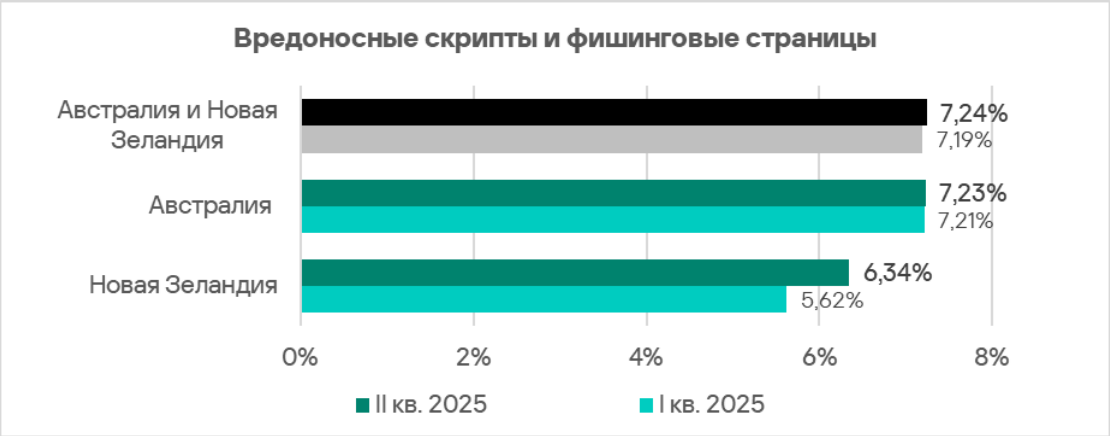
Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Австралия и Новая Зеландия занимают шестое место с 7,24%. Этот показатель в 2,4 раза выше, чем в Северной Европе, где он наименьший из всех регионов.

Во втором квартале 2025 года доля компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, уменьшилась во всех регионах, кроме Австралии и Новой Зеландии, а также Северной Америки (Канады).



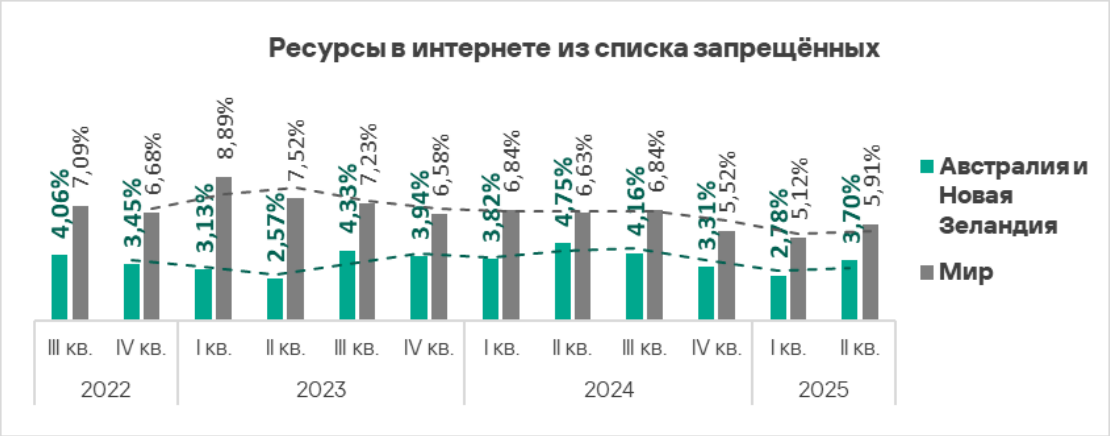
В Австралии за квартал показатель почти не изменился, в Новой Зеландии он вырос, но не достиг значения в Австралии.



