Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Статистика за второе полугодие 2020

25.03.2021

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 телеметрия содержит только те типы и категории информации, которые описаны в соответствующем Соглашении KSN. Эти данные в значительной мере не только помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT[1].

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

Методика подготовки статистики

Статистические данные, представленные в отчете, получены с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky ICS CERT относит к технологической инфраструктуре организаций. В эту группу входят компьютеры, работающие на операционных системах Windows и выполняющие одну или несколько функций:

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

Атакованными мы считаем те компьютеры, на которых в течение отчетного периода защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете процента машин, на которых было предотвращено заражение вредоносным ПО, используется количество компьютеров, атакованных в течение отчетного периода, по отношению ко всем компьютерам из нашей выборки, с которых в течение отчетного периода мы получали обезличенную информацию.

2020 — цифры

Показатель	H1 2020	H2 2020	2020
Процент атакованных компьютеров АСУ в мире	32,6%	33,42%	38,55%
Процент атакованных компьютеров АСУ в регионах			
Северная Европа	10,1%	11,5%	12,3%
Западная Европа	15,1%	14,8%	17,6%
Австралия	16,3%	17,0%	18,9%
США и Канада	17,2%	16,5%	19,6%
Восточная Европа	26,4%	28,0%	30,5%
Южная Европа	27,6%	29,6%	33,1%
Латинская Америка	33,6%	34,3%	38,8%
Россия	32,2%	34,6%	39,5%
Ближний Восток	34,0%	34,6%	40,2%
Восточная Азия	42,9%	41,8%	46,3%
Южная Азия	38,8%	41,3%	47,0%
Центральная Азия	43,7%	43,9%	48,8%
Африка	45,6%	46,4%	51,2%
Юго-Восточная Азия	49,8%	47,5%	53,9%
Основные источники угроз в мире			
Интернет	16,7%	16,7%	20,5%
Съемные носители	5,8%	5,4%	7,0%
Почтовые клиенты	3,4%	4,1%	4,4%

2020 — особенности

1. **Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, перестал снижаться**

   Со второй половины 2019 года мы наблюдали уменьшение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, по полугодиям — как среди АСУ, так и в корпоративной и персональной средах. Во втором полугодии 2020 года уменьшения этого показателя не отмечено.

   - **В мире** по итогам второго полугодия процент атакованных компьютеров АСУ **вырос по сравнению с первым полугодием на 0,85 п.п.** и составил 33,4%.

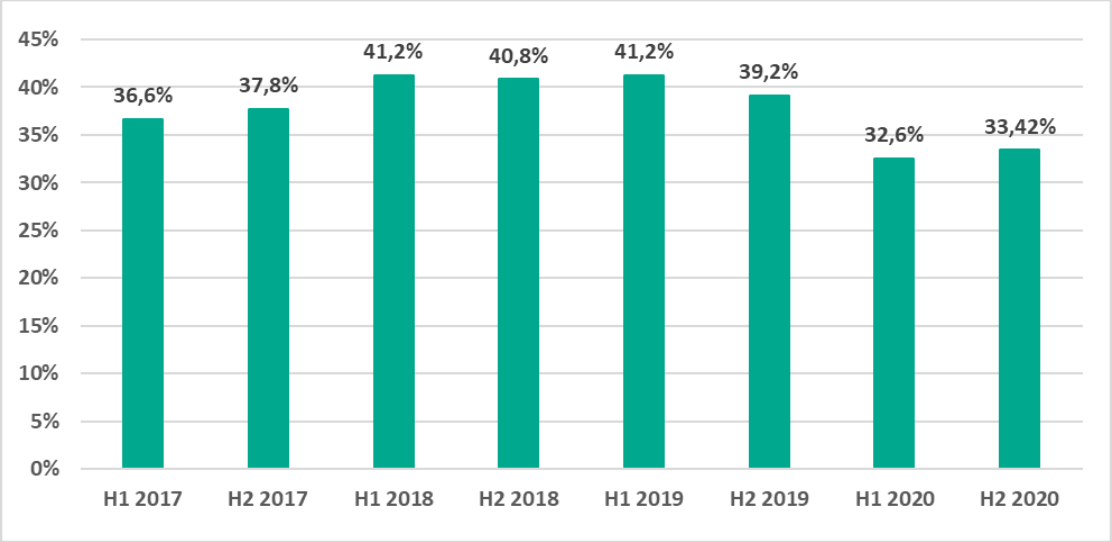


Рис.1. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по полугодиям 2017 — 2020

   - **В 62% стран процент атакованных компьютеров АСУ вырос.**

     Во втором полугодии 2020 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась по отношению к первому полугодию в 62% стран. Для сравнения — в 2019 аналогичный показатель составил 7% стран, таким же он был и в первом полугодии 2020 по отношению ко второму полугодию 2019.

