Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Австралия и Новая Зеландия

Третий квартал 2025 года

23.12.2025

Версия 1.0

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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, в третьем 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 высокую позицию:

- вредоносные скрипты и фишинговые страницы — седьмое место;
- вредоносные документы — седьмое место;
- угрозы из почтовых клиентов — седьмое место;
- угрозы в сетевых папках — седьмое 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.

В третьем квартале 2025 года Австралия и Новая Зеландия находится на первом месте по росту показателя угроз из почтовых клиентов. Это один из четырех регионов, где увеличилась доля компьютеров АСУ, на которых блокируются вредоносные документы.

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.

В третьем квартале 2025 года в регионе Австралия и Новая Зеландия вырос показатель угроз из сетевых папок, по его росту Австралия и Новая Зеландия находятся на втором месте среди тех четырех регионов, где он увеличился. Увеличилась также доля компьютеров АСУ, на которых угрозы блокировались на съемных носителях.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Особенности стран

В Австралии доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, превышает соответствующий показатель Новой Зеландии в 2,8 раза.

Показатели региона по угрозам на съемных носителях и в сетевых папках определяются прежде всего ситуацией в Австралии, в Новой Зеландии показатели по этим источникам угроз незначительные.

Доля компьютеров АСУ, на которых блокируются вирусы, в третьем квартале 2025 года увеличилась в обеих странах региона, в Новой Зеландии — в 3,0 раза.

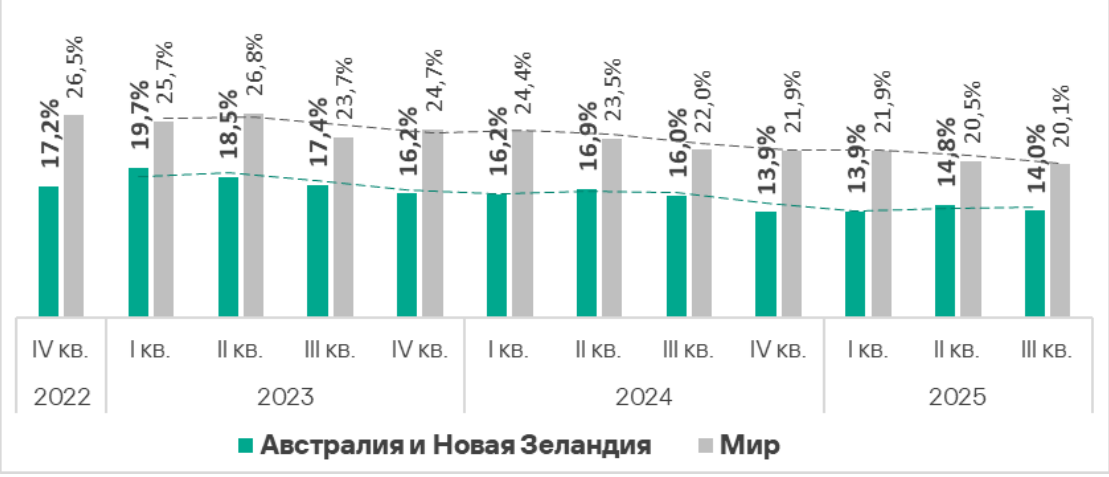
Отрасли

В рейтингах регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в различных отраслях, Австралия и Новая Зеландия не поднимается выше 11-го места.

Однако в двух отраслях регион вошел в тройку лидеров по показателям угроз из почтовых клиентов (в отрасли строительство) и категорий угроз, которые распространяются преимущественно через почту, — вредоносные документы и вредоносные скрипты и фишинговые страницы (в электроэнергетике).

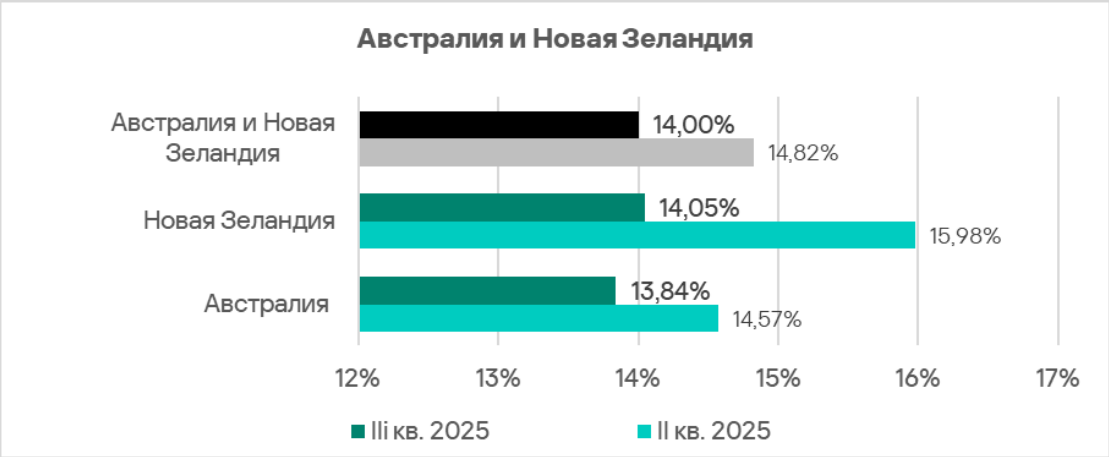
Статистика по всем угрозам

Регион Австралия и Новая Зеландия занимает 11-е место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Значение показателя (14,0%) — существенно ниже среднемирового, но в 1,5 раза выше, чем в Северной Европе, которая замыкает этот рейтинг.



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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. В обеих странах показатель заметно уменьшился.



Источники угроз

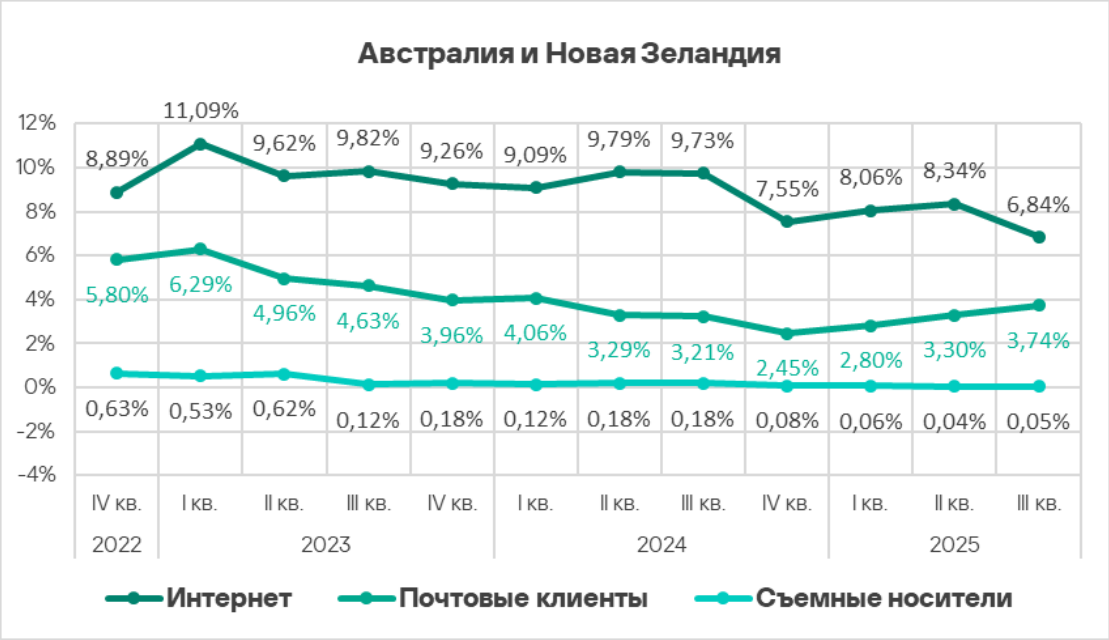
Показатели всех источников угроз, кроме почтовых клиентов, в Австралии и Новой Зеландии ниже среднемировых. Доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, в регионе в 1,2 раза выше среднемирового показателя.