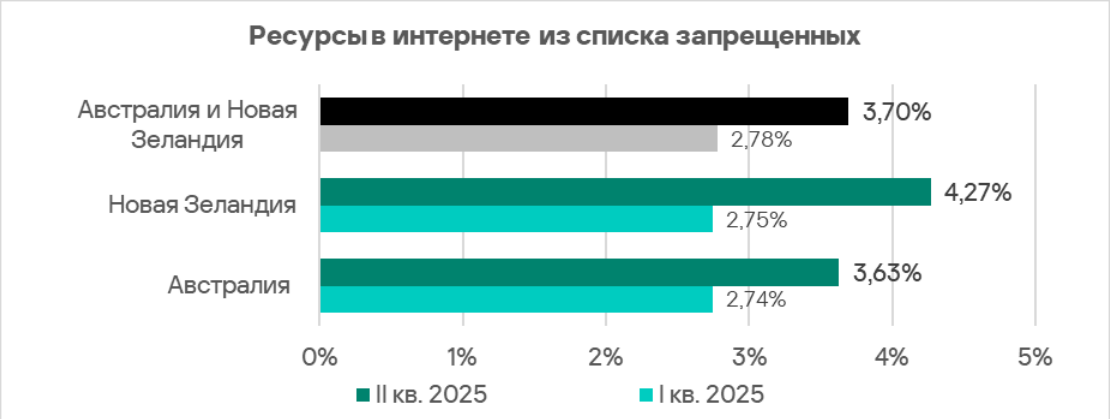
Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и по электронной почте.

Ресурсы в интернете из списка запрещенных

По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Австралия и Новая Зеландия занимают предпоследнее место с 3,70%. Однако по росту этого показателя регион находится на шестом месте — за квартал значение выросло в 1,3 раза.



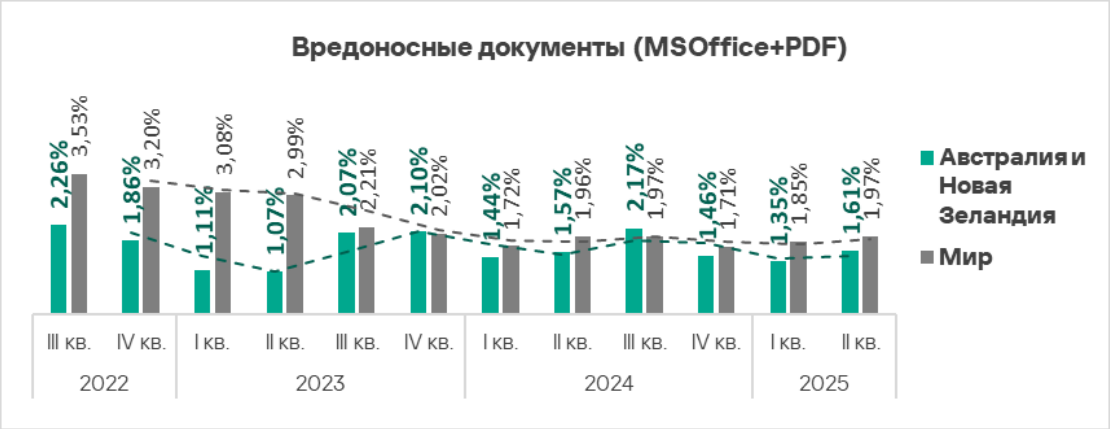
Доля компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в Новой Зеландии выше, чем в Австралии, в 1,2 раза. Рост показателя отмечен в обеих странах региона.



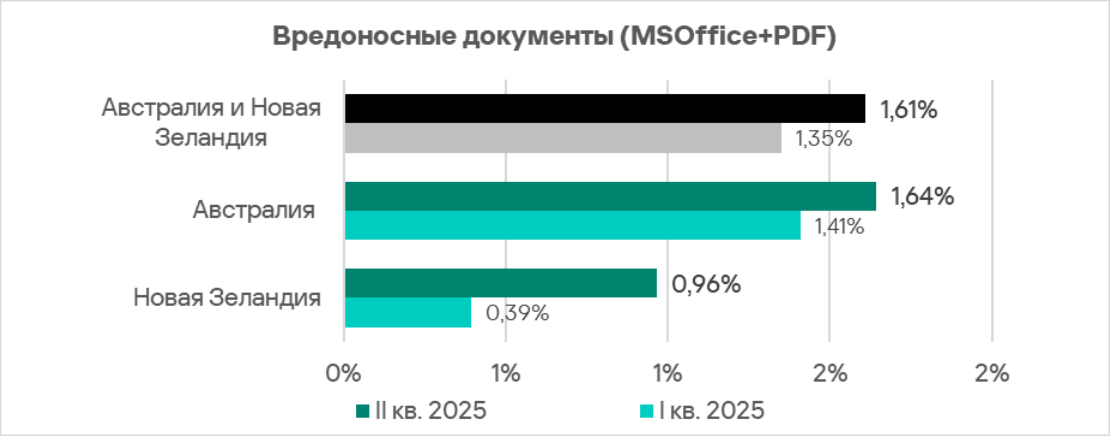
Вредоносные документы

Австралия и Новая Зеландия занимают восьмое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные документы. Показатель в регионе — 1,61% — в 2,5 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, в регионе колеблется.