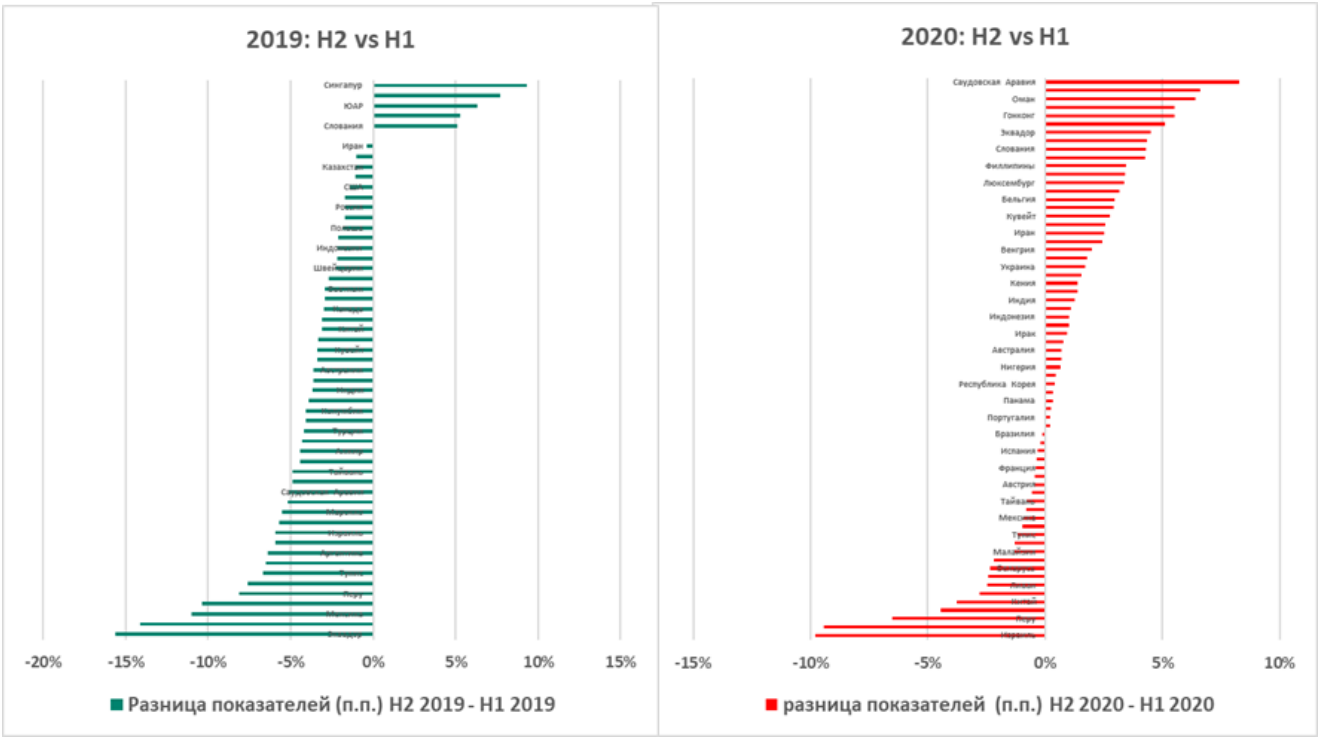


Рис. 2. Изменение процента атакованных компьютеров в странах мира (п.п.) во втором полугодии по сравнению с первым полугодием, 2019 и 2020

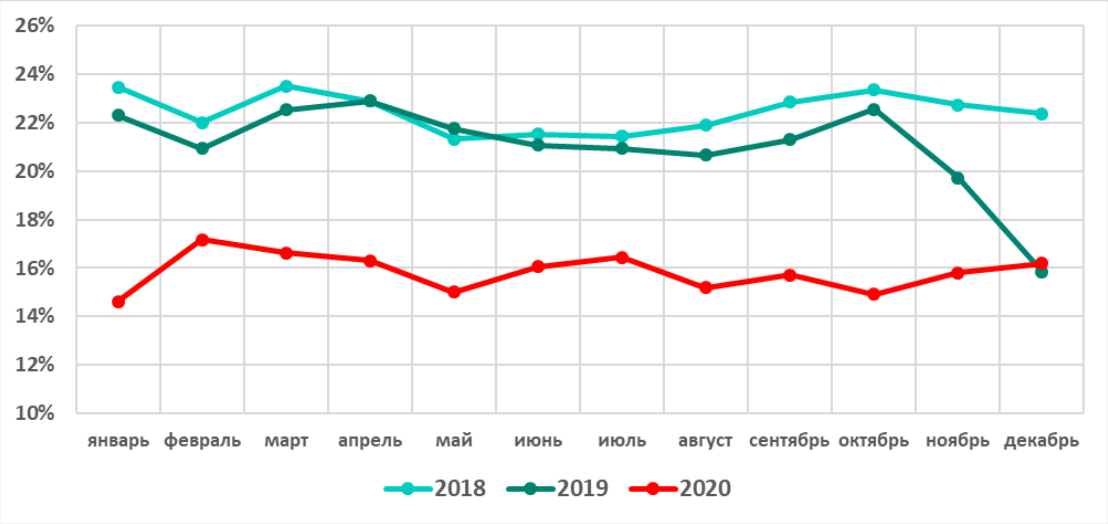
При этом максимальный рост показателя в стране составил 8,2 п.п. (в Саудовской Аравии), а в большинстве стран не превысил 4 п.п., поэтому по итогам полугодия изменения в среднем по миру не были значительными.

2. **Отсутствовали сезонные колебания, характерные для прошлых лет**

В предыдущие годы процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, был максимальным в марте/апреле и октябре, а между этими месяцами показатель в динамике «прогибался».

В 2020 году динамика этого показателя была иной. С максимума февраля он падал почти до минимума в мае. В первые два месяца лета он рос, достигая в июле значения, близкого к максимуму. В октябре же процент атакованных компьютеров АСУ был одним из самых низких.

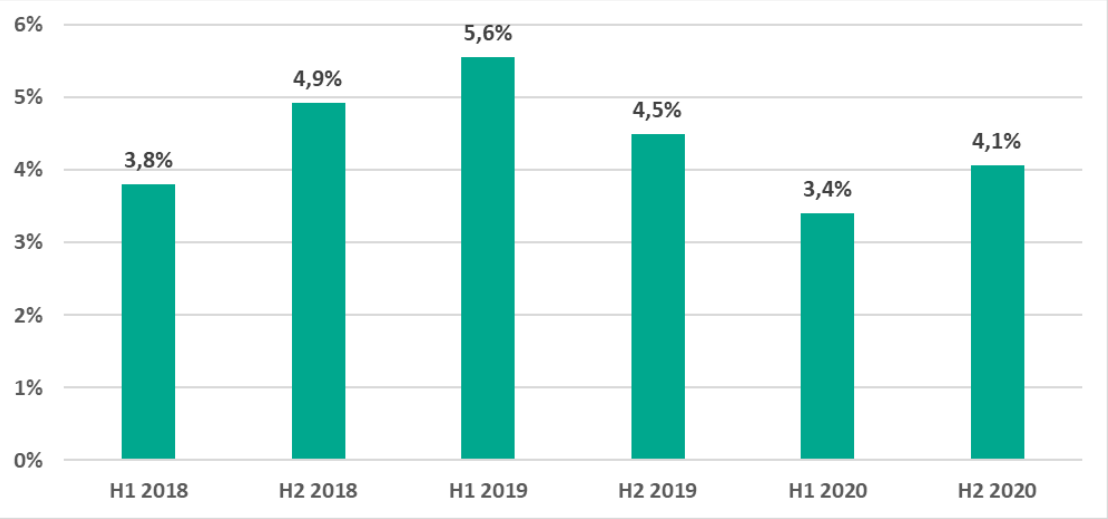
Рис. 3. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам 2017, 2018, 2019, 2020



3. Увеличился процент компьютеров АСУ, на которых были заблокированы вредоносные вложения в электронных письмах

- **В мире** во втором полугодии 2020 по сравнению с первым полугодием процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, увеличился на 0,7 п.п.