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

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионе увеличилась у всех

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

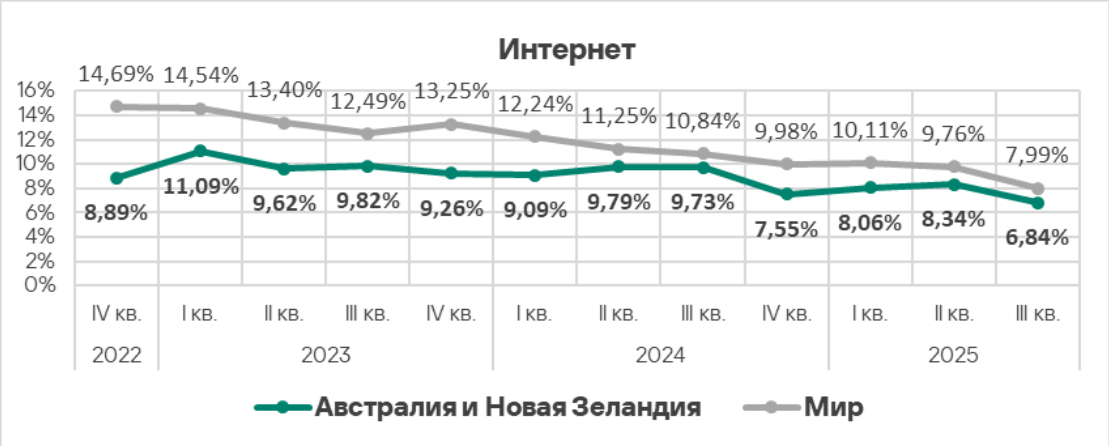
источников угроз, кроме интернета. По росту показателя угроз из почтовых клиентов регион Австралия и Новая Зеландия лидирует, а по росту показателя угроз из сетевых папок находится на втором месте.



Интернет

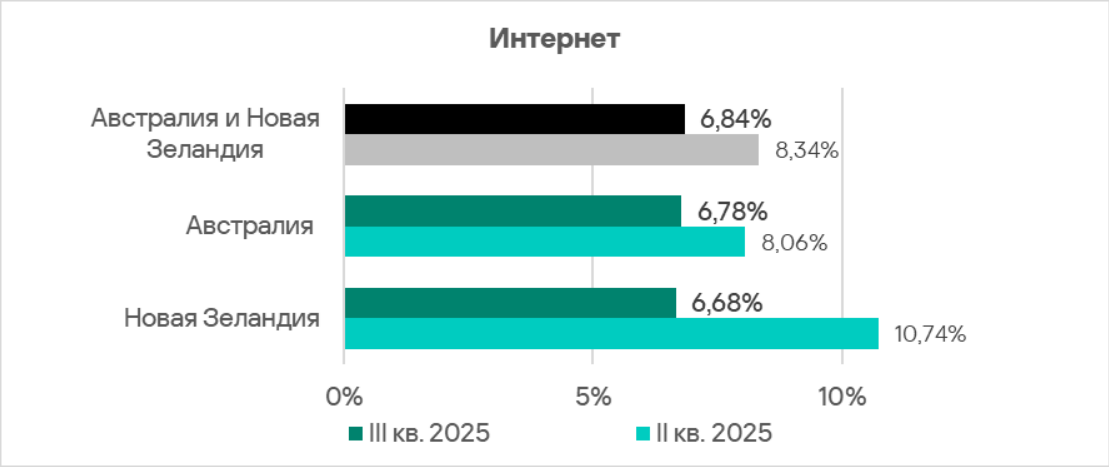
По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, регион Австралия и Новая Зеландия занимает девятое место с 6,84%. Это в 1,5 раза больше показателя в Северной Европе, которая замыкает соответствующий рейтинг.

В Австралии и Новой Зеландии, как и в остальных регионах, показатель за квартал уменьшился.

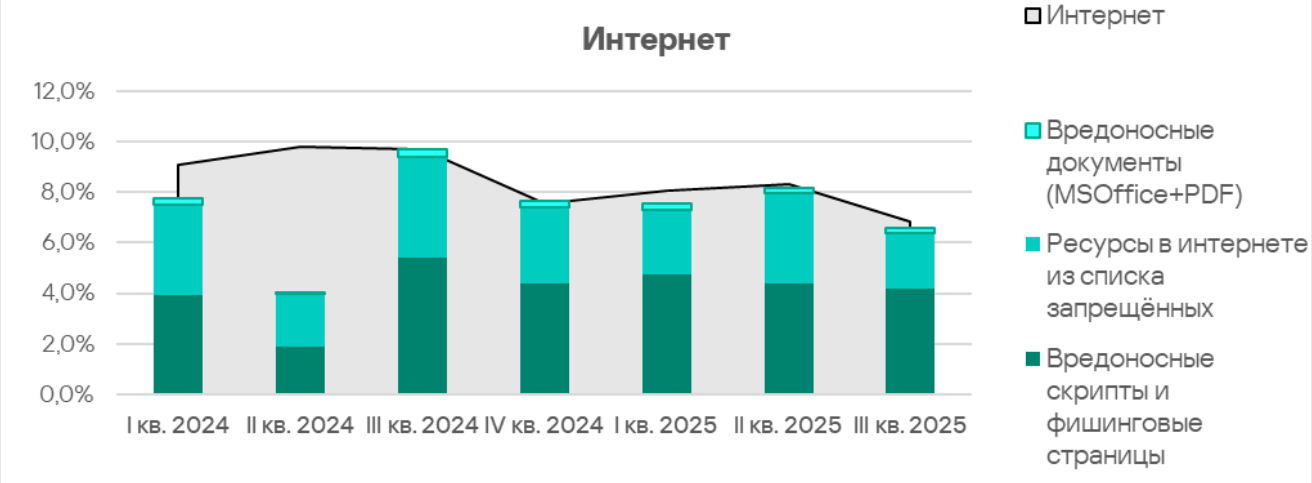


© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых блокируются угрозы из интернета, за квартал уменьшилась в обеих странах региона. В Австралии показатель выше, чем в Новой Зеландии.



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



Почтовые клиенты

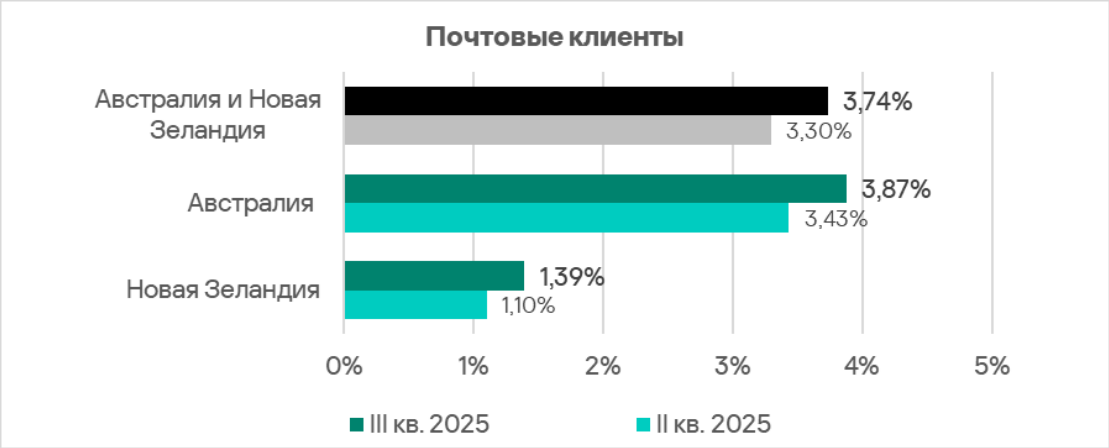
По доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, в третьем квартале 2025 года регион Австралия и Новая Зеландия занимает седьмое место. Это самая высокая позиция региона в рейтингах и по источникам, и по категориям угроз.

