Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Австралия и Новая Зеландия

Четвертый квартал 2025 года

30.04.2026

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, в четвертом квартале 2025 года Австралия и Новая Зеландия занимают 11-е место в рейтинге регионов. При этом по показателям некоторых источников и категорий угроз регион в соответствующих рейтингах занимает более высокие позиции.

Самые высокие позиции региона – в рейтингах регионов по показателям следующих источников угроз:

- интернет — седьмое место;
- почтовые клиенты — седьмое место.

Австралия и Новая Зеландия – один из пяти регионов, где показатель угроз из интернета за квартал вырос. По его росту регион находится на третьем месте.

В рейтингах регионов по доле компьютеров АСУ, на которых блокируются вредоносные объекты различных категорий, самые высокие позиции у Австралии и Новой Зеландии по показателям угроз следующих категорий:

- программы-вымогатели — седьмое место;
- вредоносные скрипты и фишинговые страницы — восьмое место;
- вредоносные документы — девятое место;
- веб-майнеры — девятое место.

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.

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 четвертом квартале 2025 года в регионе отмечен рост доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

- веб-майнеры — в 1,7 раза, регион занимает первое место по росту показателя;
- программы-вымогатели — в 1,6 раза, второе место по росту показателя;
- майнеры в формате исполняемых файлов — в 1,5 раза, второе место по росту показателя;
- черви — в 1,1 раза.

Показатели майнеров обеих категорий больше всего выросли в автоматизации зданий.

Показатель программ-вымогателей увеличился только в строительстве и автоматизации зданий.

Показатель червей увеличился только в автоматизации зданий.

Особенности стран

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

Соответственно, в Австралии выше, чем в Новой Зеландии, показатели угроз, которые распространяются в почте: вредоносных документов, вредоносных скриптов и фишинговых страниц и червей (черви в четвертом квартале 2025 года распространялись через почту в ходе очередной волны фишинговых атак, известных как Curriculum-vitae-catalina). Также в Австралии выше доля компьютеров АСУ, на которых блокируются шпионские программы.

Новая Зеландия в четвертом квартале 2025 года занимает первое место по показателям угроз из интернета. Соответственно, в Новой Зеландии выше, чем в Австралии, показатели категорий угроз, которые распространяются через интернет: ресурсы в интернете из списка запрещенных, майнеры обоих видов.

Кроме того, Новая Зеландия находится на первом месте по показателю программ-вымогателей.

Отрасли

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

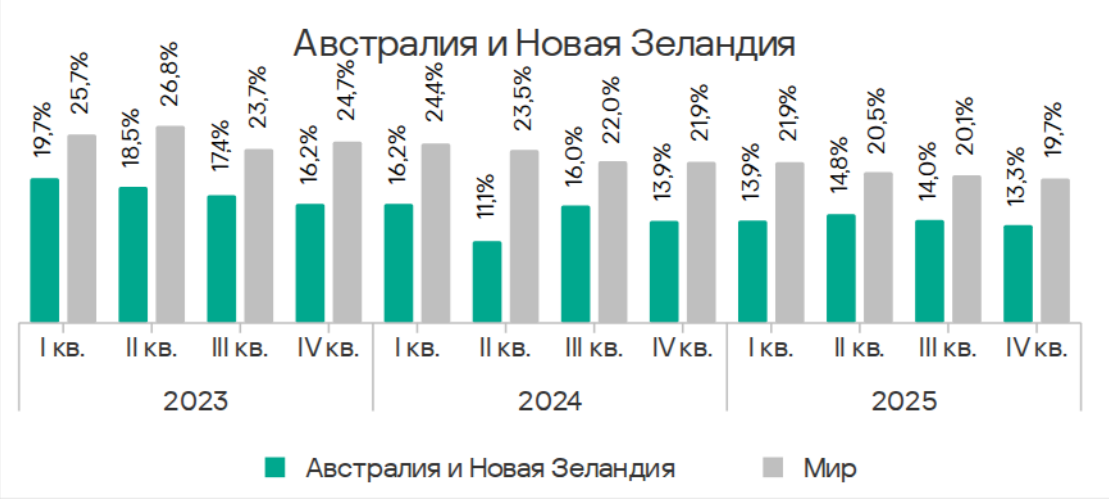
Среди отраслей в регионе по большинству показателей лидирует автоматизация зданий.

В четвертом квартале 2025 года автоматизация зданий среди отраслей в регионе является:

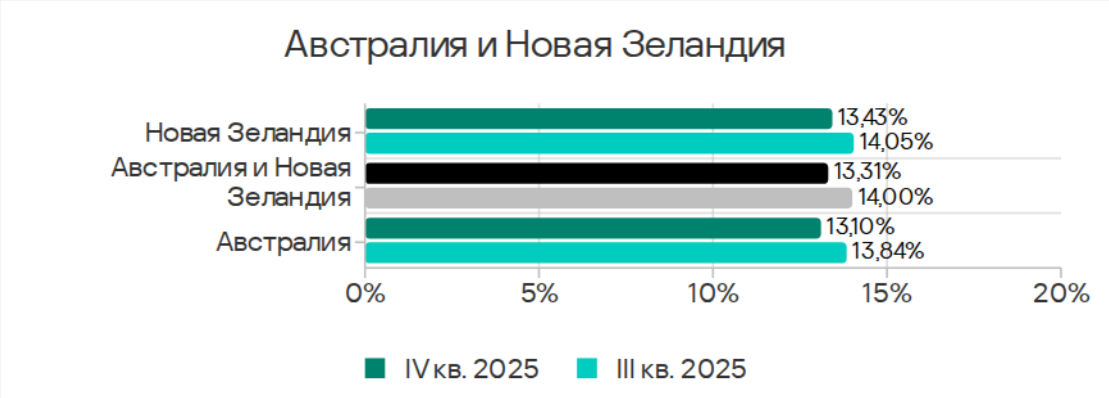
- лидером по росту показателей майнеров обеих категорий;
- одной из двух отраслей, где вырос показатель программ-вымогателей (вторая – строительство);
- единственной отраслью, где в результате фишинговой атаки увеличился показатель червей.

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, с 13,31%. Значение в регионе существенно ниже среднемирового, но в 1,6 раза выше, чем в Северной Европе, которая замыкает этот рейтинг.

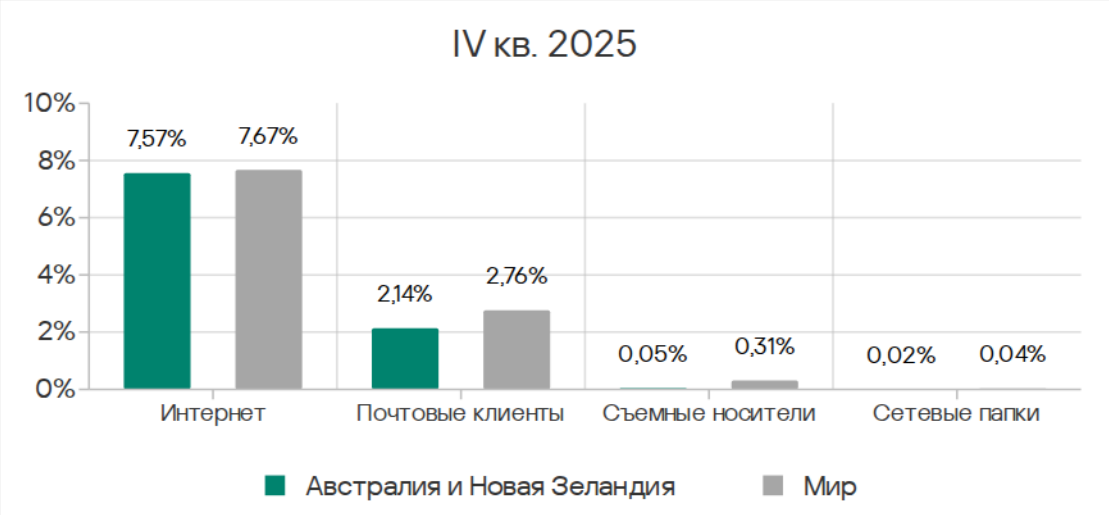


Показатель региона в целом во многом зависит от ситуации в Австралии. Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в этой стране меньше, чем в Новой Зеландии. В обеих странах показатель за квартал заметно уменьшился.



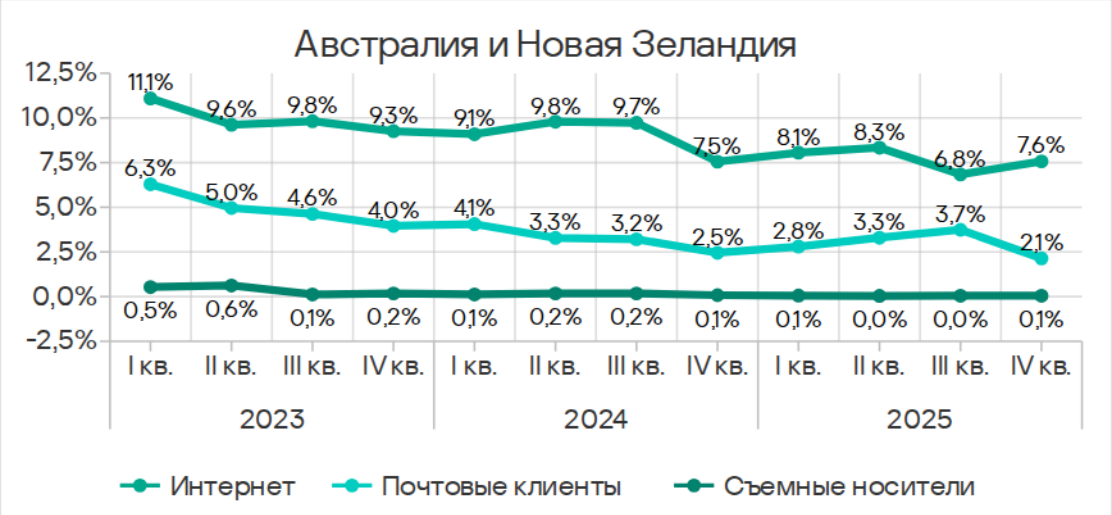
Источники угроз

Показатели всех источников угроз в Австралии и Новой Зеландии ниже среднемировых. Ближе всего к мировому показателю значение у угроз из интернета.