Показатель в Австралии выше, чем в Новой Зеландии, в 1,7 раза.

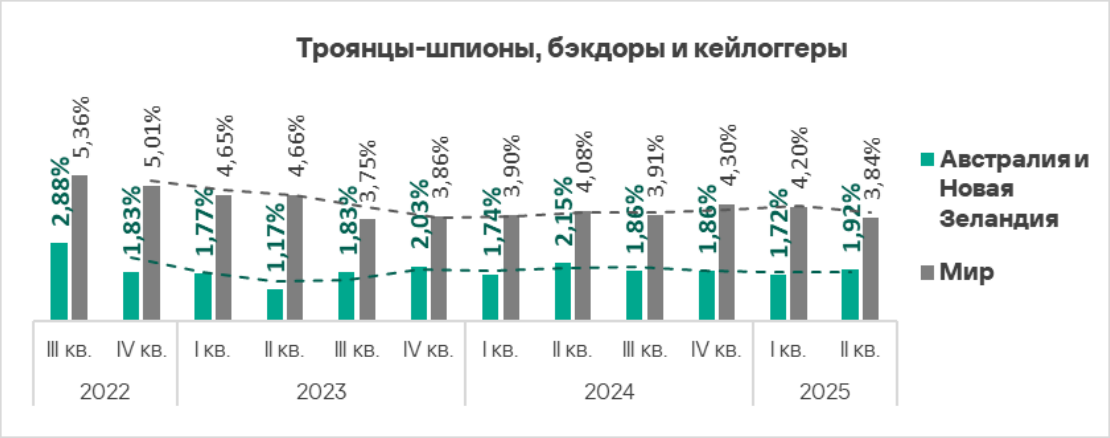


Распространяются вредоносные документы преимущественно по электронной почте.

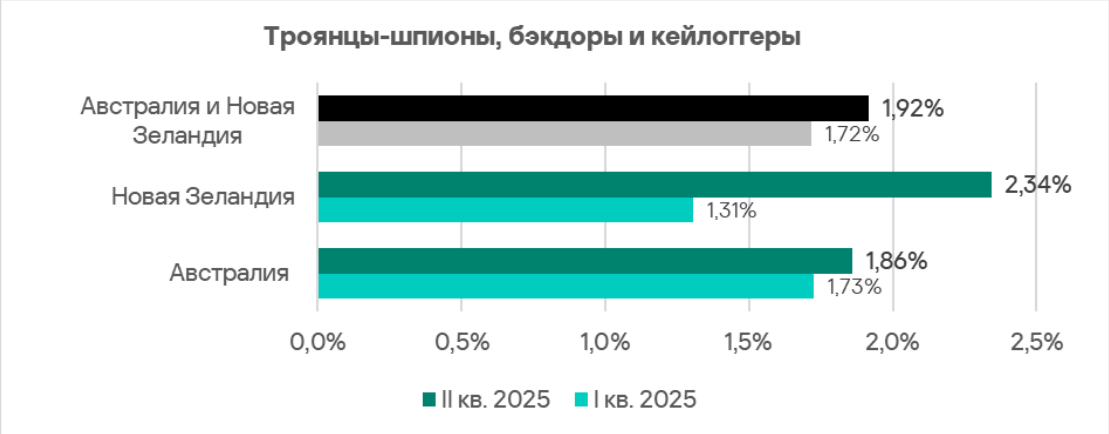
Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, в соответствующем рейтинге регионов Австралия и Новая Зеландия находятся на 11-м месте с 1,92%. Это в 1,4 раза больше, чем в Западной Европе, где значение наименьшее.

Доля компьютеров АСУ, на которых блокируются шпионские программы, в регионе колеблется. Австралия и Новая Зеландия — один из двух регионов, где этот показатель во втором квартале 2025 года вырос.



Доля компьютеров АСУ, на которых блокируются шпионские программы, в Новой Зеландии в 1,3 раза выше, чем в Австралии.