Показатель в Австралии и Новой Зеландии (3,74%) — в 4,8 раза больше, чем в России, которая замыкает соответствующий рейтинг.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

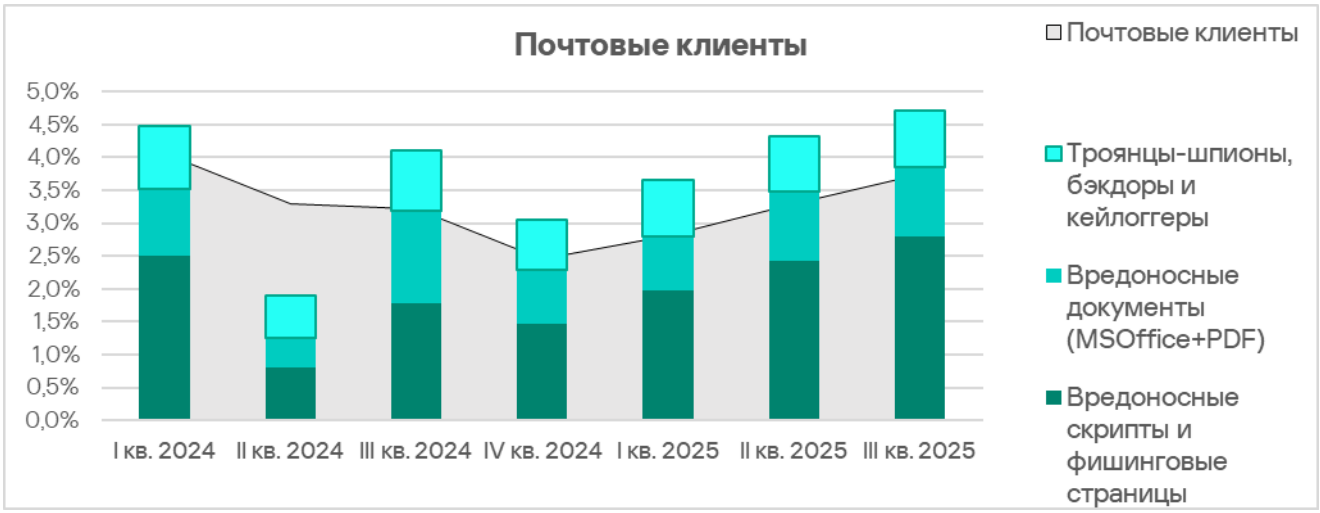
Показатель почтовых клиентов в регионе растет третий квартал подряд. В третьем квартале 2025 года по его росту Австралия и Новая Зеландия занимают первое место среди регионов.

Доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, в Австралии в 2,8 раза больше, чем в Новой Зеландии.



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

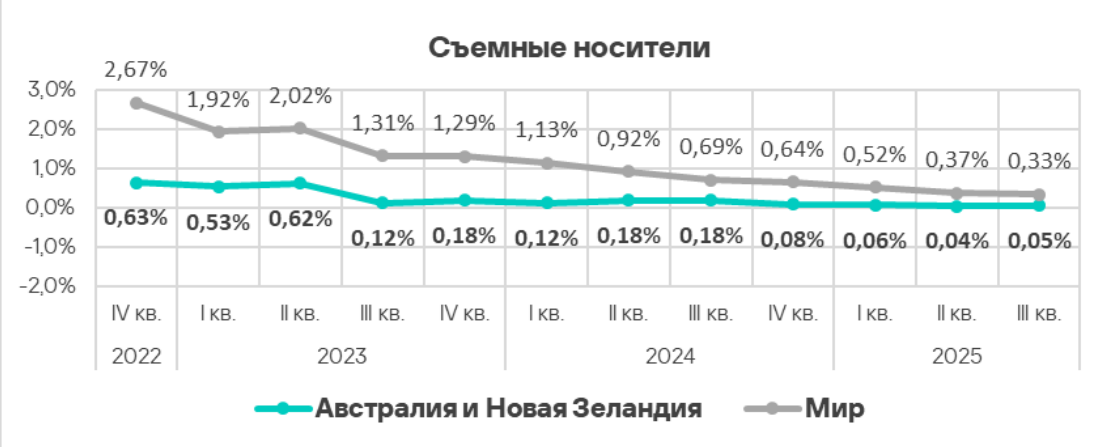
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Съемные носители

По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, в третьем квартале 2025 года регион Австралия и Новая Зеландия занимает 14-е место с наименьшим из всех регионов показателем 0,05%.

Показатель за квартал стабильно уменьшался со второго квартала 2023 года. В третьем квартале 2025 года Австралия и Новая Зеландия стала одним из четырех регионов, где доля компьютеров АСУ, на которых блокируются угрозы на съемных носителях, за квартал подросла.



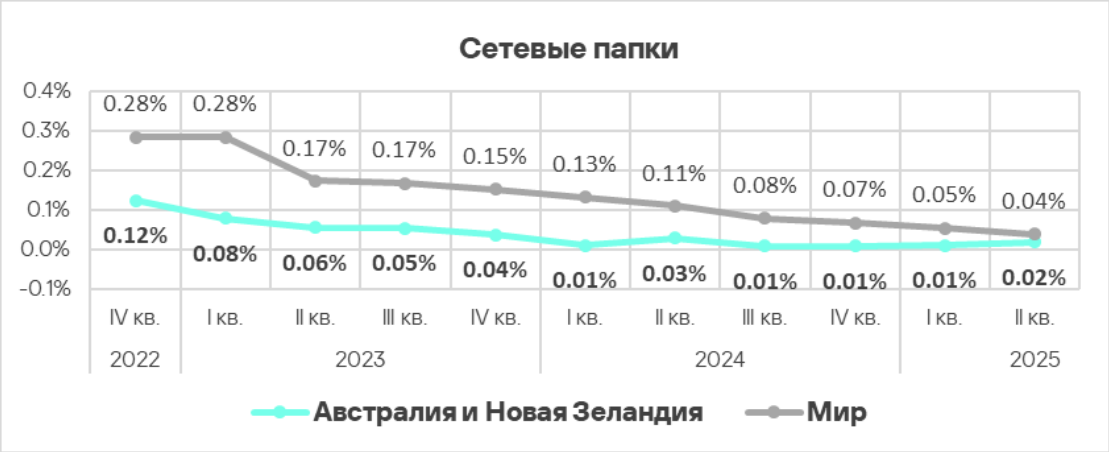
Угрозы на съемных носителях в регионе блокируются преимущественно в Австралии, показатель страны совпадает с показателем региона в целом.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Сетевые папки

По доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, в третьем квартале 2025 года регион Австралия и Новая Зеландия занимает седьмое место с показателем 0,020%. Это самая высокая позиция региона в рейтингах как по источникам, так и по категориям угроз.