Вредоносные объекты в регионе распространяются преимущественно через интернет и почту. По показателям этих источников угроз Австралия и Новая Зеландия занимают седьмое место в соответствующих рейтингах регионов.

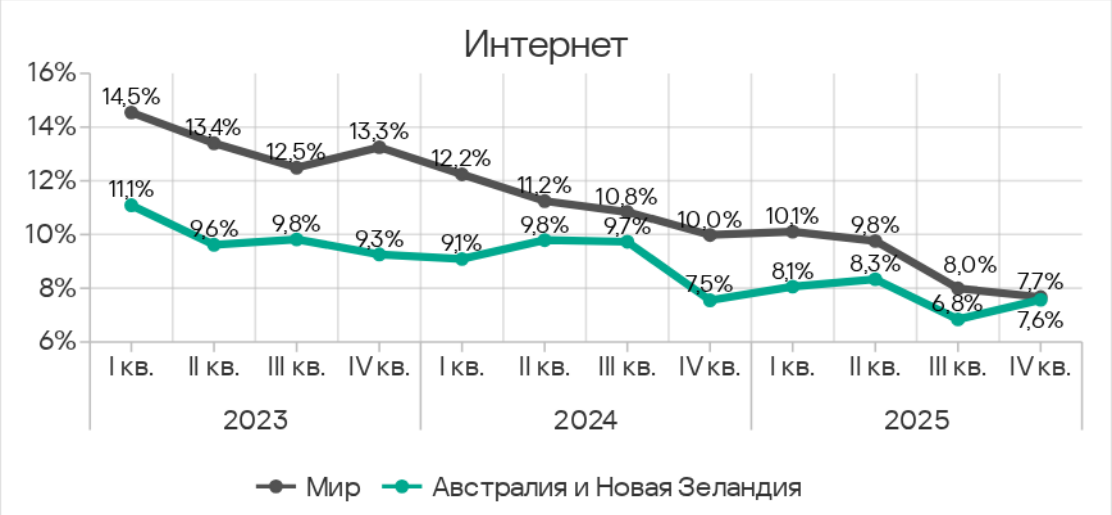
В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в регионе, увеличилась только у угроз интернета.



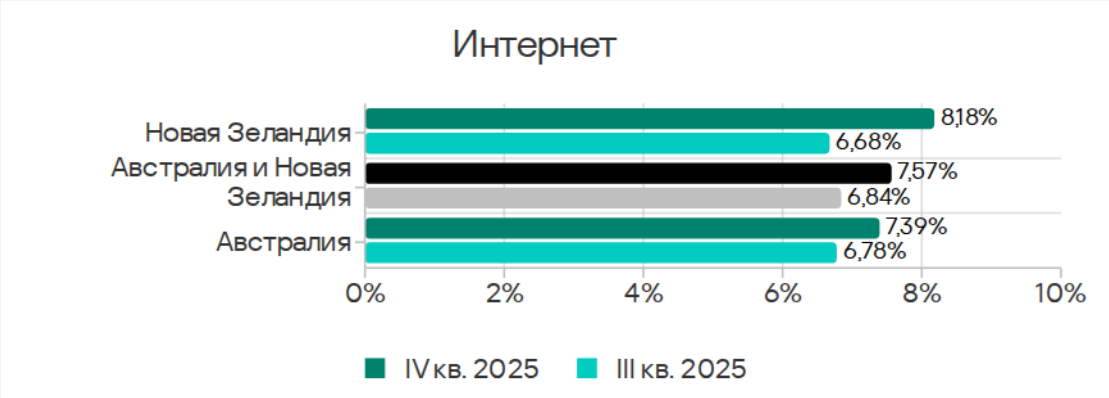
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, регион Австралия и Новая Зеландия занимает седьмое место с 7,57%. Это в 1,9 раза больше показателя в Северной Европе, которая замыкает соответствующий рейтинг.

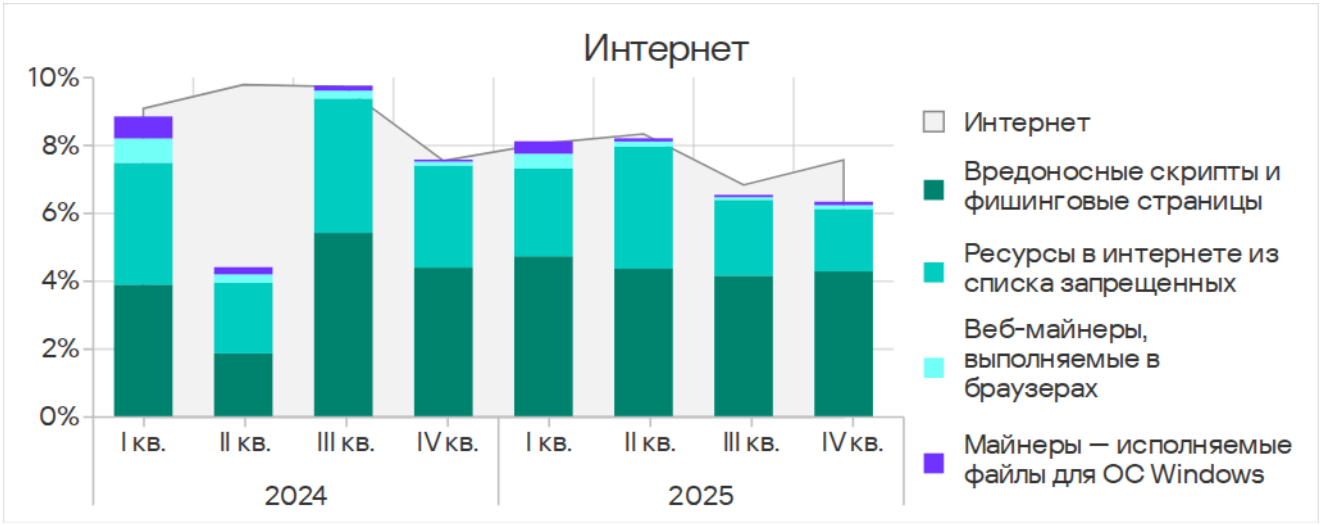
Австралия и Новая Зеландия – один из пяти регионов, где показатель угроз из интернета за квартал вырос. По его росту регион находится на третьем месте.



Доля компьютеров АСУ, на которых блокируются угрозы из интернета, за квартал увеличилась в обеих странах региона.



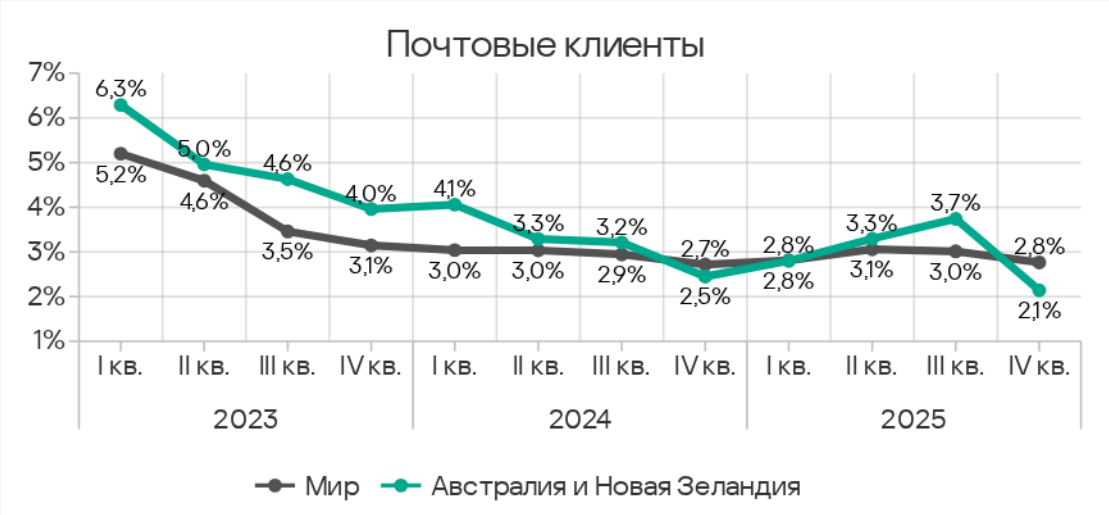
Основные категории угроз из интернета, которые блокируются на компьютерах АСУ в регионе: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных.



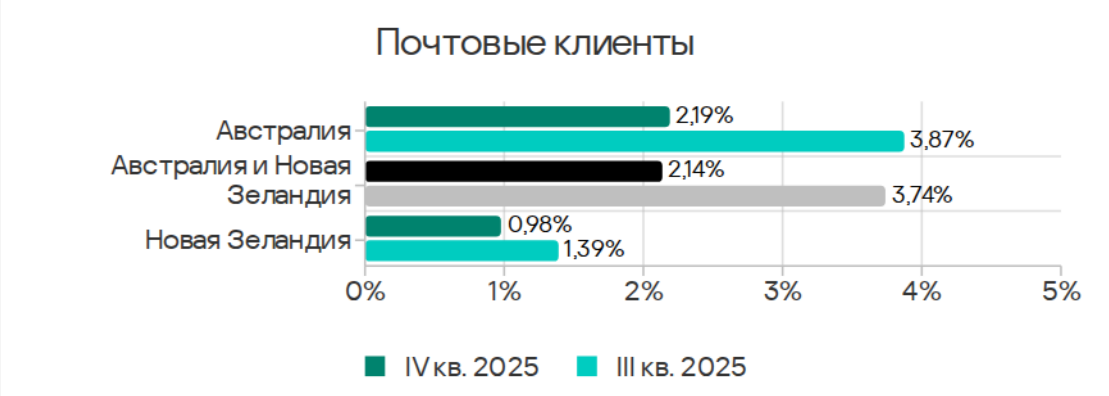
Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, в четвертом квартале 2025 года регион Австралия и Новая Зеландия занимает седьмое место.