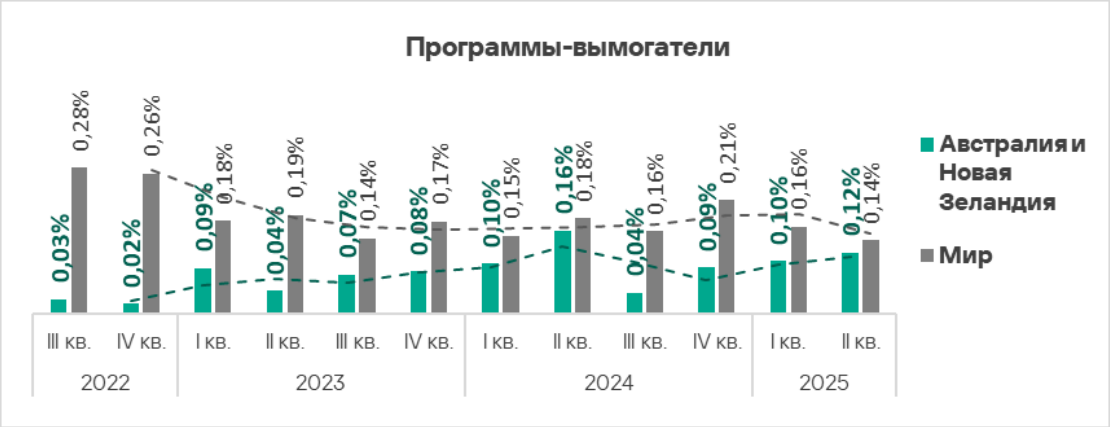


Шпионские программы в регионе блокируются во всех источниках угроз, преимущественно в почтовых клиентах.

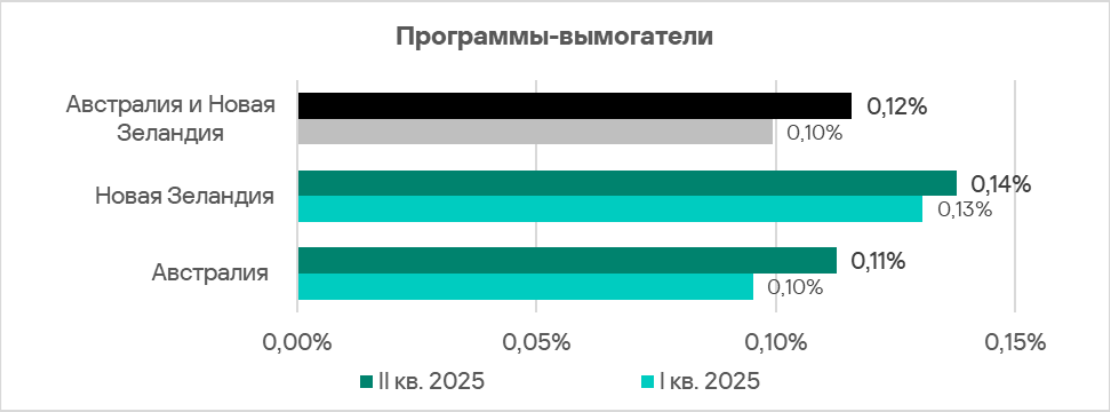
Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Австралия и Новая Зеландия занимают седьмое место с показателем 0,12%. Это в 1,8 раза больше, чем в Западной Европе, которая замыкает соответствующий рейтинг.

Показатель в регионе растет третий квартал подряд, и по его росту во втором квартале 2025 года Австралия и Новая Зеландия занимают второе место в мире.