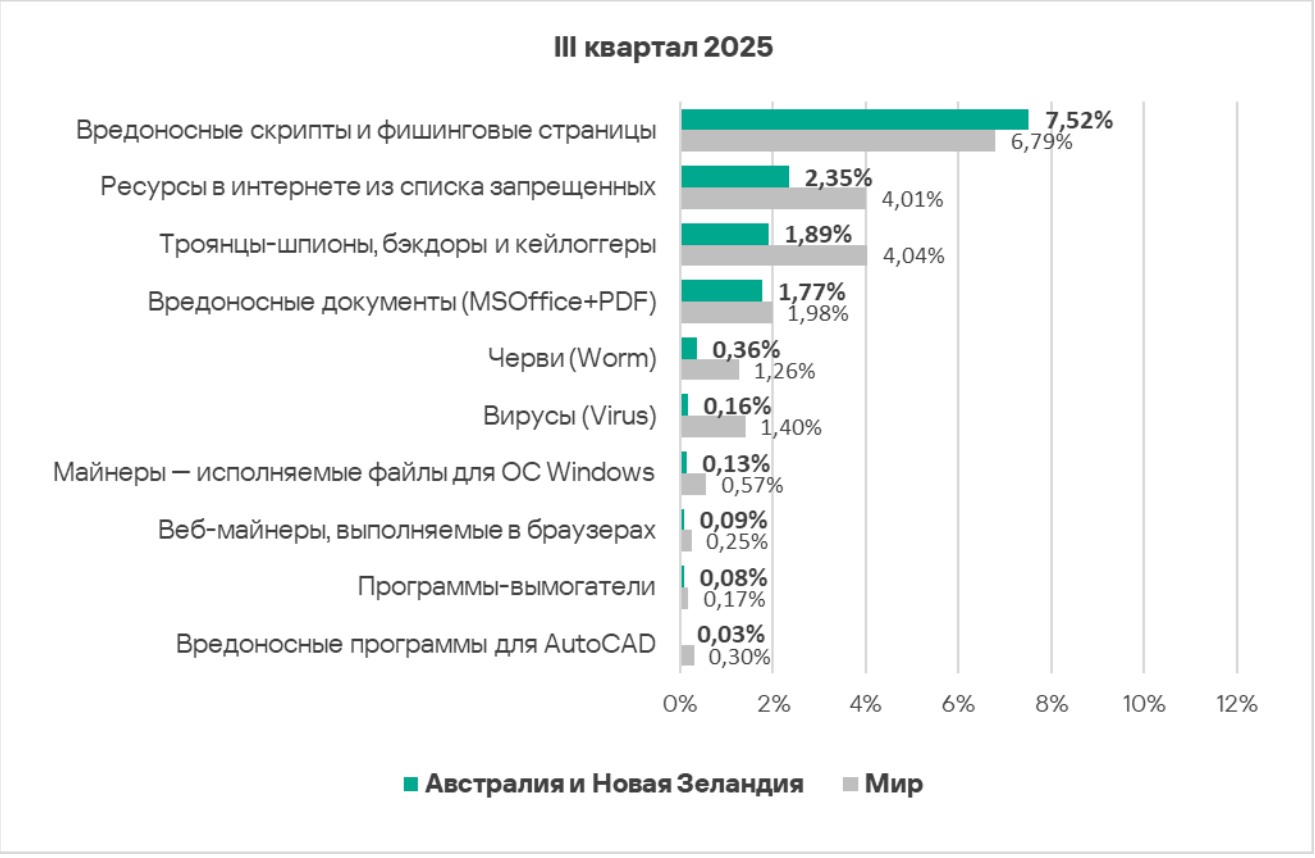
Показатель за квартал в регионе вырос, по его росту Австралия и Новая Зеландия находится на втором месте среди тех четырех регионов, где он увеличился.

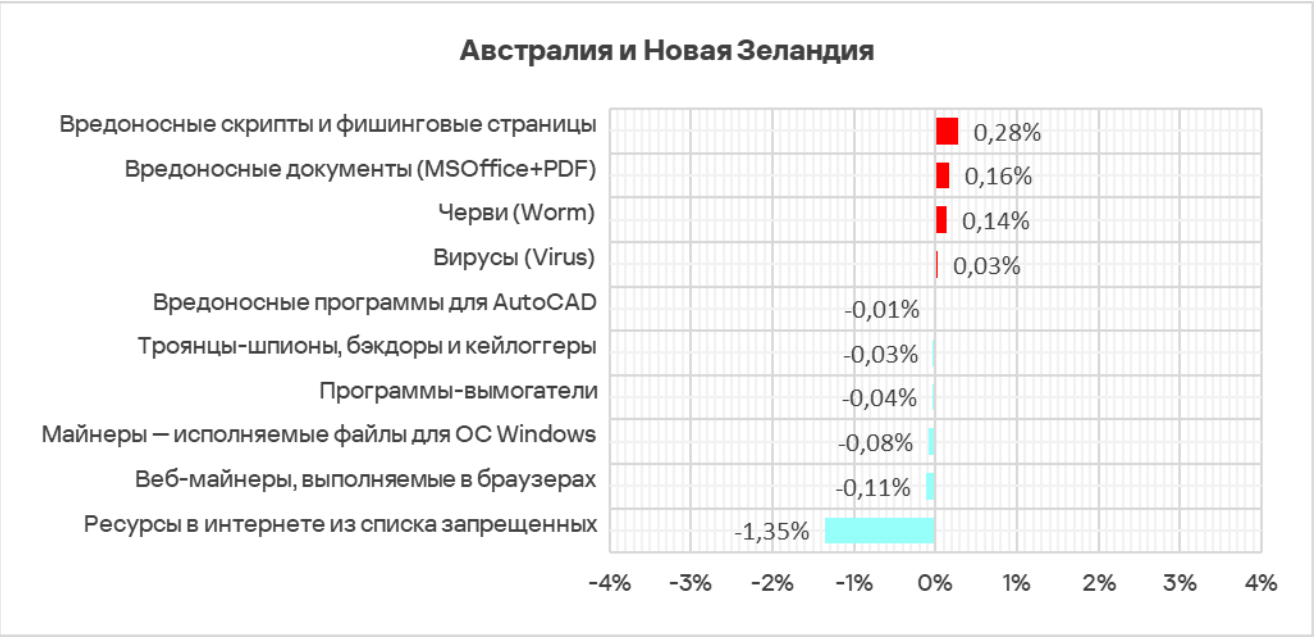


Как и в случае угроз на съемных носителях, угрозы в сетевых папках обнаруживаются преимущественно в Австралии.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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 1,2 раза.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

- вредоносные скрипты и фишинговые страницы;
- вредоносные документы — в 1,1 раза;
- вирусы — в 1,2 раза;
- черви — в 1,6 раза.

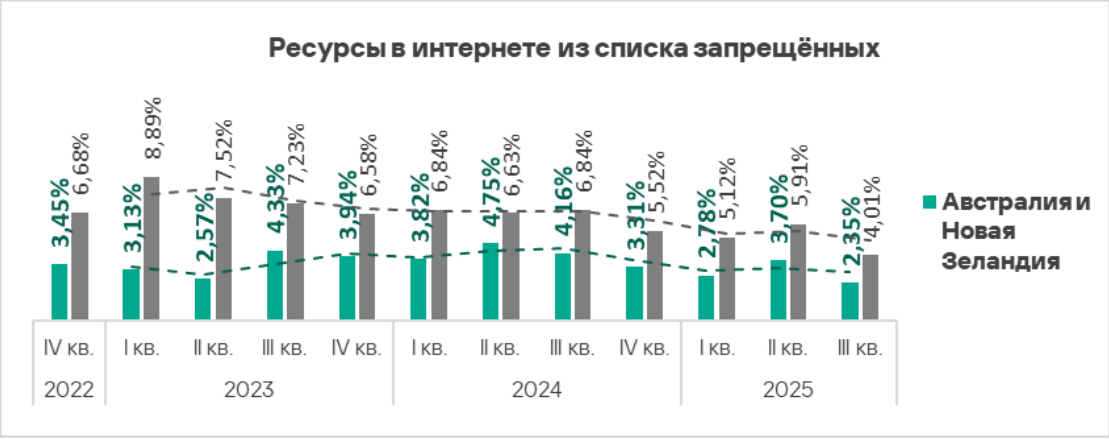
В рейтингах регионов по доле компьютеров АСУ, на которых блокируются вредоносные объекты различных категорий, самые высокие позиции у Австралии и Новой Зеландии по показателям вредоносных документов и вредоносных скриптов — регион находится на седьмом месте в рейтингах по обеим категориям.

Австралия и Новая Зеландия — один из четырех регионов, где категория ресурсы в интернете из списка запрещенных не опустилась ниже второй позиции в рейтинге.