Рис. 4. Процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения



- Этот показатель вырос во всех регионах, за исключением Восточной Азии, США и Канады, Западной Европы и России.
- В 73,4% всех стран во втором полугодии 2020 по сравнению с первым полугодием увеличился процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения. Это второе больше аналогичного показателя 2019 года (23,6%).

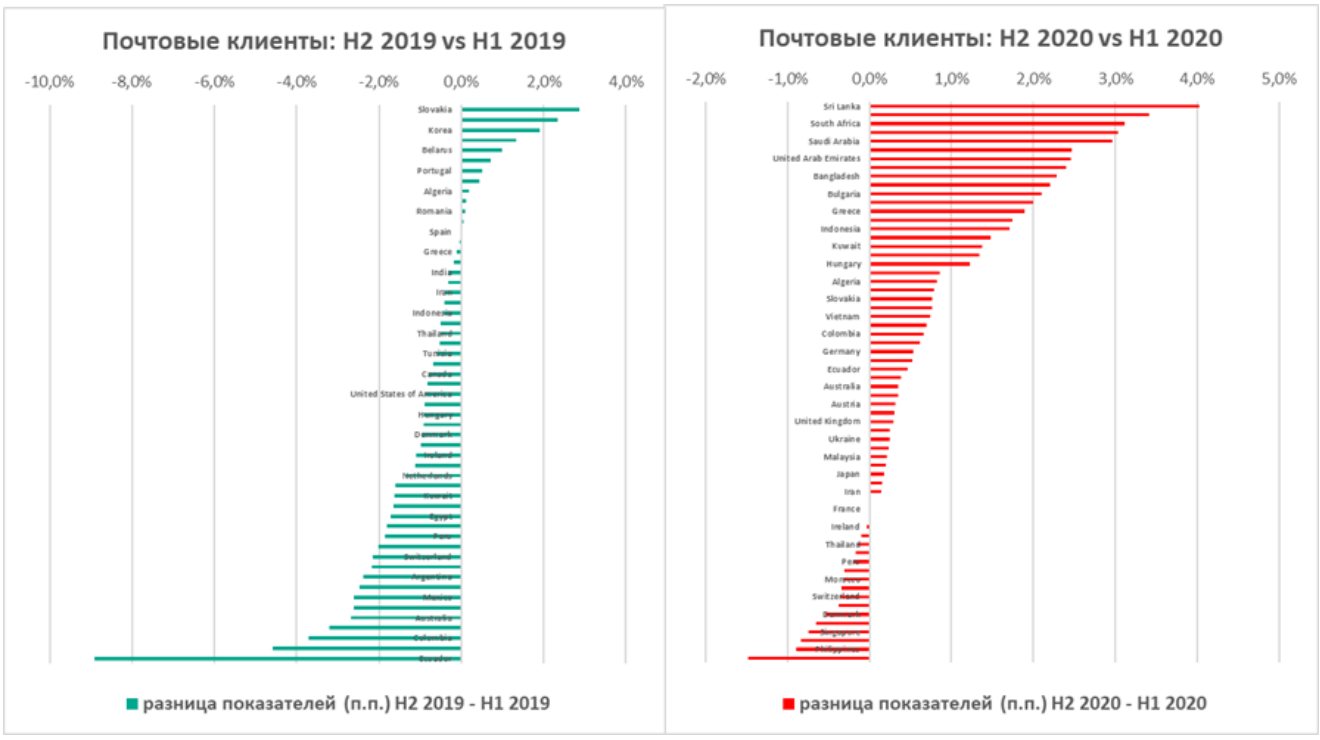


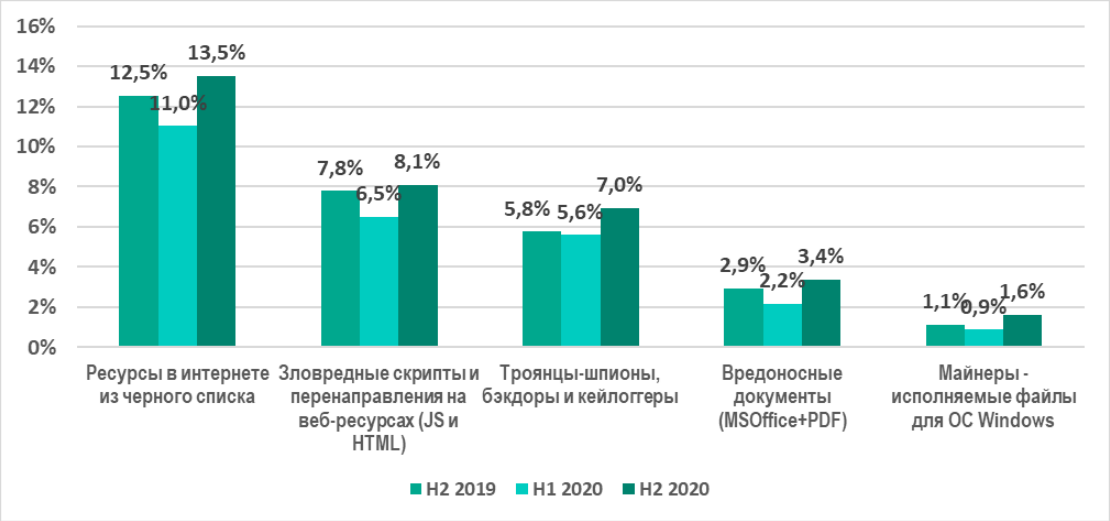
Рис. 5. Изменение во втором полугодии по сравнению с первым полугодием процента компьютеров АСУ (п.п.), на которых были заблокированы вредоносные почтовые вложения, страны и территории, 2019 и 2020

4. **Вырос процент компьютеров АСУ, на которых были заблокированы угрозы, распространяемые через интернет и электронную почту, а также программы-шпионы и майнеры**

   - вредоносные объекты из интернета — веб-ресурсы, задействованные в распространении или управлении вредоносным ПО (+2,5 п.п), и зловредные скрипты и перенаправления на веб-ресурсах (JS и Html) (+1,6 п.п).
   - типичные угрозы, распространяемы по электронной почте (+1,2 п.п.). — вредоносные документы MSOffice и PDF (+1,2 п.п.).
   - шпионское ПО (+ 1,4 п.п.) — троянцы-шпионы, бэкдоры и кейлоггеры.
   - майнеры (+ 0,7 п.п.) — исполняемые файлы для ОС Windows.