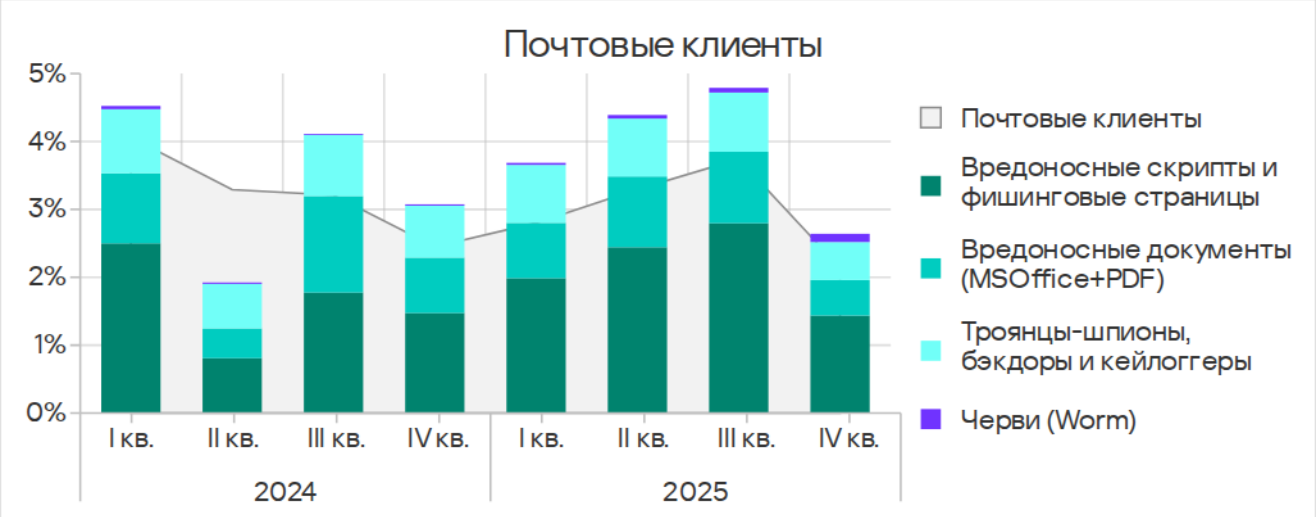
После роста в течение предыдущих трех кварталов в четвертом квартале 2025 года показатель почтовых клиентов в регионе снизился до 2,14%. Это значение – наименьшее за исследуемый период. Оно ниже среднемирового, но в 3,5 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.



Доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, в Австралии в 2,2 раза больше, чем в Новой Зеландии. Показатели за квартал снизились в обеих странах региона.



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

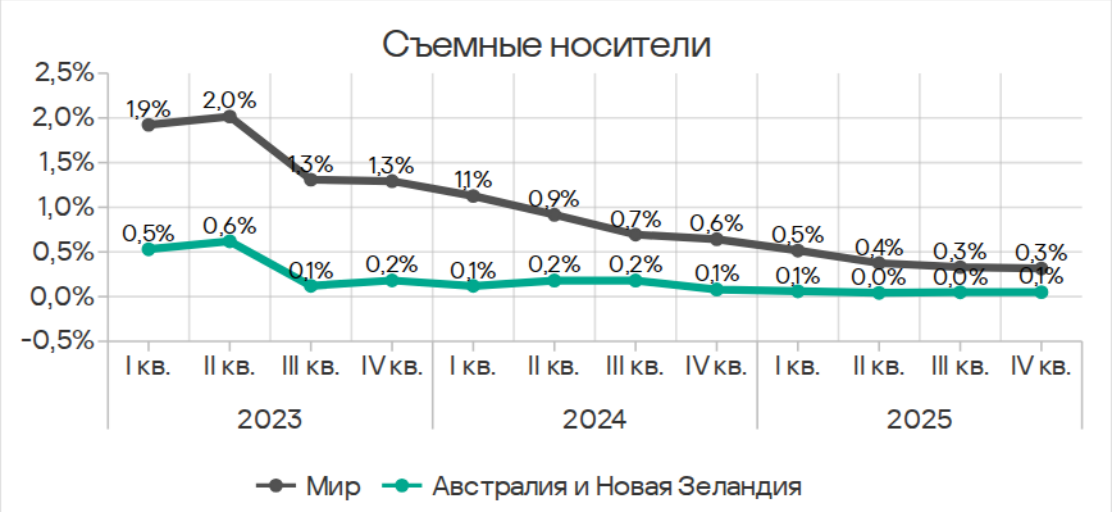


В четвертом квартале 2025 года во всех регионах увеличилась доля компьютеров АСУ, на которых были заблокированы черви из почтовых клиентов. Это связано с очередной волной фишинговых кампаний, известных как Curriculum-vitae-catalina, в ходе которых по электронной почте рассылались фишинговые письма с вредоносным вложением (червь-бэкдор Backdoor.MSIL.XWorm). В Австралии и Новой Зеландии показатель червей также вырос, но это изменение было наименьшим среди регионов.

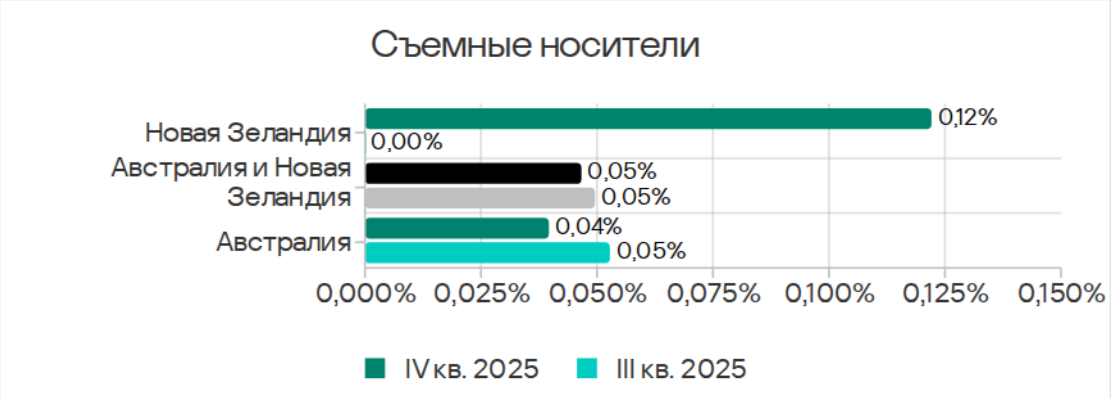
Съемные носители

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

Показатель за квартал не изменился.