Ресурсы в интернете из списка запрещенных

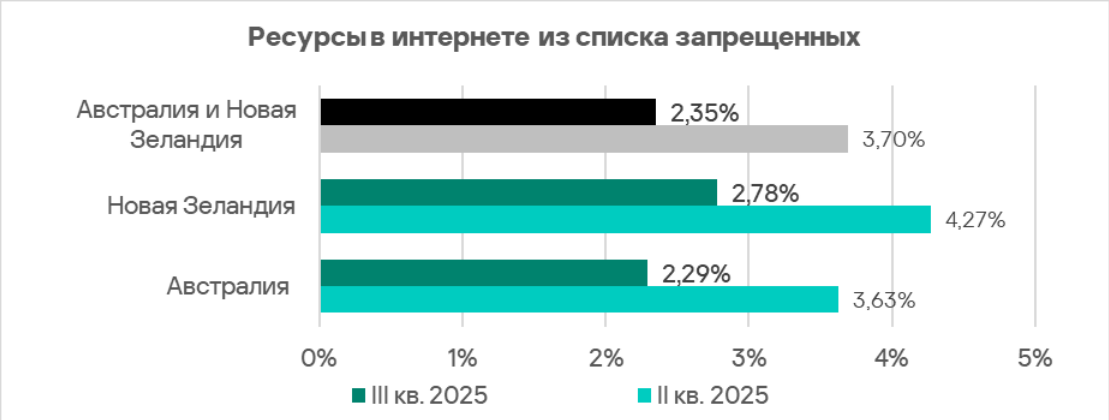
По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, регион Австралия и Новая Зеландия занимает 14-е место с 2,35%.

Как и во всех регионах, в Австралии и Новой Зеландии за квартал показатель уменьшился.



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

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

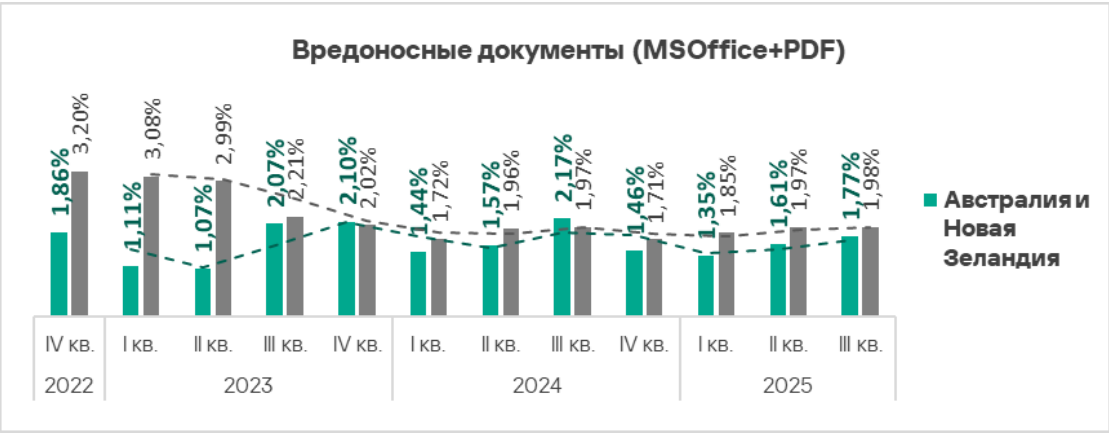


Вредоносные документы

Австралия и Новая Зеландия занимают седьмое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные документы. Это самая высокая позиция региона в рейтингах как по источникам, так и по категориям угроз.

Показатель в регионе (1,77%) — в 3,3 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

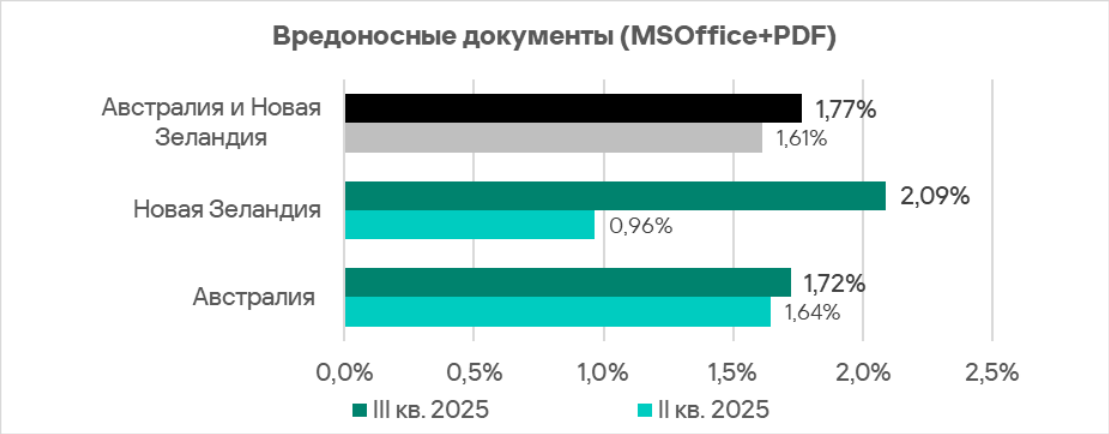
Доля компьютеров АСУ, на которых блокируются вредоносные документы, в регионе колеблется. В третьем квартале 2025 года показатель увеличился. Отметим, что кроме Австралии и Новой Зеландии, он вырос только в трех регионах.



Показатель увеличился в обеих странах региона.

В прошлом квартале доля компьютеров АСУ, на которых блокируются вредоносные документы, в Австралии была выше, чем в Новой Зеландии. В третьем квартале 2025 года Новая Зеландия опередила Австралию.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

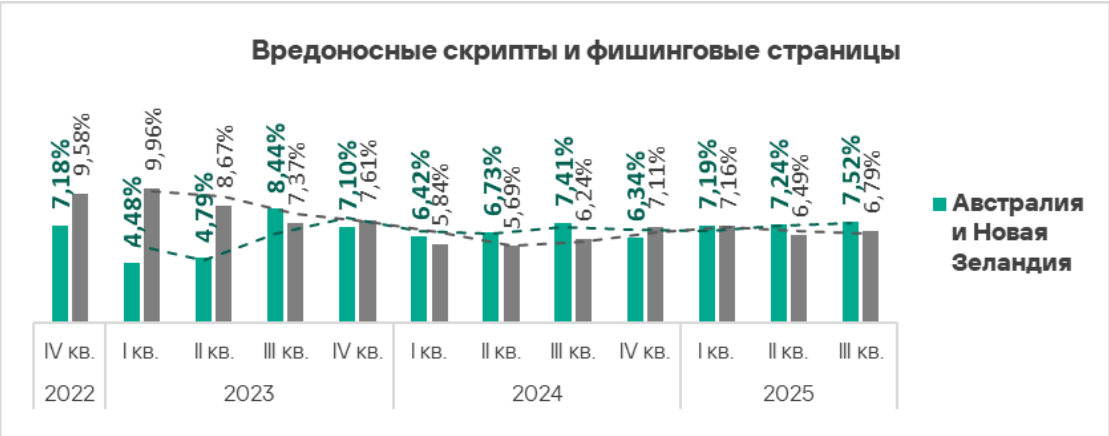


Распространяются вредоносные документы преимущественно по электронной почте.

Вредоносные скрипты и фишинговые страницы

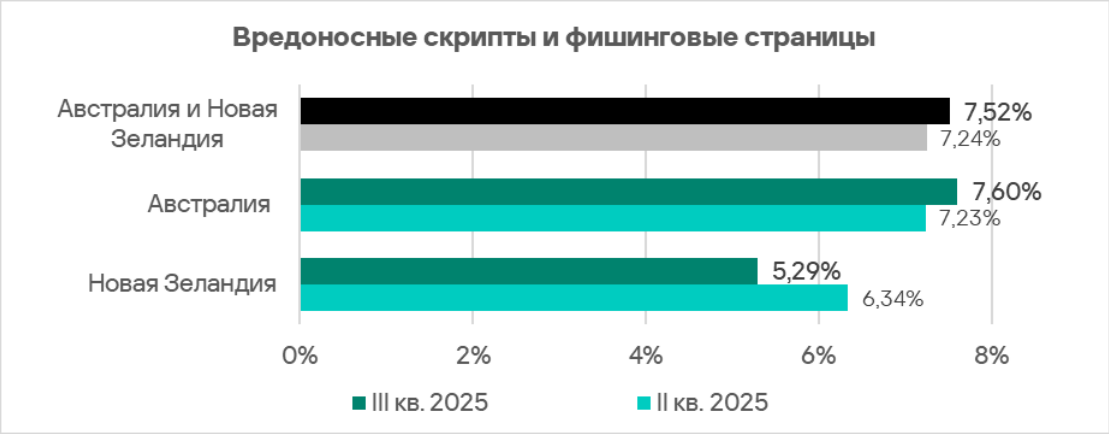
По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, регион Австралия и Новая Зеландия занимает седьмое место. Это самая высокая позиция региона в рейтингах как по источникам, так и по категориям угроз.