   По всем этим угрозам показатели второго полугодия 2020 превысили аналогичные результаты не только первой половины 2020, но и второго полугодия 2019 года.

Рис. 6. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных типов, H2 2019 — H2 2020



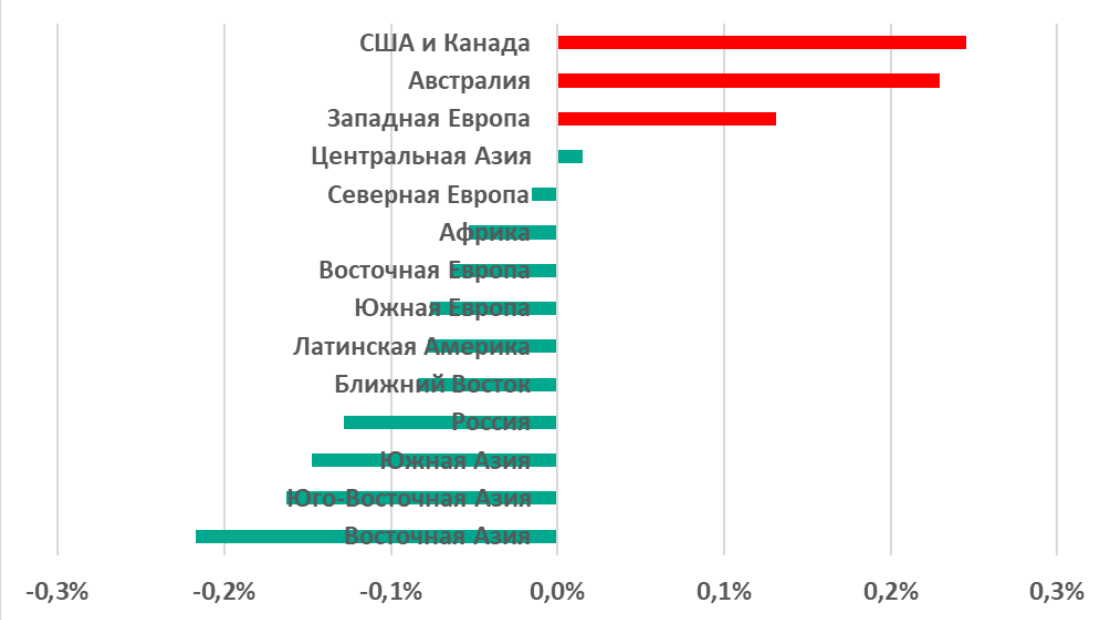
5. **В развитых странах увеличился процент компьютеров АСУ, атакованных программами-вымогателями**

В мире процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, с 0,63% в первом полугодии уменьшился до 0,49% во втором.

В то же время в регионах с развитыми странами этот показатель увеличился:

- в США и Канаде — на 0,25 п.п.
- в Австралии — на 0,23 п.п.
- в Западной Европе — на 0,13 п.п.

Рис. 7. Изменение во втором полугодии по сравнению с первым полугодием процента компьютеров АСУ (п.п.), на которых были заблокированы вредоносные программы-вымогатели



Влияние пандемии COVID-19

В отчёте за H1 2020 мы уже оценивали вклад пандемии COVID-19 в наблюдаемые нами изменения поверхности атаки и ландшафта угроз промышленных предприятий и систем промышленной автоматизации. Во втором полугодии мы продолжили наши наблюдения и обнаружили ещё несколько тенденций, которые, по нашему мнению, могут быть обусловлены влиянием обстоятельств, так или иначе связанных с пандемией, сопутствующей реакцией государств, отдельных организаций и людей.

Изменение сезонных колебаний процента атакованных компьютеров

Как видно на Рис. 3, в предыдущие годы процент атакованных компьютеров АСУ существенно снижался в летние месяцы и в декабре. Вероятно, это снижение обусловлено периодами традиционных отпусков — заражённая флэшка сама себя не перенесёт с одного компьютера на другой, и кликнуть по ссылке, ведущей на фишинговый сайт, рабочая станция инженера без участия самого инженера не сможет.

В 2020 году ситуация, однако, заметно изменилась — значительных сезонных колебаний процента атакованных компьютеров мы более не наблюдали. Вероятно, причина кроется в изменении графиков отпусков сотрудников организаций — многие решили отказаться от отпусков во время локдауна, ограничений на перемещение и закрытых границ.

Атаки на сервисы удалённых подключений RDP

Другим последствием пандемии стал заметный рост процента ICS-компьютеров, доступных удалённо по протоколу RDP.