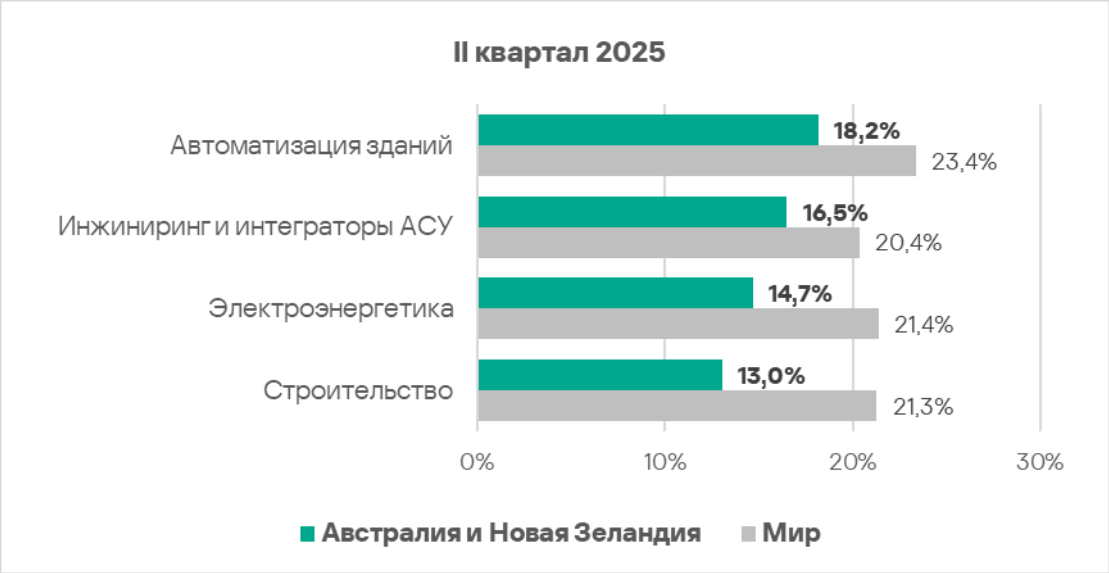


Доля компьютеров АСУ, на которых блокируются программы-вымогатели, в Новой Зеландии в 1,2 раза выше, чем в Австралии. Показатель за квартал подрос в обеих странах.



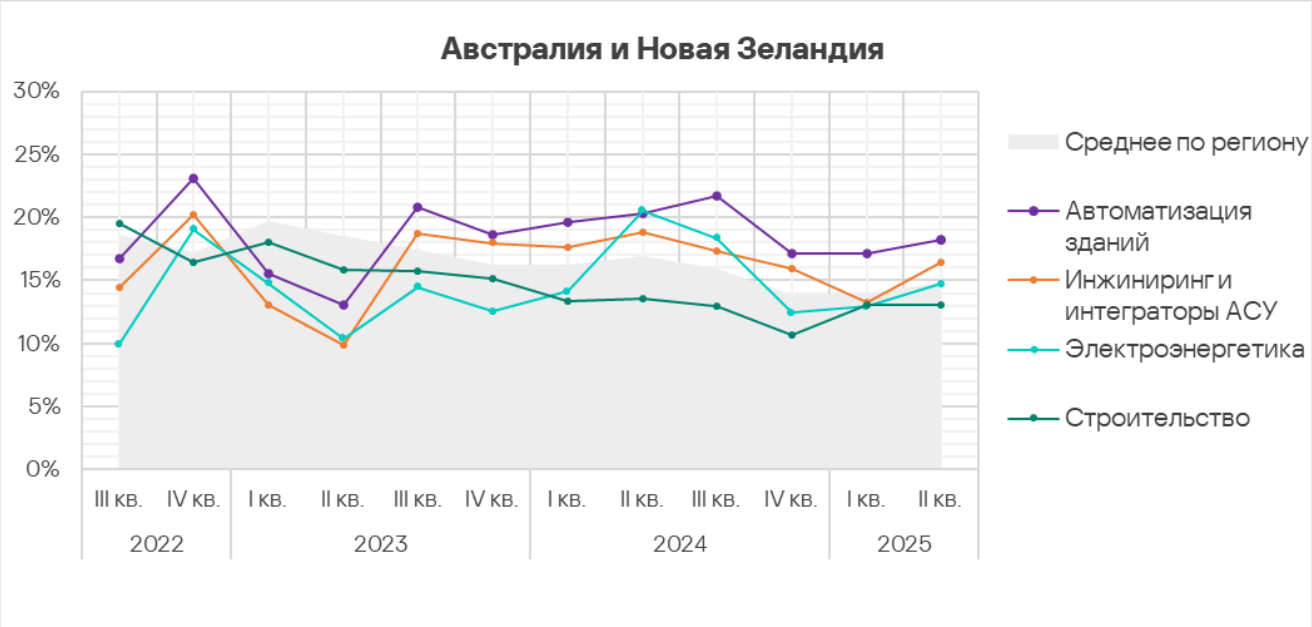
Отрасли

Среди рассмотренных в отчете отраслей чаще всего встречается с угрозами автоматизация зданий.



Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась во всех рассматриваемых отраслях, кроме отрасли строительство.

Показатели отраслей автоматизация зданий и инжиниринг и интеграторы АСУ превышают среднее для региона значение.