В третьем квартале 2025 года доля компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, в регионе увеличилась до 7,52%. Этот показатель в 2,9 раза выше, чем в Северной Европе, где он наименьший из всех регионов.



В Австралии показатель выше, чем в Новой Зеландии, в 1,4 раза. В Австралии за квартал он вырос, а в Новой Зеландии – уменьшился.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



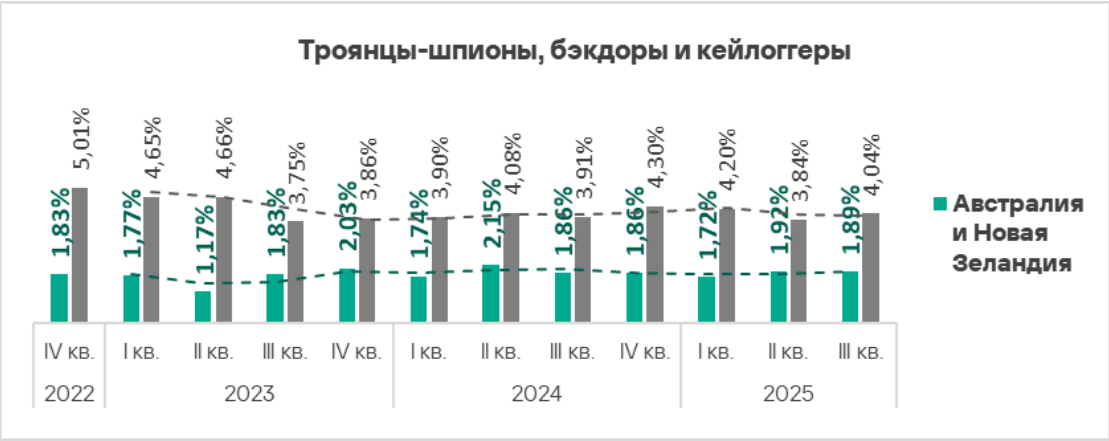
Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и в письмах по электронной почте.

Вредоносные скрипты могут использоваться злоумышленниками для целого ряда задач, в том числе для загрузки на компьютер шпионских программ.

Шпионские программы

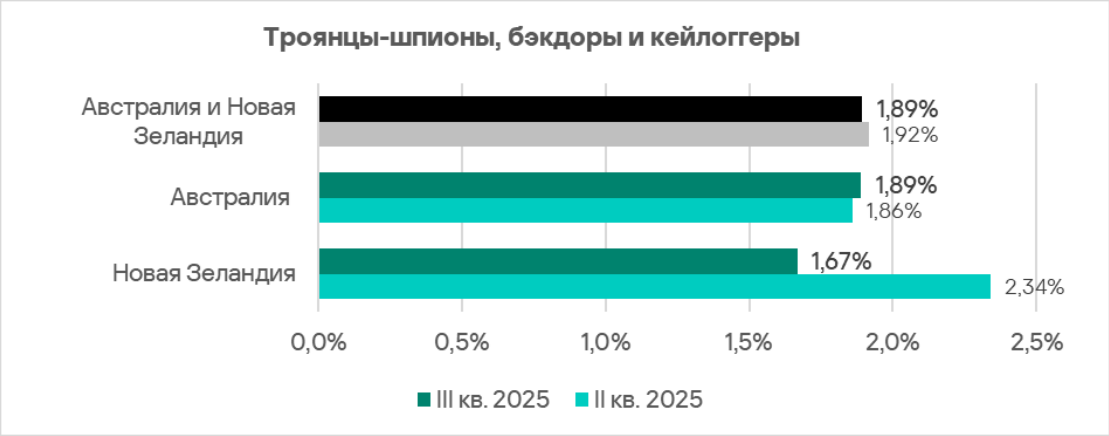
По доле компьютеров АСУ, на которых блокируются шпионские программы, регион Австралия и Новая Зеландия занимает в соответствующем рейтинге 11-е место с 1,89%. Это в 1,4 раза больше, чем в Северной Европе, где значение наименьшее.

Доля компьютеров АСУ, на которых блокируются шпионские программы, в регионе колеблется. В третьем квартале 2025 года этот показатель немного уменьшился.



В предыдущем квартале доля компьютеров АСУ, на которых блокируются шпионские программы, в Новой Зеландии была заметно выше, чем в Австралии. За квартал показатель Новой Зеландии уменьшился, и она уступила первенство Австралии.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

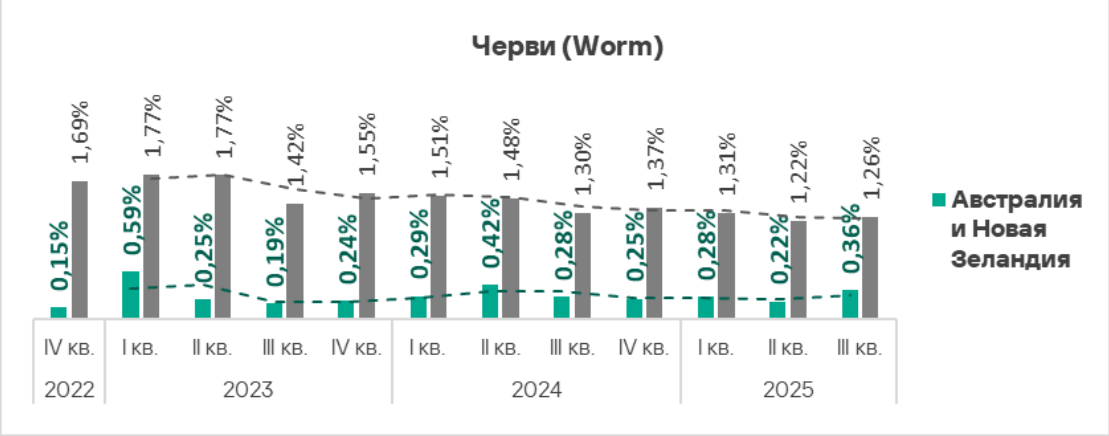


Шпионские программы в регионе блокируются в интернете и, преимущественно, в почтовых клиентах.

Черви

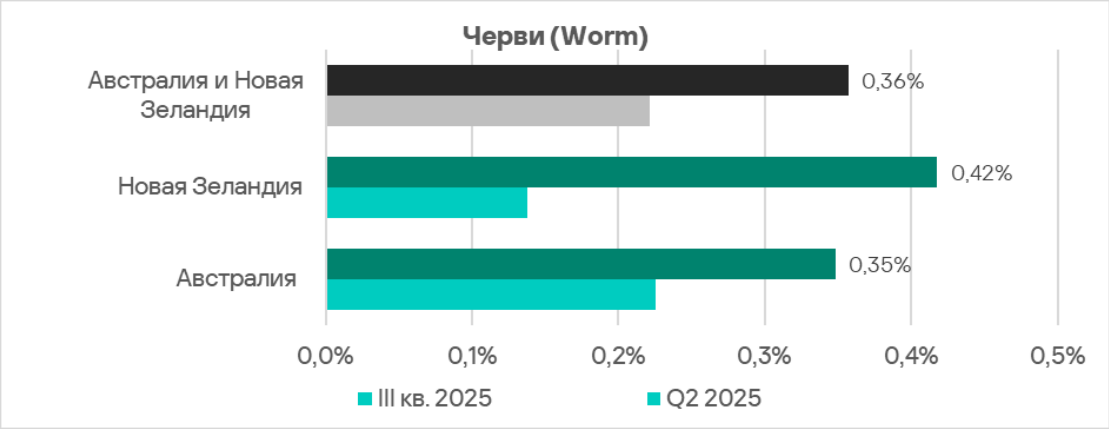
По доле компьютеров АСУ, на которых блокируются черви, регион Австралия и Новая Зеландия занимает 12-е место в рейтинге с показателем 0,36%. Это в 1,6 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Показатель в регионе колеблется, в третьем квартале 2025 года он вырос до наибольшего со второго квартала 2024 года значения.