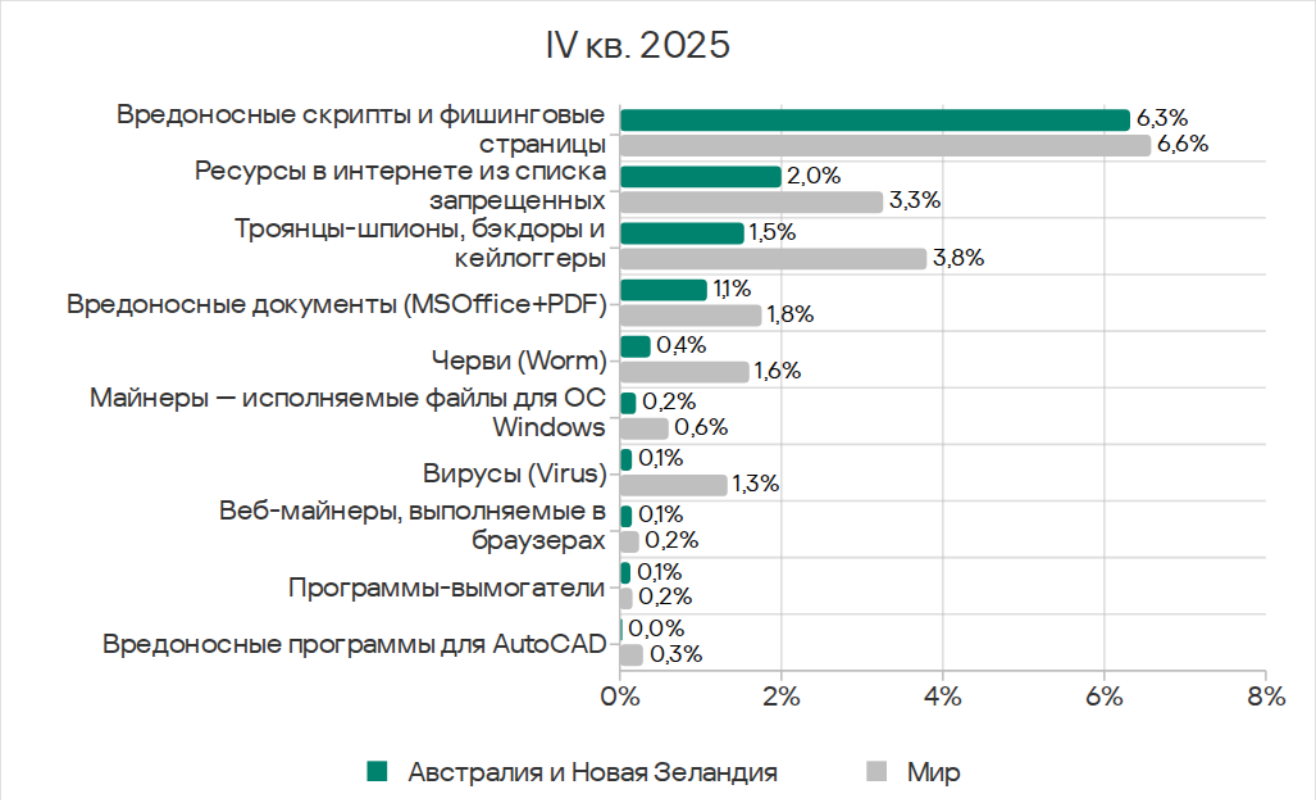


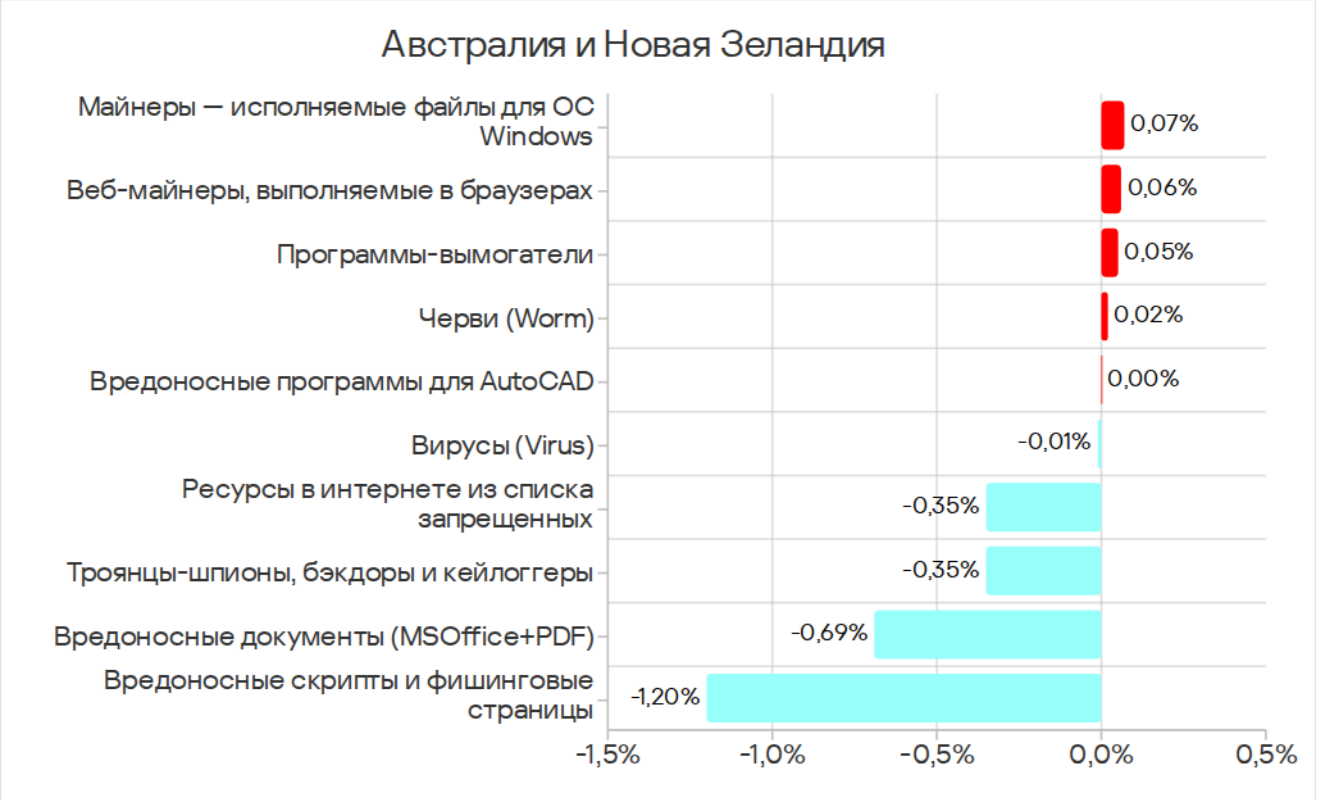
Угрозы на съемных носителях в регионе блокируются преимущественно в Австралии, но в четвертом квартале 2025 года резко вырос показатель в Новой Зеландии.



Основные категории угроз на съемных носителях, которые блокируются на компьютерах АСУ: черви и вирусы.

Категории угроз





В четвертом квартале 2025 года в регионе Австралия и Новая Зеландия показатели всех категорий угроз меньше среднемировых.

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

- веб-майнеры — в 1,7 раза, регион на первом месте по росту показателя;
- программы-вымогатели — в 1,6 раза;
- майнеры в формате исполняемых файлов — в 1,5 раза;
- черви — в 1,1 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 угроз следующих категорий:

- программы-вымогатели — седьмое место;
- вредоносные скрипты и фишинговые страницы — восьмое место;
- вредоносные документы — девятое место;
- веб-майнеры — девятое место.

В регионе показатели майнеров обеих категорий больше всего выросли в автоматизации зданий.

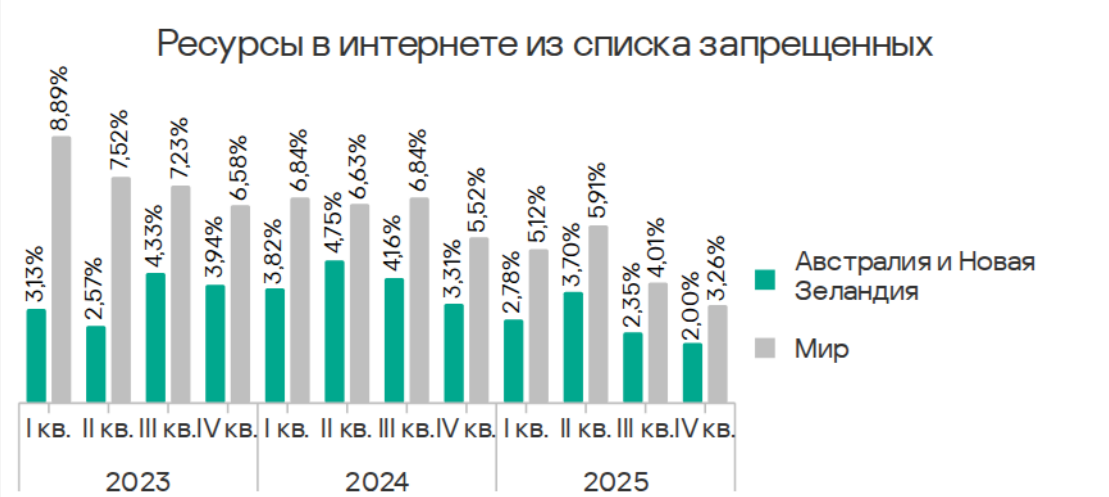
Показатели программ-вымогателей увеличились только в строительстве и автоматизации зданий.

Показатель червей увеличился в единственной отрасли — автоматизация зданий – и только в Австралии.

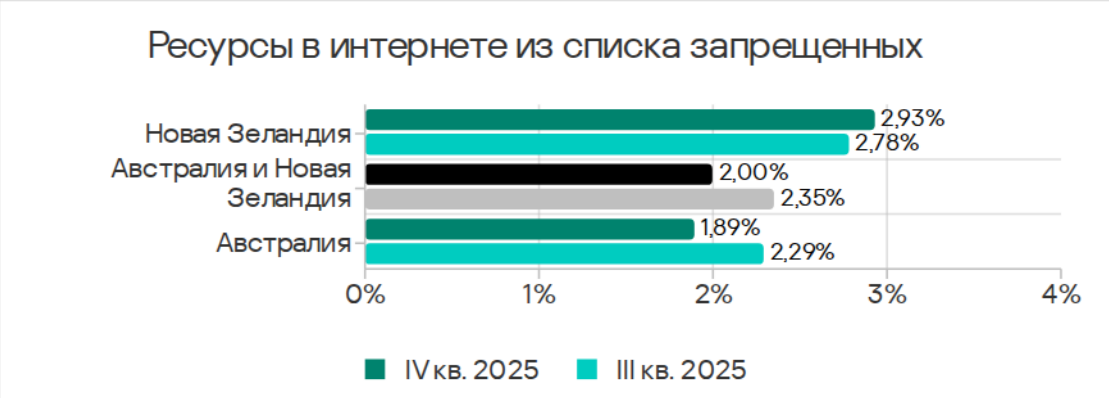
Ресурсы в интернете из списка запрещенных

По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, регион Австралия и Новая Зеландия занимает 12-е место с 2,00%. Это в 1,1 раза больше, чем в Северной Европе, где он наименьший среди регионов.