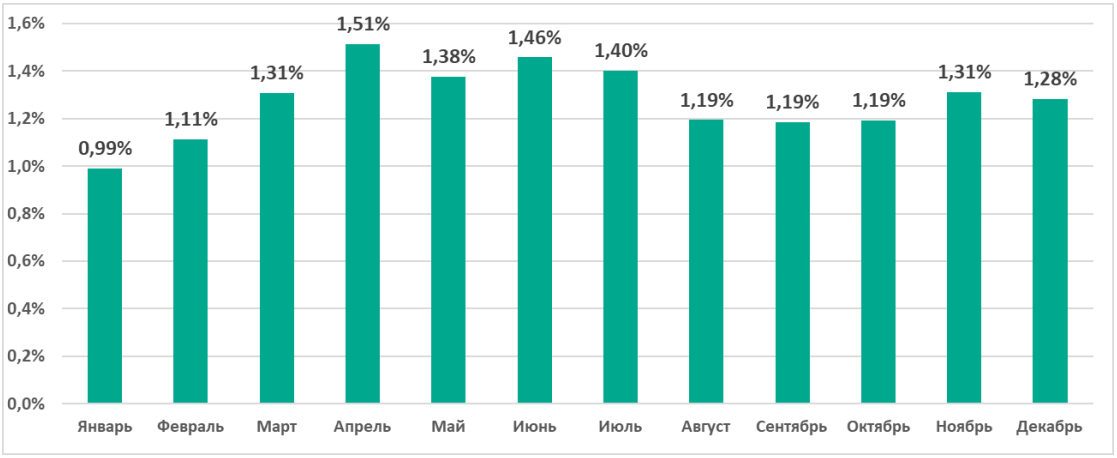


Рис. 8. Процент компьютеров АСУ, доступных по RDP, по месяцам 2020

Как видно на графике, этот показатель непрерывно рос с января по апрель. Тогда многие организации решали задачи по обеспечению работы в условиях надвигающегося и наступившего локдауна. Далее после некоторых колебаний, этот показатель немного снизился и стабилизировался на уровне, несколько более высоком, чем до начала пандемии.

Имеющихся у нас данных недостаточно, чтобы сделать вывод о том, к какой части этих компьютеров доступ возможен только из технологической сети предприятия, к какой — из корпоративного сегмента, а к какой, возможно, даже и извне периметра организации. Тем не менее, можем с уверенностью сказать, что увеличение доступности ICS-компьютеров не могло не сказаться на изменении поверхности атаки. Чем, по всей видимости, не преминули воспользоваться злоумышленники — это хорошо видно на следующем графике, отображающем процент компьютеров АСУ, на которых были обнаружены и предотвращены атаки типа подбора данных аутентификации (brute force) к сервису RDP:

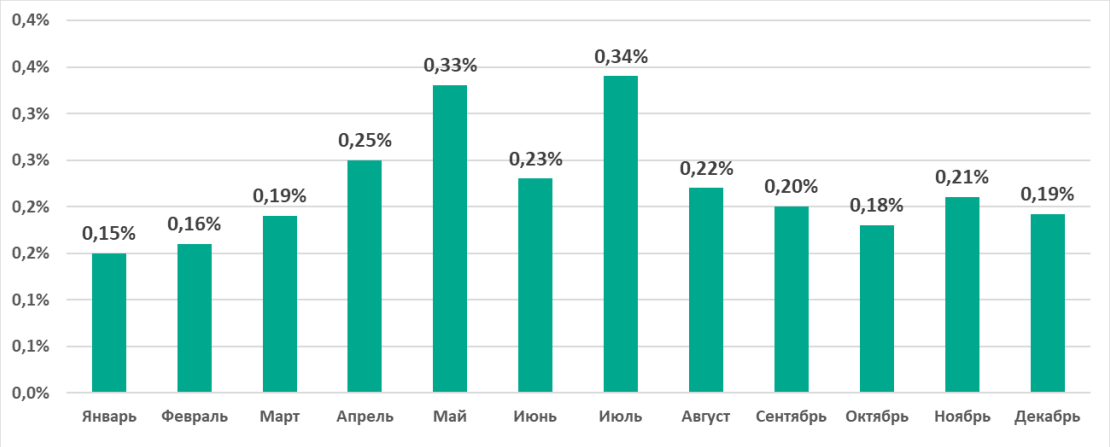


Рис. 9. Процент компьютеров АСУ, на которых фиксировались попытки подбора паролей к RDP, по месяцам 2020

Нетрудно заметить некую синхронность изменения этих двух показателей: процент атакованных RDP следует за процентом компьютеров АСУ, доступных по RDP, на протяжении почти всего года (с января по октябрь) с опозданием примерно в один месяц — и догоняет его (изменения синхронизируются) в октябре-ноябре.

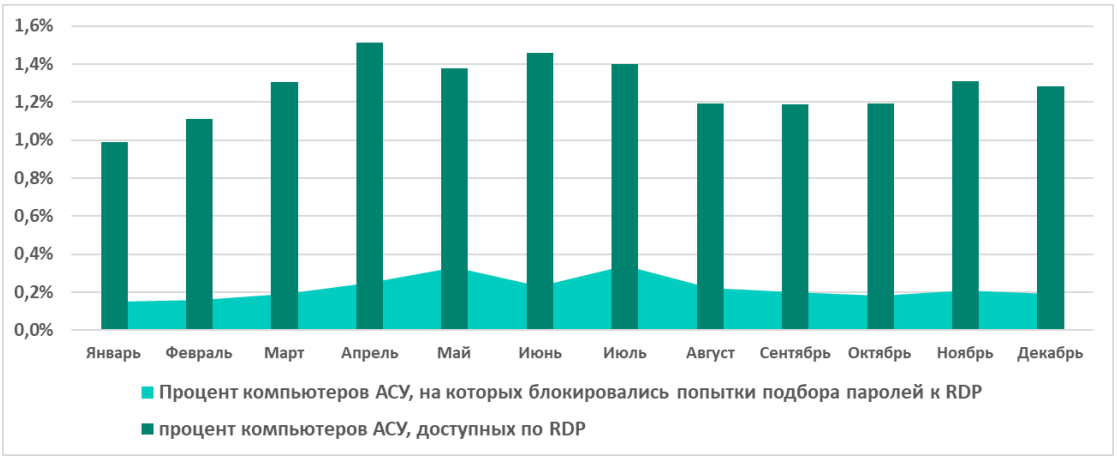


Рис. 10. Процент компьютеров АСУ, на которых фиксировались попытки подбора паролей к RDP и процент компьютеров АСУ, доступных по RDP

О чем говорит месячное «запаздывание» процента атакованных компьютеров — о скорости распространения атак внутри сети организации, или о скорости реакции злоумышленников на изменение ландшафта возможностей (поверхности атаки) — мы можем пока только гадать.

Изменение приоритетов вымогателей

Еще одно из вероятных последствий пандемии можно обнаружить, анализируя динамику атак вымогателей на промышленные предприятия в различных регионах, о которой мы косвенно можем судить по проценту атакованных вымогательским вредоносным ПО (ransomware) компьютеров АСУ. Как видно на рис. 7 и на графике ниже, этот показатель снизился во втором полугодии во всех регионах мира, за исключением Северной Америки, Западной Европы и Австралии, где он не только не снизился, но и (в разы!) вырос.