Источники и категории вредоносного ПО в отраслях: «горячие точки»

При оценке проблем отраслей мы используем тепловые карты. На таких картах ячейки окрашиваются в цвета в диапазоне от красного к зеленому,

где красный цвет указывает на максимальное значение индустрии в регионе, источника или категории угроз среди всех регионов и индустрий. В Австралии и Новой Зеландии значения, близкие к максимальным, наблюдаются для интернет-угроз в секторе инжиниринга и интеграции АСУ.

Показатели источников угроз в отраслях в Австралии и Новой Зеландии, II квартал 2025 года

Отрасль / Источник угрозы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Показатель категорий в регионе
Интернет	8,37%	8,30%	9,90%	7,15%	8,34%
Почтовые клиенты	6,76%	1,89%	2,32%	3,36%	3,30%
Съемные носители	0,00%	0,00%	0,12%	0,04%	0,04%
Сетевые папки	0,00%	0,00%	0,00%	0,00%	0,01%
Показатель отрасли в регионе	18,20%	14,72%	16,48%	13,03%	

Показатели категорий угроз в отраслях в Австралии и Новой Зеландии, II квартал 2025 года

Отрасль / Категории вредоносного ПО	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	3,89%	4,91%	4,49%	2,81%	3,70%
Вредоносные скрипты и фишинговые страницы	9,78%	5,28%	7,16%	6,81%	7,24%
Троянцы-шпионы, бэкдоры и кейлоггеры	3,45%	1,89%	1,86%	1,53%	1,92%
Черви (Worm)	0,29%	0,75%	0,27%	0,17%	0,22%
Майнеры — исполняемые файлы для ОС Windows	0,39%	0,00%	0,19%	0,21%	0,21%
Вредоносные документы (MSOffice+PDF)	3,21%	1,13%	1,04%	1,23%	1,61%
Вирусы (Virus)	0,10%	0,00%	0,08%	0,21%	0,13%
Программы-вымогатели	0,34%	0,38%	0,04%	0,09%	0,12%
Веб-майнеры, выполняемые в браузерах	0,29%	0,00%	0,15%	0,30%	0,20%
Вредоносные программы для AutoCAD	0,00%	0,00%	0,04%	0,17%	0,04%
Показатель отрасли в регионе	18,2%	14,72%	16,48%	13,03%	

«Горячие точки» отраслей

Автоматизация зданий

- Первое место среди отраслей в регионе по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах. Второе место в регионе по показателю угроз из интернета.
- Первое место среди отраслей по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, майнеры — исполняемые файлы для ОС Windows.
- Второе место среди отраслей в регионе по показателям следующих категорий угроз: черви, вирусы, веб-майнеры, программы-вымогатели.
- Восьмое месте среди отраслей во всех регионах по показателю угроз в категории вредоносные скрипты и фишинговые страницы.

Инжиниринг и интеграторы АСУ

- Первое место в регионе среди отраслей по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета.
- Второе место в регионе среди отраслей по показателю следующих категорий угроз: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, вредоносные программы для AutoCAD.

Электроэнергетика

- Первое место среди отраслей региона по показателю следующих категорий угроз: ресурсы в интернете из списка запрещенных, черви, программы-вымогатели.
- Второе место среди отраслей региона по показателю шпионского ПО.

Строительство

- Второе место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах.
- Первое место среди отраслей региона по показателям следующих категорий угроз: веб-майнеры, вирусы и вредоносные программы для AutoCAD.
- Второе место среди отраслей региона по показателям следующих категорий: вредоносные документы, майнеры — исполняемые файлы для ОС Windows.

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 дает нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счет обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за ее объема и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные не только в значительной мере 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 автоматизации зданий;
- 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 и сетей автоматизации зданий;
- компьютеры программистов АСУ/ПЛК.

Компьютеры, передающие нам статистику, принадлежат организациям из разных отраслей. Наиболее широко представлены химическая промышленность, металлургия, инжиниринг и интеграторы АСУ,

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

нефтегазовая отрасль, энергетика, транспорт и логистика, пищевая промышленность, легкая промышленность и фармацевтическая отрасль. Сюда же входят системы инжиниринговых компаний и интеграторов АСУ, работающих с предприятиями в самых разных отраслях, а также системы управления зданиями, физической безопасности и обработки биометрических данных.

Атакованными мы считаем те компьютеры, на которых в течение исследуемого периода (на графиках выше это месяц, полугодие, год — в зависимости от контекста) защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете доли 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», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com