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



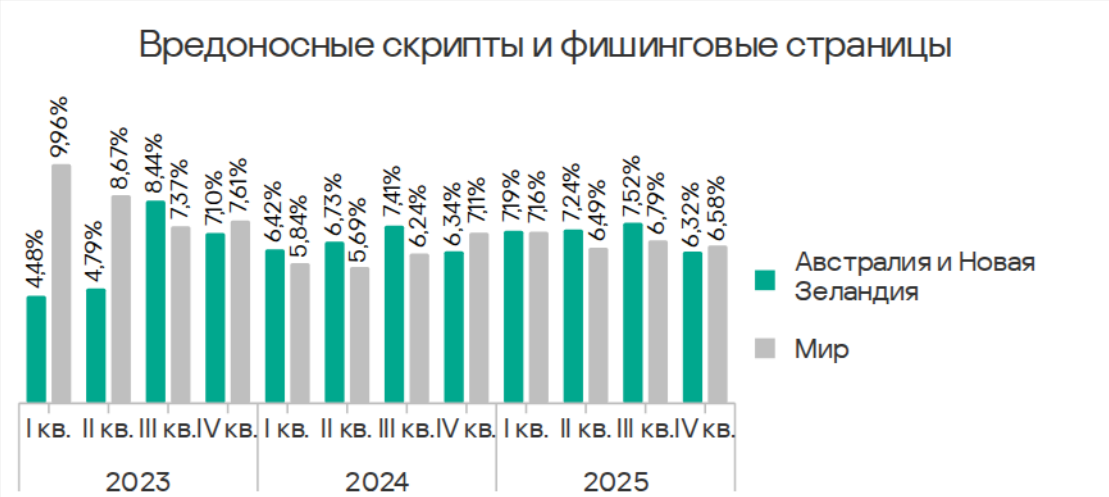
Доля компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в Новой Зеландии выше, чем в Австралии, в 1,6 раза.



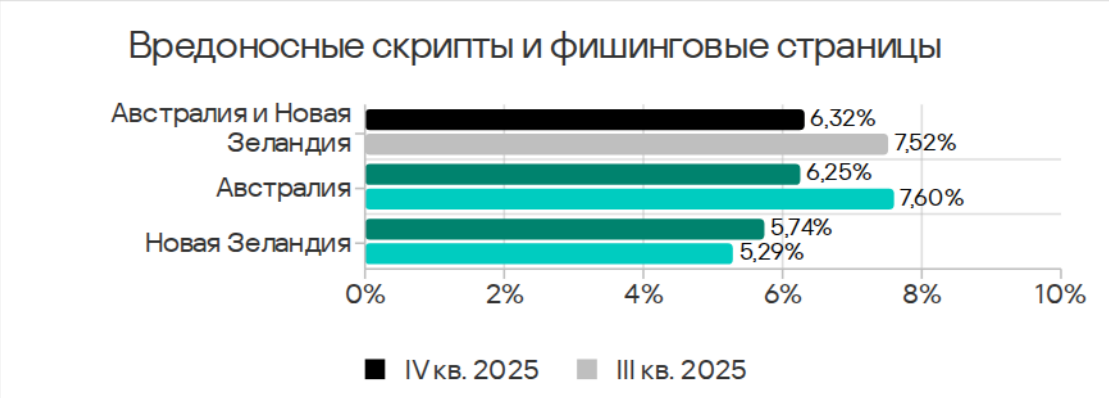
Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, регион Австралия и Новая Зеландия занимает восьмое место.

После роста в течение предыдущих трех кварталов, в четвертом квартале 2025 года доля компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, в регионе уменьшилась до 6,32%. Этот показатель в 2,5 раза выше, чем в Северной Европе, где он наименьший из всех регионов.



За квартал показатель уменьшился в Австралии и вырос в Новой Зеландии, но в Австралии он по-прежнему выше, чем в Новой Зеландии.



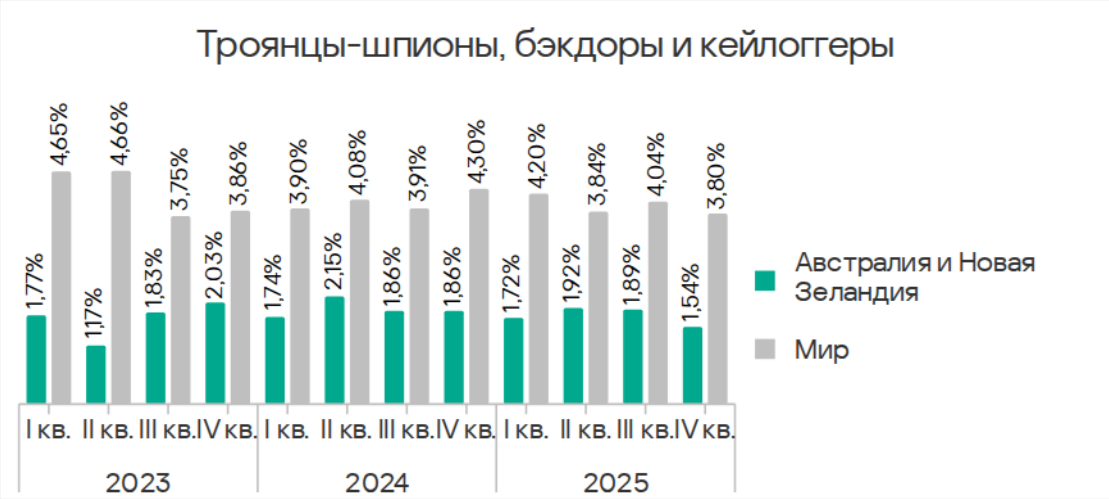
В регионе вредоносные скрипты и фишинговые страницы распространяются преимущественно в интернете, встречаются также в электронной почте.

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

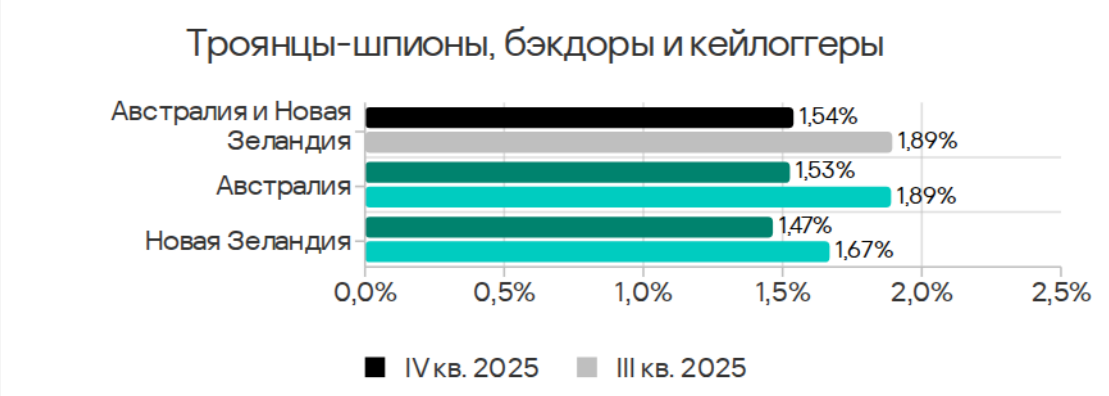
Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, регион Австралия и Новая Зеландия занимает в соответствующем рейтинге 11-е место с 1,54%. Это в 1,2 раза больше, чем в Северной Европе, где значение наименьшее.

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



Доля компьютеров АСУ, на которых блокируются шпионские программы, в Австралии выше, чем в Новой Зеландии. Показатель уменьшился в обеих странах.



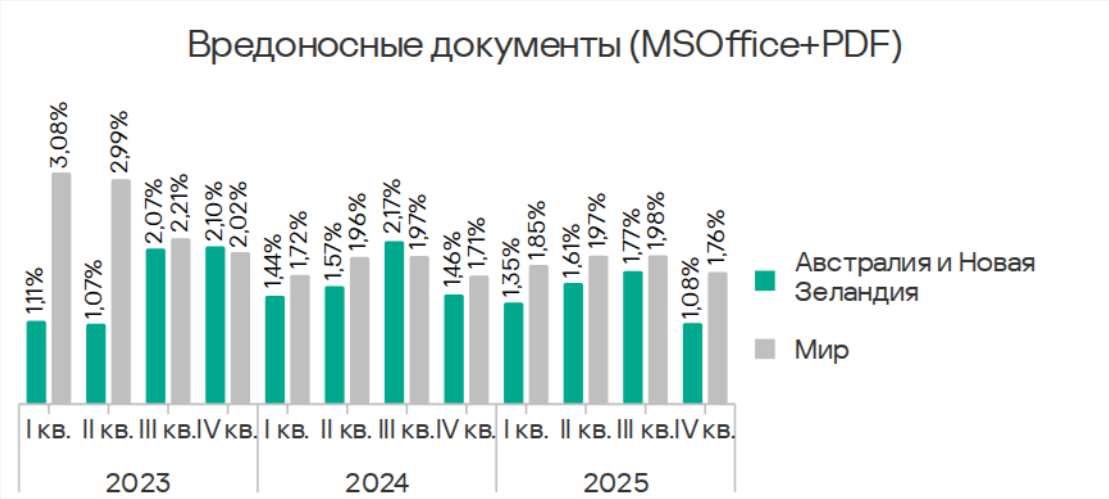
Шпионские программы в регионе блокируются преимущественно в почтовых клиентах.

Вредоносные документы

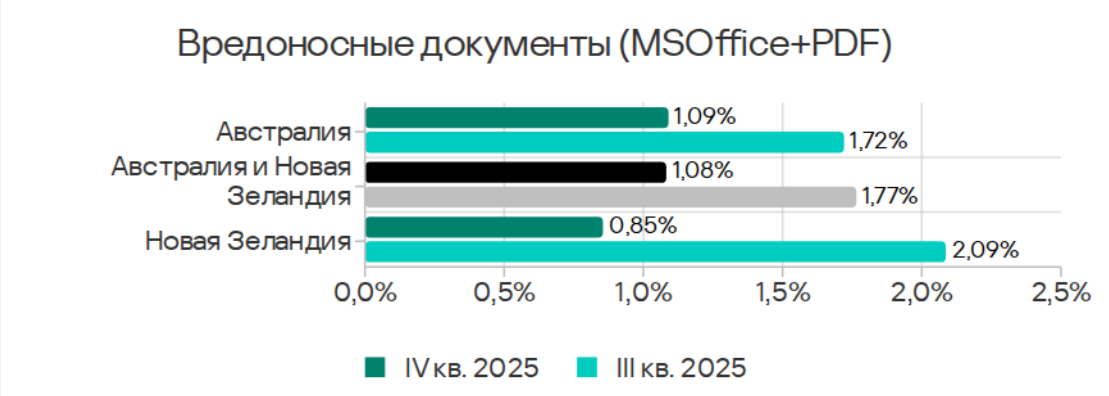
Регион Австралия и Новая Зеландия занимает девятое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные документы, с 1,08%.