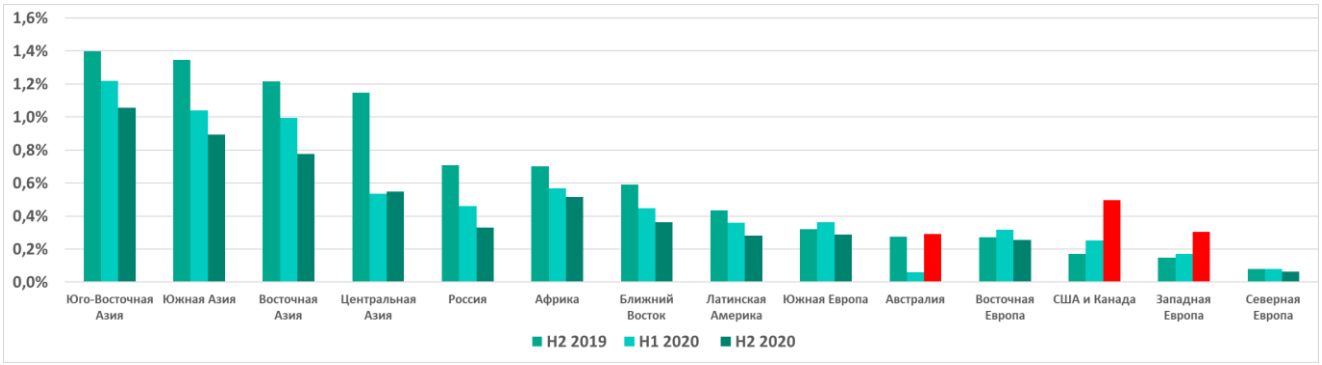


Рис. 11. Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, H2 2019 — H2 2020

На наш взгляд, эта странная динамика может свидетельствовать о реакции злоумышленников на экономические последствия пандемии. В странах, «платёжеспособность» организаций в которых снизилась в результате

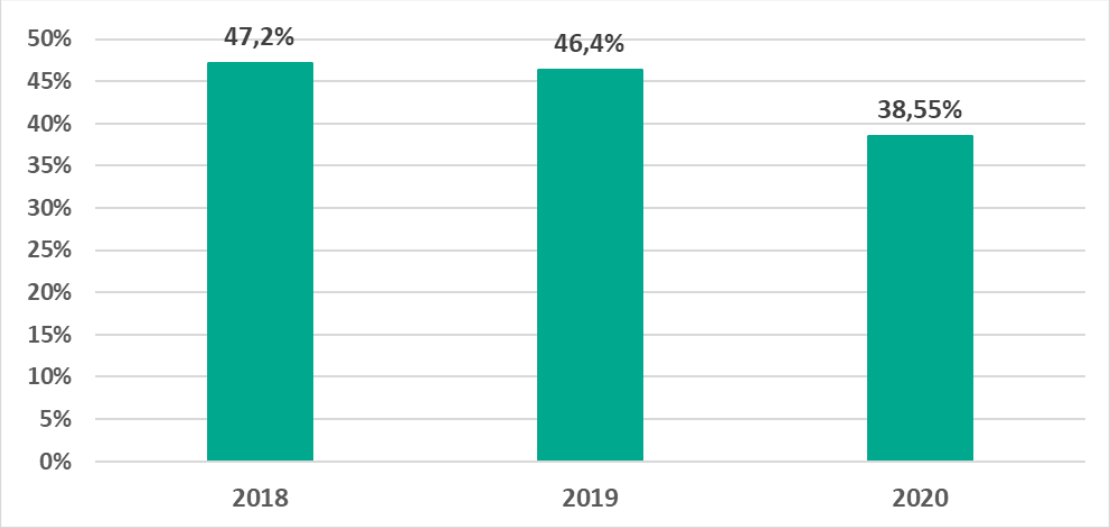
пандемии, атак на промышленные предприятия стало меньше (процент атакованных компьютеров АСУ упал). В тех странах, где сосредоточены более финансово стабильные и всё ещё способные платить выкуп промышленные организации, активность злоумышленников увеличилась (процент атакованных компьютеров АСУ резко вырос). Можно предположить, что наблюдаемые нами изменения обусловлены, в том числе, сдвигом фокуса некоторых группировок при поиске жертв в сторону организаций в более экономически устойчивых странах.

Основная статистика

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

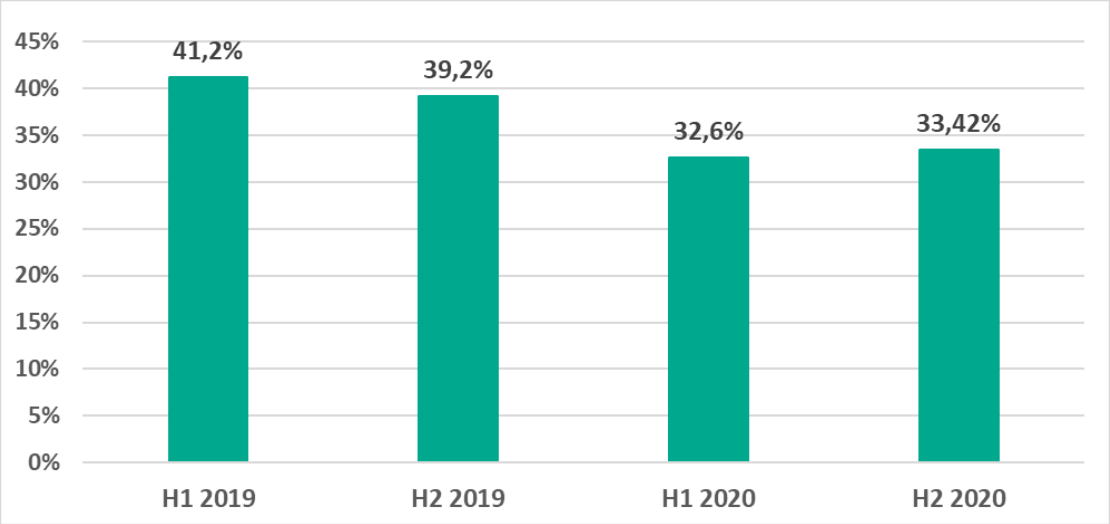
По итогам 2020 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, составил 38,6% — на 7,8 п.п. меньше, чем в 2019 году.