Доля компьютеров АСУ, на которых блокируются черви, за квартал заметно выросла в обеих странах региона. Показатель в Новой Зеландии больше, чем в Австралии.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

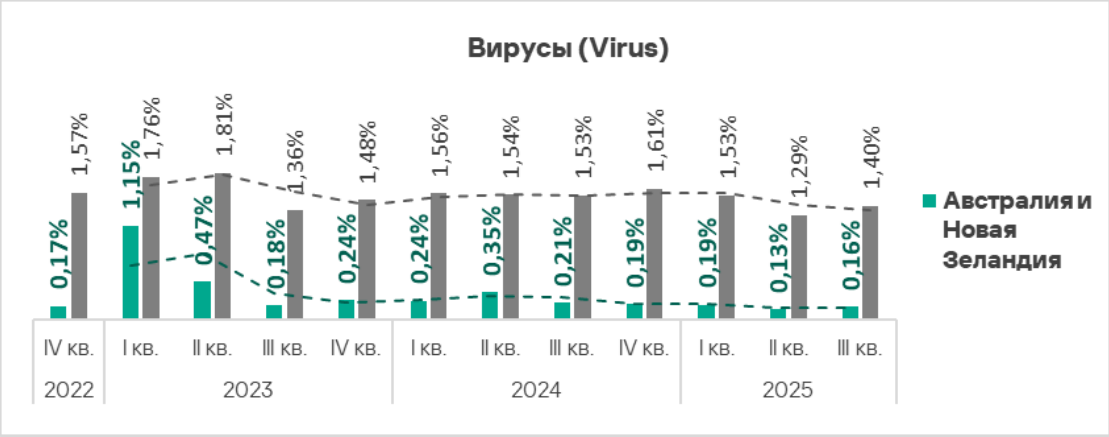


Распространяются черви через все источники угроз. В третьем квартале 2025 года чаще всего они распространялись в почтовых клиентах и на съемных носителях.

Вирусы

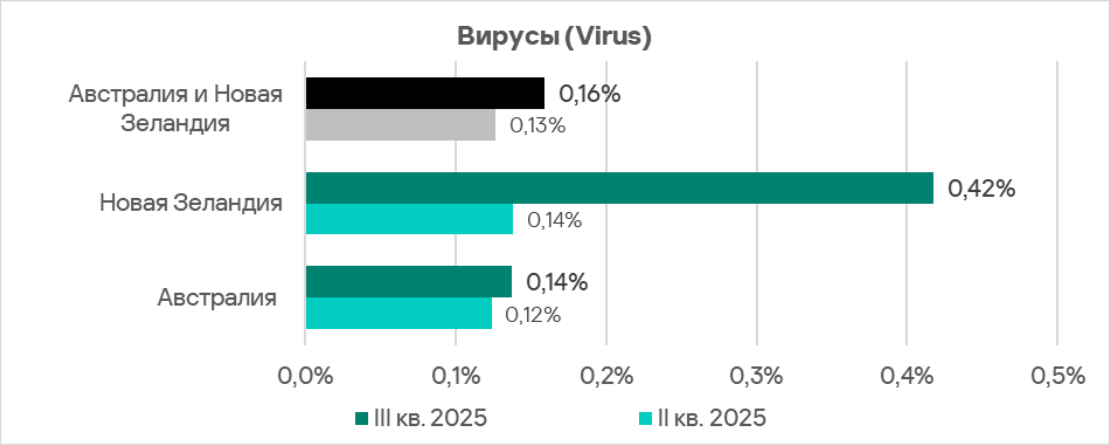
По доле компьютеров АСУ, на которых блокируются вирусы, Австралия и Новая Зеландия занимает 14-е место в рейтинге регионов с показателем 0,16%.

Показатель в регионе подрос впервые со второго квартала 2024 года.



Доля компьютеров АСУ, на которых блокируются вирусы, увеличилась в обеих странах региона, в Новой Зеландии – в 3,0 раза. Во столько же показатель за третий квартал 2025 года в этой стране выше, чем в Австралии.

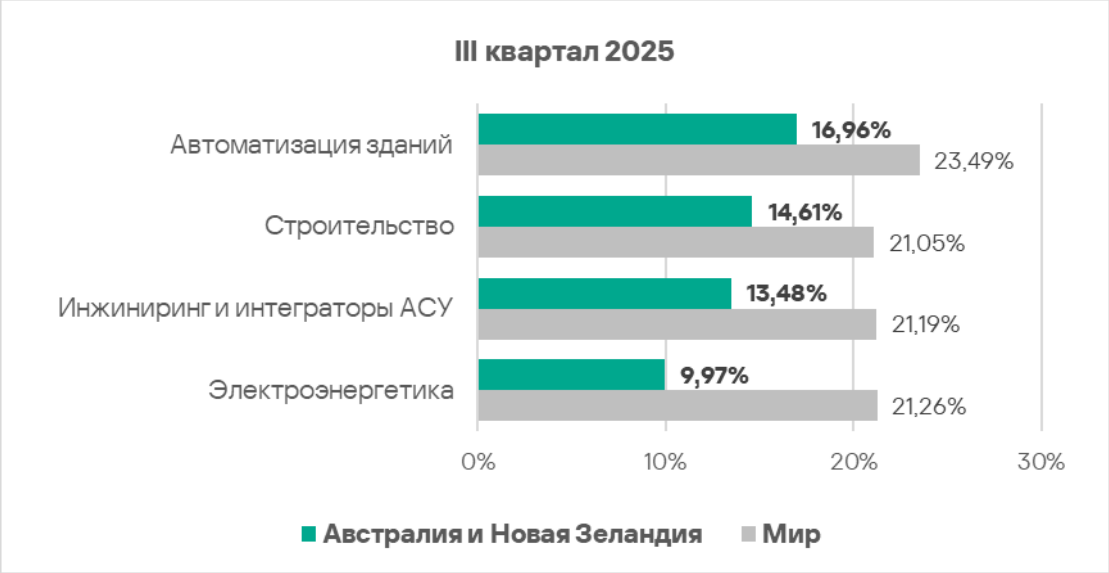
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Как и черви, вирусы в регионе распространяются через все источники угроз. В третьем квартале 2025 года чаще всего они распространялись в почтовых клиентах и на съемных носителях.

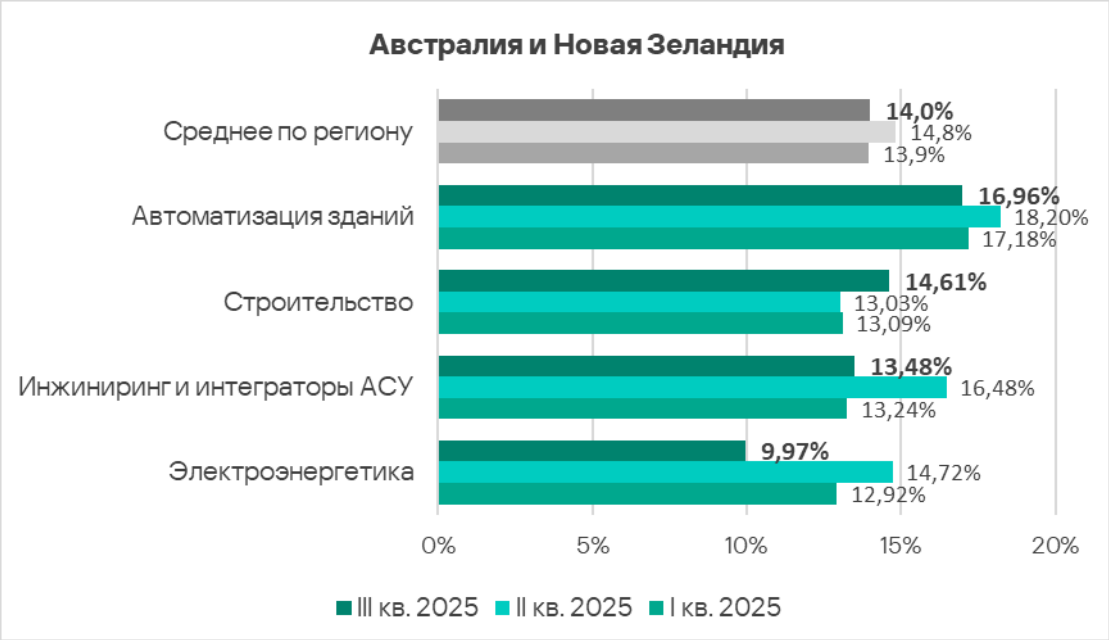
Отрасли

Среди рассмотренных в отчете отраслей в Австралии и Новой Зеландии чаще всего встречается с угрозами автоматизация зданий.