Показатель в регионе в 2,3 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, в регионе колеблется. В четвертом квартале 2025 года показатель уменьшился.



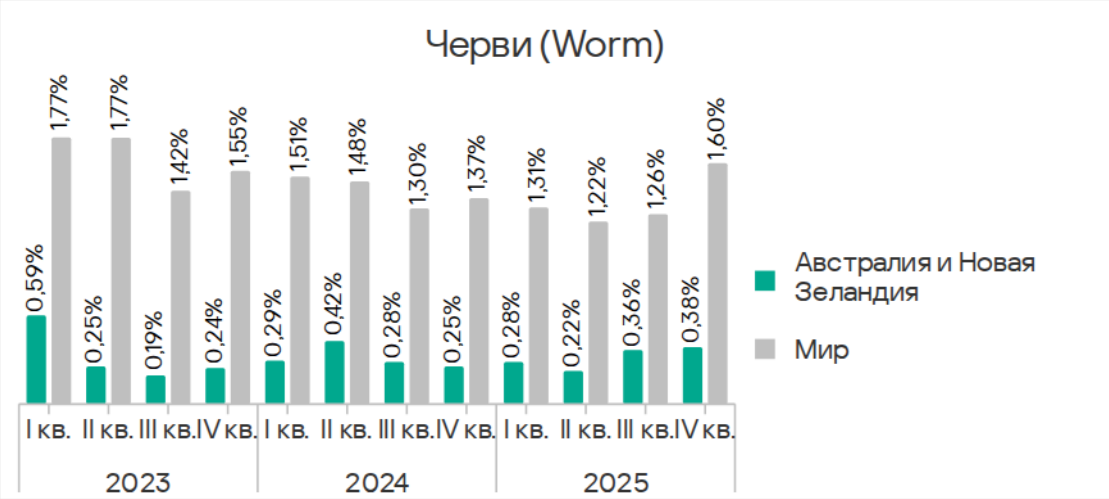
За квартал показатель уменьшился в обеих странах региона. Австралия вернула первенство по доле компьютеров АСУ, на которых блокируются вредоносные документы.



Распространяются вредоносные документы преимущественно по электронной почте.

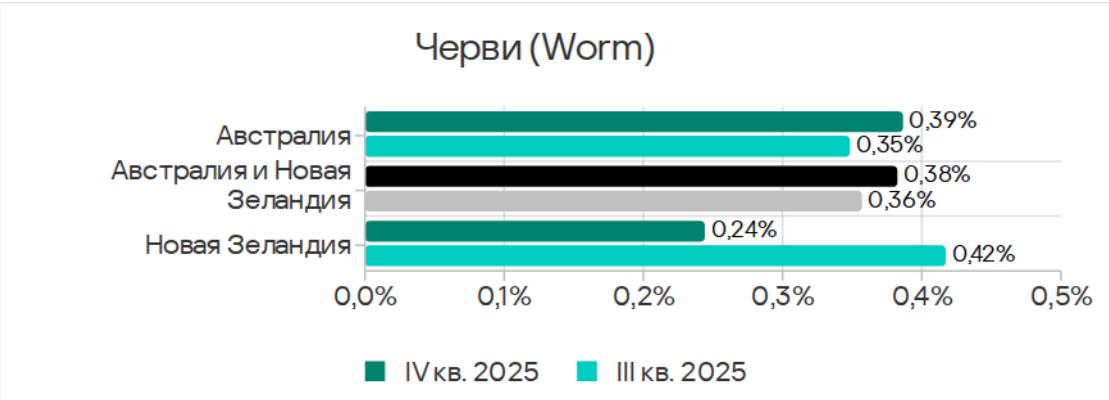
Черви

По доле компьютеров АСУ, на которых блокируются черви, регион Австралия и Новая Зеландия занимает 12-е место в рейтинге с показателем 0,38%. Это в 1,2 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.



В четвертом квартале 2025 года показатель червей вырос во всех регионах вследствие глобальной фишинговой кампании Curriculum-vitae-catalina, в ходе которой по электронной почте рассылались фишинговые письма с вредоносным вложением (червь-бэкдор Backdoor.MSIL.XWorm). Рост доли компьютеров АСУ, на которых блокировались черви, в регионе Австралия и Новая Зеландия был наименьшим среди регионов.

Доля компьютеров АСУ, на которых блокируются черви, за квартал уменьшилась в Новой Зеландии и выросла в Австралии.



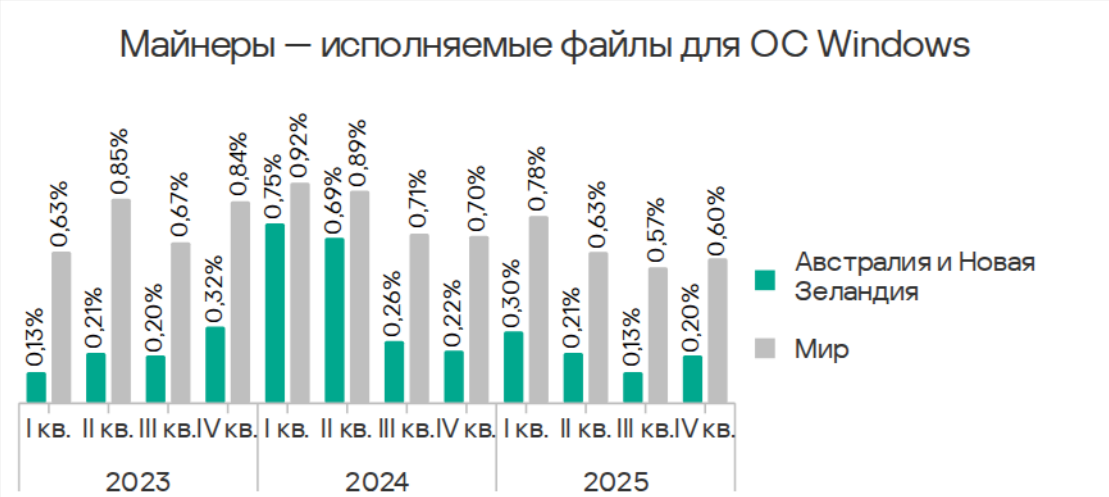
В четвертом квартале 2025 года черви распространялись в основном в почтовых клиентах – в ходе очередной волны фишинговых атак Curriculum-vitae-catalina.

Из исследуемых отраслей региона показатель червей увеличился только в автоматизации зданий.

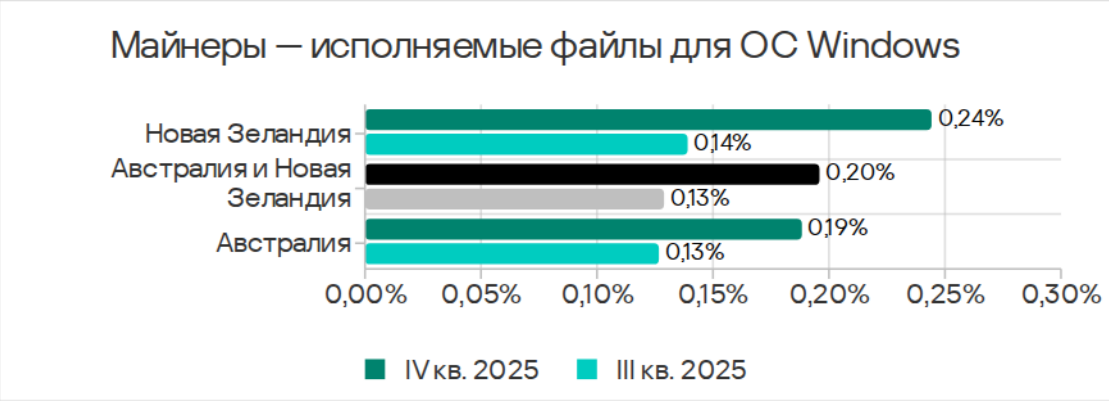
Майнеры – исполняемые файлы для ОС Windows

По доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows, Австралия и Новая Зеландия занимает 10-е место в рейтинге регионов с показателем 0,20%. Это в 1,4 раза больше, чем в Северной Америке (Канаде), где значение наименьшее среди регионов.

Австралия и Новая Зеландия – один из четырех регионов, где показатель майнеров в формате исполняемых файлов за квартал вырос. В Австралии и Новой Зеландии значение увеличилось в 1,5 раза.



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



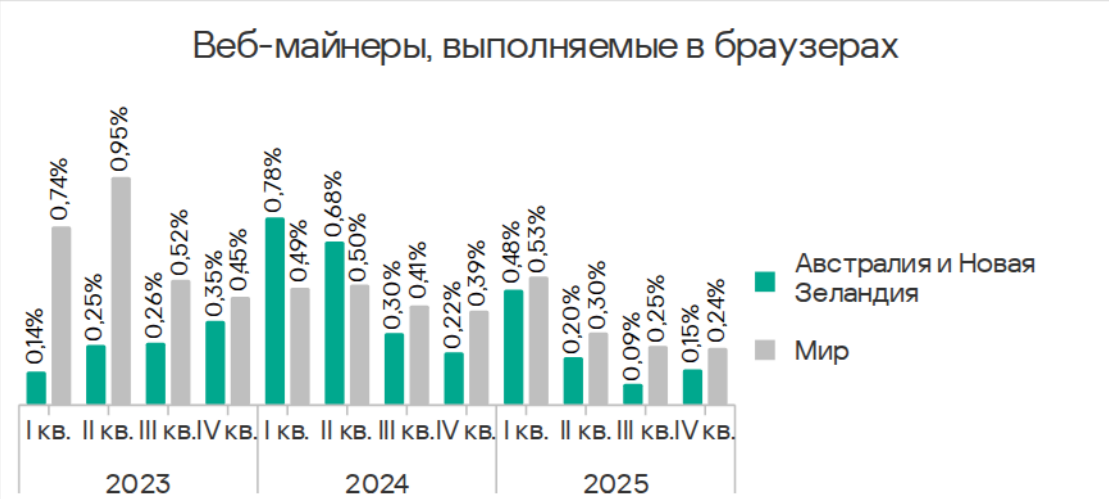
В регионе майнеры – исполняемые файлы распространяются в интернете.