Рис. 12. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, 2018 — 2020 г.г.



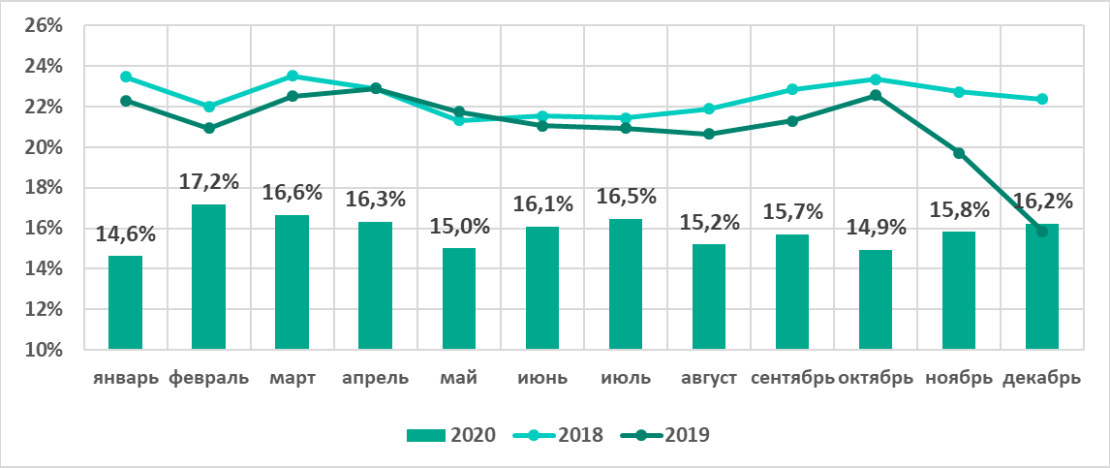
Во втором полугодии 2020 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, вырос на 0,85 п.п. по сравнению с первым полугодием 2020 и составил 33,4%.

Рис. 13. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по полугодиям H1 2019 — H2 2020



В 2020 году динамика процента атакованных компьютеров АСУ по месяцам была довольно ровной, ярко выраженная тенденция снижения показателя отсутствовала. Также не было отмечено сезонных колебаний, которые мы наблюдали в предыдущие годы.

Рис. 14. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам 2018, 2019, 2020

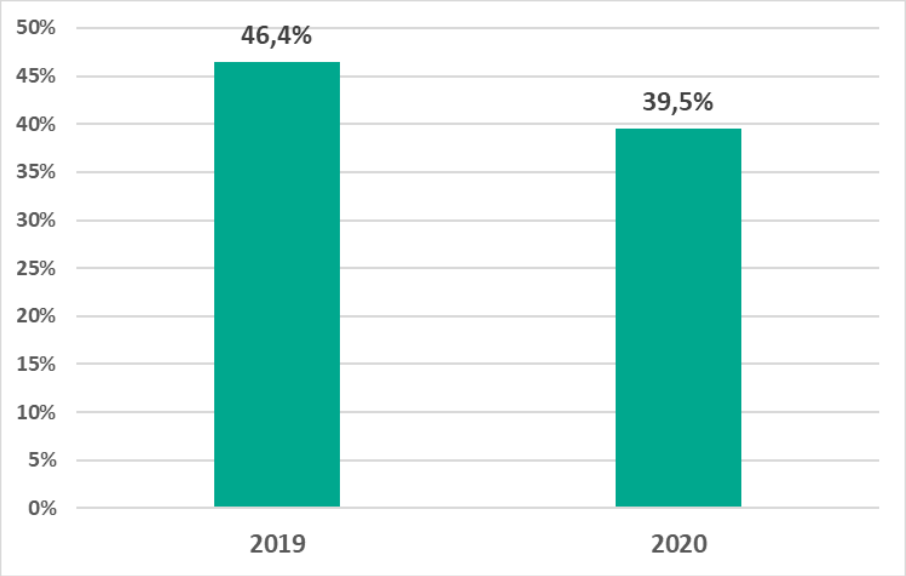


Минимальные значения были зарегистрированы в январе (14,6%), в октябре (14,9%) и в мае (15,0%). Максимальные — в феврале (17,2%), в марте (16,6%) и июле (16,5%).

Россия

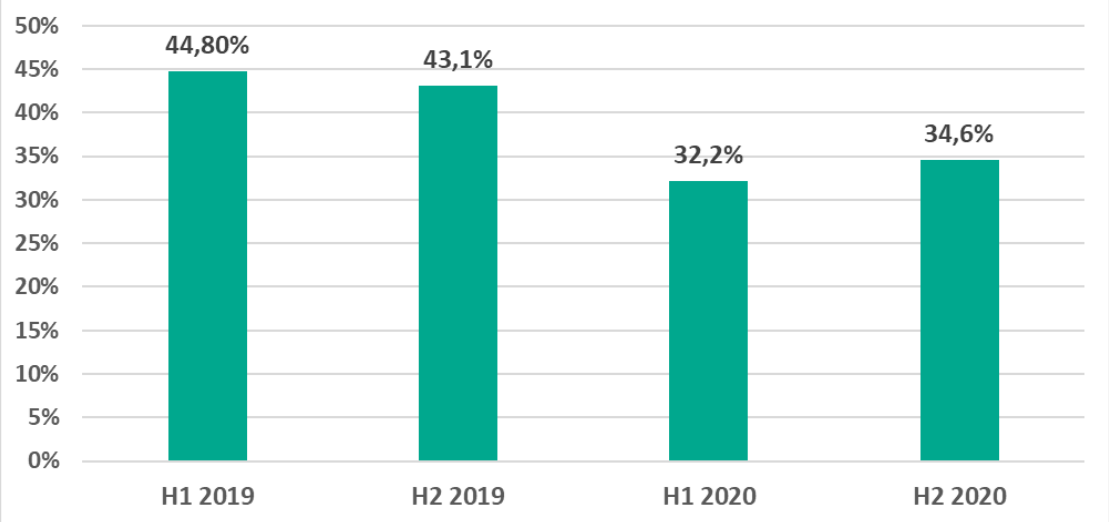
По итогам 2020 года в России вредоносные объекты были заблокированы на 39,5% компьютеров АСУ.