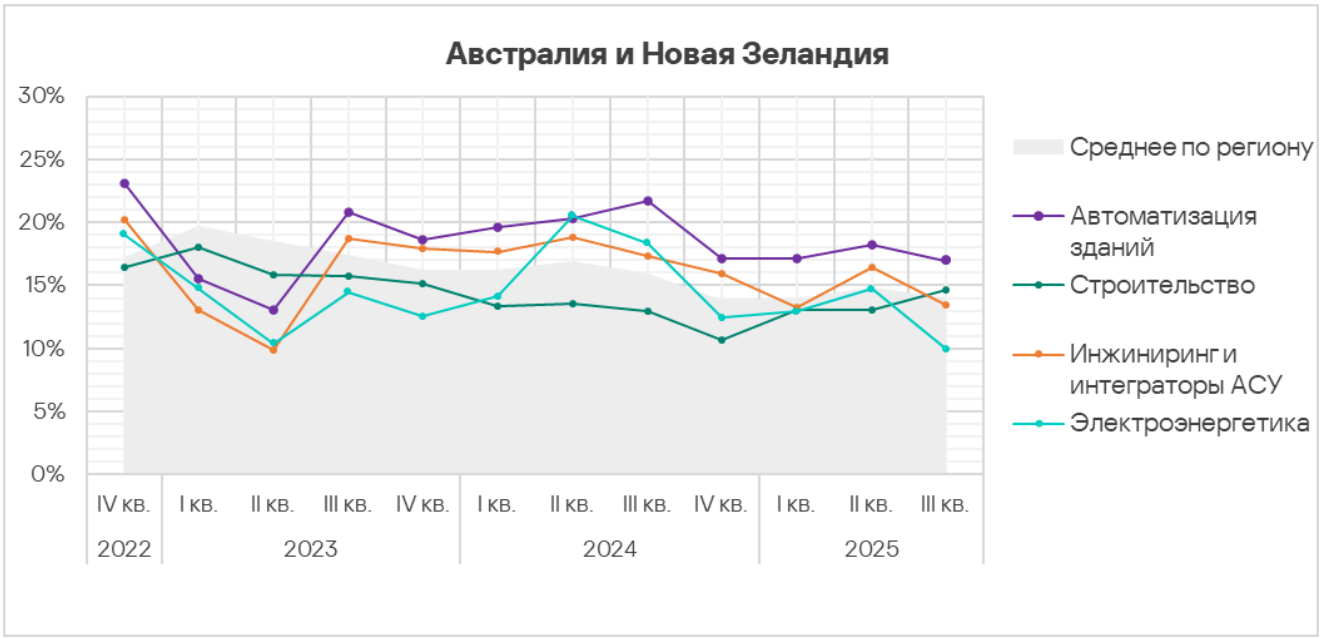


В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась во всех рассматриваемых отраслях, кроме строительства.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



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 в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

источнику). Красный цвет указывает на то, что значение близко к максимальному.

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

Отрасль / Источник угрозы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Показатель категорий в регионе
Интернет	6,65%	2,66%	7,20%	6,60%	6,84%
Почтовые клиенты	6,46%	1,66%	2,56%	4,80%	3,74%
Съемные носители	0,05%	0,00%	0,04%	0,00%	0,05%
Сетевые папки	0,00%	0,00%	0,00%	0,00%	0,02%
Показатель отрасли в регионе	16,96%	9,97%	13,48%	14,61%	

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Показатели категорий угроз в отраслях в Австралии и Новой Зеландии, III 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	2,80%	0,33%	2,32%	1,67%	2,35%
Вредоносные скрипты и фишинговые страницы	8,99%	3,99%	6,50%	9,29%	7,52%
Троянцы-шпионы, бэкдоры и кейлоггеры	3,03%	1,99%	1,83%	1,19%	1,89%
Черви (Worm)	0,50%	0,33%	0,35%	0,35%	0,36%
Майнеры — исполняемые файлы для ОС Windows	0,23%	0,00%	0,14%	0,09%	0,13%
Вредоносные документы (MSOffice+PDF)	3,07%	2,66%	1,19%	1,72%	1,77%
Вирусы (Virus)	0,28%	0,33%	0,04%	0,18%	0,16%
Программы-вымогатели	0,23%	0,00%	0,07%	0,00%	0,08%
Веб-майнеры, выполняемые в браузерах	0,09%	0,00%	0,14%	0,09%	0,09%
Вредоносные программы для AutoCAD	0,00%	0,00%	0,00%	0,13%	0,03%
Показатель отрасли в регионе	16,96%	9,97%	13,48%	14,61%	

В рейтингах регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в различных отраслях, Австралия и Новая Зеландия не поднимается выше 11-го места.

В двух отраслях — строительство и электроэнергетика — регион вошел в тройку лидеров по показателям в отрасли угроз из почтовых клиентов, вредоносных документов и вредоносных скриптов.

- Среди регионов по показателям в строительной отрасли Австралия и Новая Зеландия занимает третье место по угрозам из почтовых клиентов и вредоносным скриптам и фишинговым страницам.
- Среди регионов по показателям в электроэнергетической отрасли регион Австралия и Новая Зеландия занимает второе место по вредоносным документам.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Напомним, что 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.

Автоматизация зданий

Австралия и Новая Зеландия находится на 11-м месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий.

Среди отраслей в регионе отрасль автоматизация зданий занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах и на съемных носителях;
- второе место по показателям угроз из интернета;
- первое место по доле компьютеров АСУ, на которых блокируются угрозы следующих категорий: ресурсы в интернете из списка запрещенных, шпионские программы, вредоносные документы, черви, майнеры — исполняемые файлы для ОС Windows;
- второе место по показателям угроз следующих категорий: вредоносные скрипты и фишинговые страницы, вирусы, веб-майнеры, программы-вымогатели.

Строительство

Регион Австралия и Новая Зеландия находится на 11-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

Среди регионов по показателям в отрасли регион занимает:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов
- третье место по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы.

Среди отраслей в регионах строительство занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах;
- третье место по показателю угроз в интернете;
- первое место по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, а также вредоносные программы для AutoCAD;
- второе место по показателю червей;

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- третье место по показателям угроз следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные документы, вирусы, майнеры обеих категорий.

Инжиниринг и интеграторы АСУ

Регион Австралия и Новая Зеландия находится на 11-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли инжиниринг и интеграторы АСУ.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета;
- второе место по показателю съемных носителей;
- третье место по показателю почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых блокируются веб-майнеры и программы-вымогатели;
- второе место по показателю следующих категорий угроз: ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы для ОС Windows;
- третье место по показателю следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, черви.

Электроэнергетика

Регион Австралия и Новая Зеландия находится на 12-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

Среди регионов по показателям в отрасли регион занимает:

- второе место по доле компьютеров АСУ, на которых блокируются вредоносные документы.

Среди отраслей в регионе электроэнергетика занимает:

- первое место по доле компьютеров АСУ, на которых блокируются вирусы;
- второе место по показателям шпионского ПО и вредоносных документов.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Методика подготовки статистики

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

Подключение к сети KSN 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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»