Из исследуемых отраслей региона показатели майнеров этой категории больше всего выросли в автоматизации зданий.

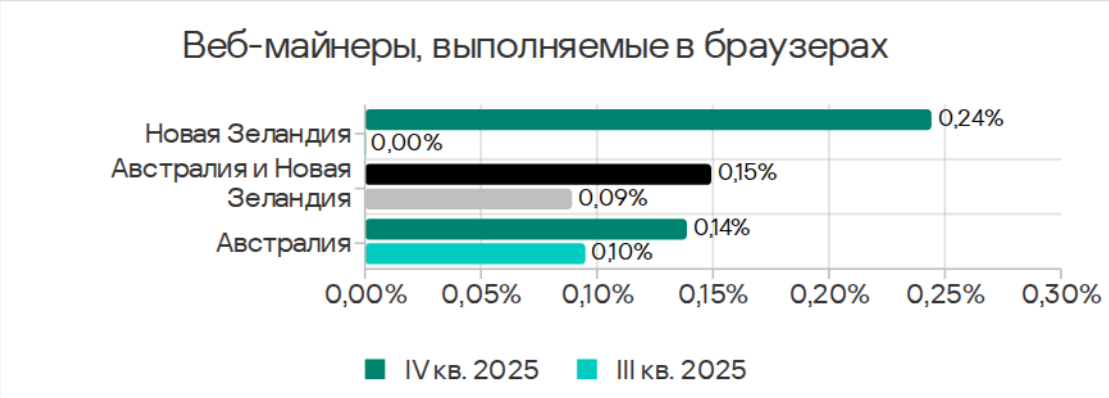
Веб-майнеры, выполняемые в браузерах

По доле компьютеров АСУ, на которых блокируются веб-майнеры, Австралия и Новая Зеландия занимают девятое место в рейтинге регионов с показателем 0,15%. Это в 2,5 раза больше, чем в Восточной Азии, где показатель – наименьший среди регионов.

Австралия и Новая Зеландия – один из трех регионов, где показатель веб-майнеров за квартал вырос. В Австралии и Новой Зеландии значение увеличилось в 1,7 раза, регион на первом месте по росту показателя.



Доля компьютеров АСУ, на которых блокируются веб-майнеры, за квартал выросла в обеих странах региона. Показатель в Новой Зеландии в четвертом квартале 2025 года больше, чем в Австралии.



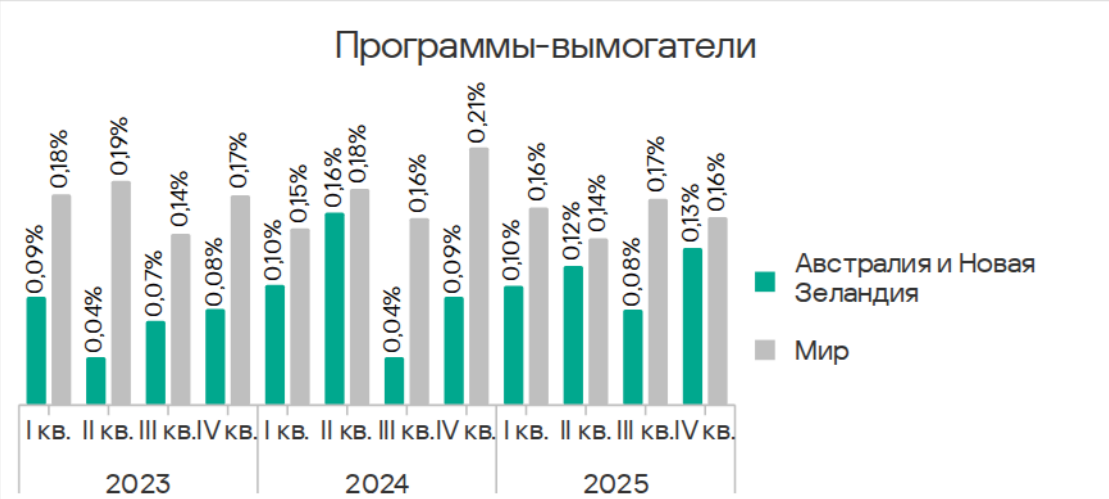
Веб-майнеры распространяются через интернет.

Из исследуемых отраслей региона показатель майнеров этой категории больше всего вырос в автоматизации зданий.

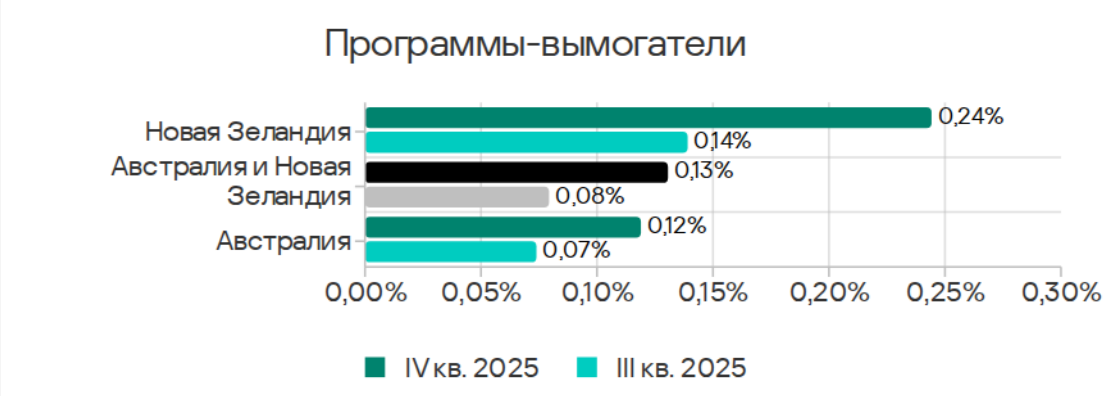
Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Австралия и Новая Зеландия занимают седьмое место в рейтинге регионов с показателем 0,13%.

Австралия и Новая Зеландия – один из трех регионов, где показатель программ-вымогателей за квартал вырос. В Австралии и Новой Зеландии значение увеличилось в 1,6 раза, регион занимает второе место по росту показателя.



Доля компьютеров АСУ, на которых блокируются программы-вымогатели, за квартал заметно выросла в обеих странах региона. Показатель выше в Новой Зеландии.

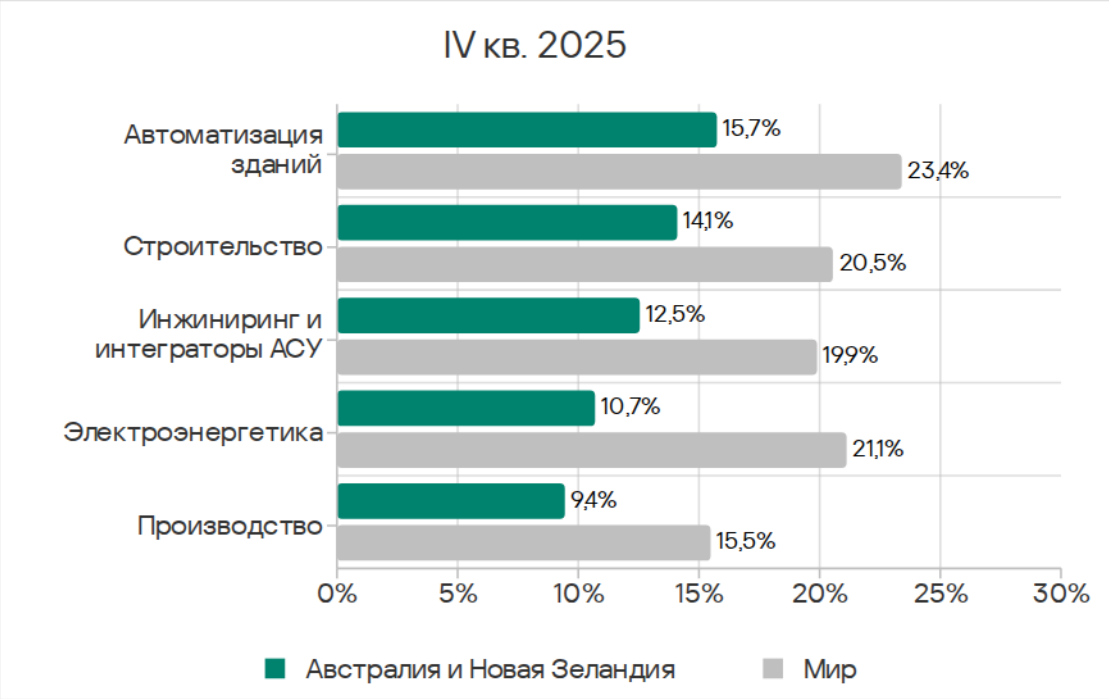


Источники программ-вымогателей в регионе — интернет и электронная почта.

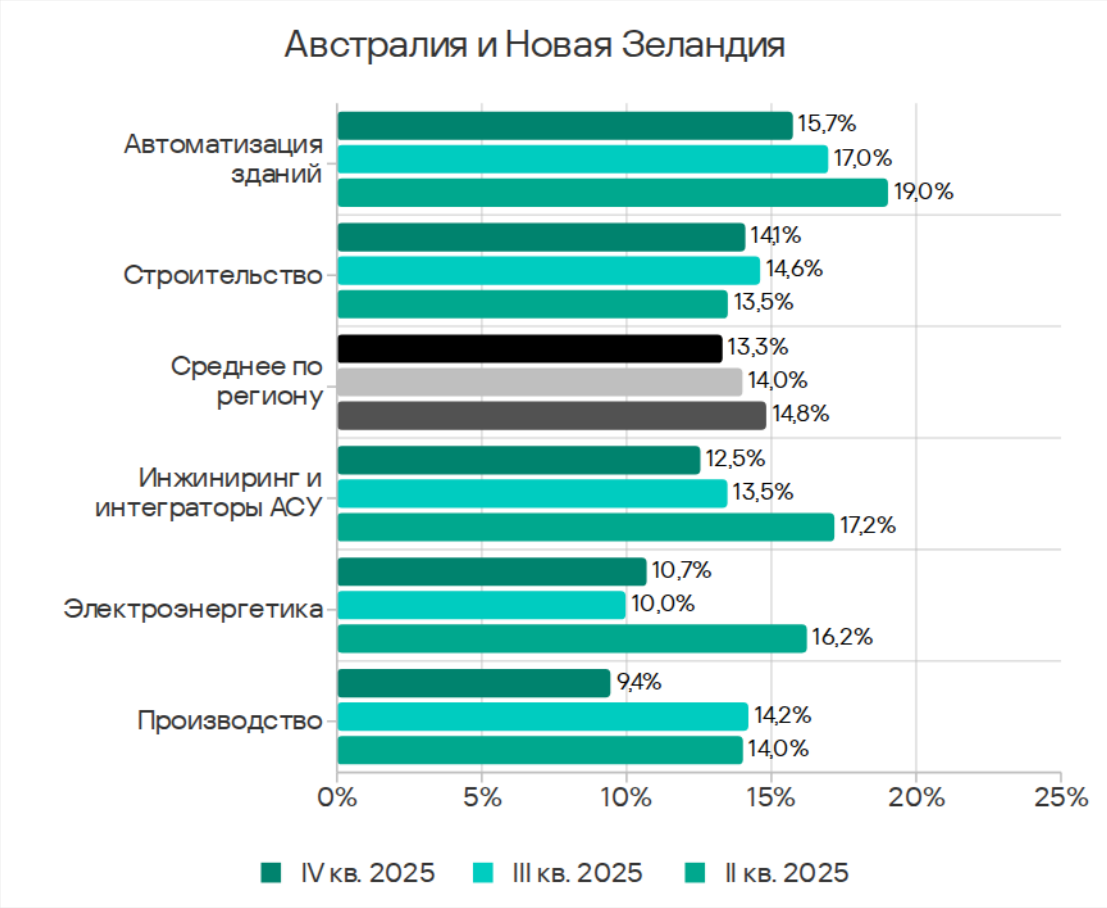
Из исследуемых отраслей региона показатель программ-вымогателей увеличился только в строительстве и автоматизации зданий.

Отрасли

Среди рассмотренных в отчете отраслей в Австралии и Новой Зеландии чаще всего встречается с угрозами автоматизация зданий. Показатели всех исследуемых отраслей в регионе значительно меньше мировых.

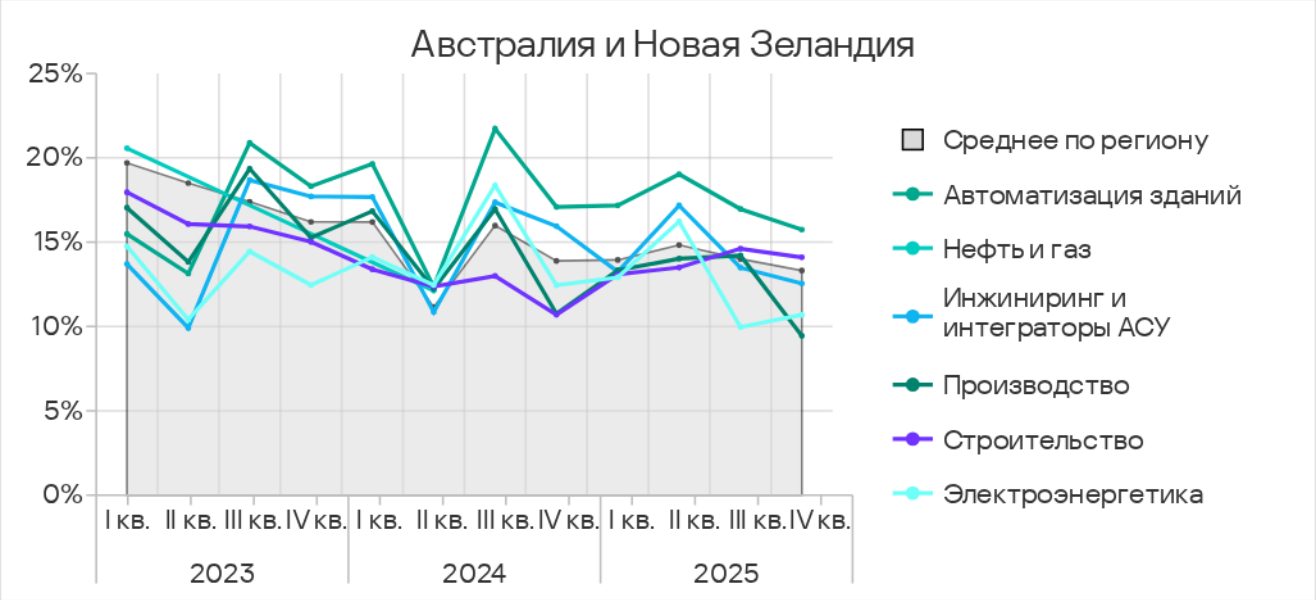


В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, из всех рассматриваемых отраслей увеличилась только в электроэнергетической отрасли.



Показатель автоматизации зданий превышают среднее для региона значение.

Показатель строительной отрасли последние два квартала также выше региональных. В то же время значение в отрасли инжиниринг и интеграторы АСУ опустилось ниже региональных показателей.



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

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

Отрасль / Источник угрозы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Строительство	Производство	Показатель категории в регионе
Интернет	7,92%	7,65%	4,91%	8,39%	5,81%	7,57%
Почтовые клиенты	4,09%	1,39%	1,45%	2,49%	1,21%	2,14%
Съемные носители	—	0,03%	—	0,05%	—	0,05%
Сетевые папки	—	—	—	0,05%	—	0,02%
Показатель отрасли в регионе	15,74%	12,55%	10,69%	14,10%	9,44%	

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

Отрасль / Тип угрозы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	2,02%	1,81%	2,02%	1,89%	1,69%	2,00%
Вредоносные скрипты и фишинговые страницы	8,31%	5,52%	4,05%	7,51%	4,12%	6,32%
Вредоносные документы (MSOffice+PDF)	1,76%	1,10%	1,45%	0,88%	0,73%	1,08%
Троянцы-шпионы, бэкдоры и кейлоггеры	2,73%	1,45%	1,16%	1,15%	1,21%	1,54%
Программы-вымогатели	0,26%	0,06%	—	0,05%	0,24%	0,13%
Майнеры — исполняемые файлы для ОС Windows	0,48%	0,16%	—	0,05%	—	0,20%
Веб-майнеры, выполняемые в браузерах	0,26%	0,16%	—	0,05%	—	0,15%
Вредоносные программы для AutoCAD	—	—	—	0,09%	—	0,03%
Черви (Worm)	0,88%	0,23%	0,29%	0,18%	0,24%	0,38%
Вирусы (Virus)	0,26%	0,03%	—	0,14%	—	0,15%
Показатель отрасли в регионе	15,74%	12,55%	10,69%	14,10%	9,44%	

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

В рейтингах регионов по показателям угроз различных категорий в отраслях самые высокие позиции у Австралии и Новой Зеландии в автоматизации зданий по показателям майнеров обеих категорий – пятое место в соответствующих рейтингах.

В регионе автоматизация зданий лидирует среди исследуемых отраслей по показателям угроз всех категорий, кроме ресурсов в интернете из списка запрещенных и вредоносных программ для AutoCAD.

Автоматизация зданий занимает первое место среди отраслей региона по росту в четвертом квартале 2025 года показателей майнеров, это одна из двух отраслей, где вырос показатель программ-вымогателей (вторая – строительство), и единственная отрасль, где увеличился показатель червей.

Автоматизация зданий

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

Среди отраслей в регионе автоматизация зданий занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах и сетевых папках;
- третье место по показателю угроз на съемных носителях;
- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы всех категорий, кроме ресурсов в интернете из списка запрещенных и вредоносных программ для AutoCAD;
- второе место по показателю ресурсов в интернете из списка запрещенных.

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 отраслей в регионах строительство занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях;
- третье место по показателям угроз из интернета, почтовых клиентов и в сетевых папках;
- первое место по показателю вредоносных программ для AutoCAD, это единственная отрасль в регионе, где были заблокированы такие угрозы;
- второе место по показателям категорий вредоносные скрипты и фишинговые страницы и вирусы;
- третье место по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: ресурсы в интернете

из списка запрещенных, программы-вымогатели и 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:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: шпионские программы, программы-вымогатели и майнеры обеих категорий;
- третье место по показателю угроз следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы, черви и вирусы.

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 отраслей в регионе электроэнергетика занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета и на съемных носителях;
- второе место по показателям угроз в почтовых клиентах и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных;
- второе место по показателям вредоносных документов и червей;
- третье место по показателю шпионского ПО.

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