Рис. 15. Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



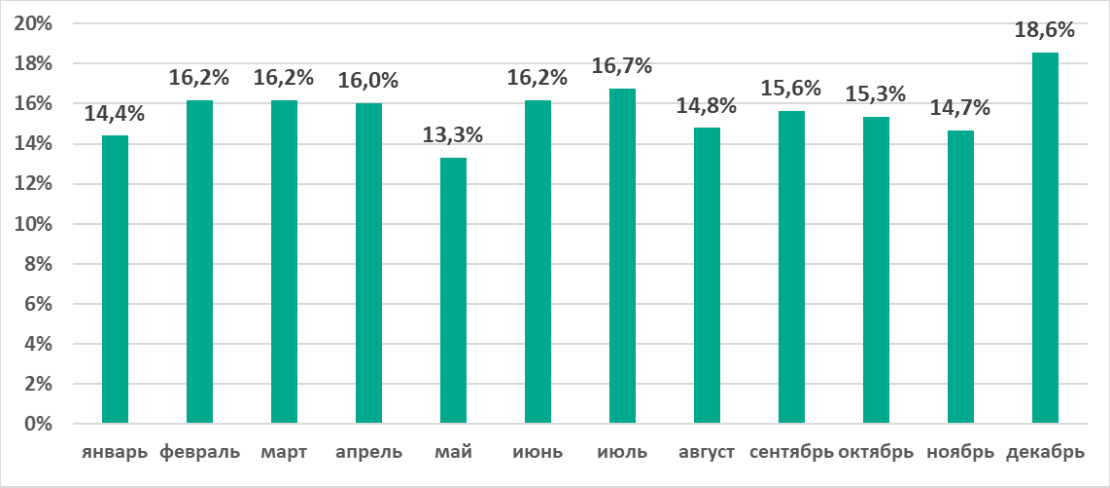
В первом полугодии этот показатель составил 32,2%, во втором — 34, 6%.

Рис. 16. Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по полугодиям 2019 — 2020



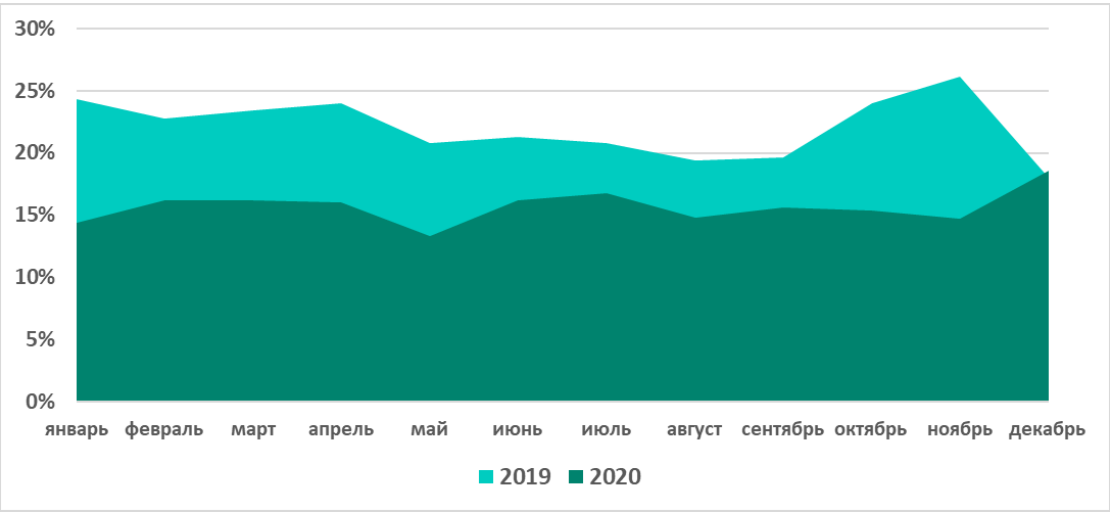
Наибольшие показатели в течение года были зафиксированы и в декабре (18,6%) и в июле (16,7%). Наименьшие — в мае (13,3%) и в январе (14,4%).

Рис. 17. Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам 2020



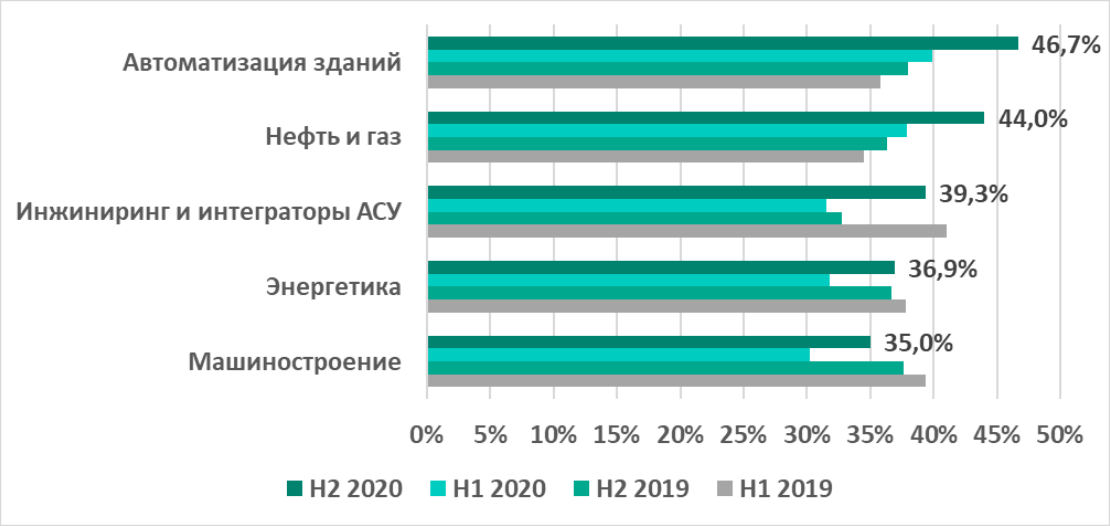
В России также отмечены изменения в сезонной динамике по сравнению с 2019 годом.

Рис. 18. Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам. 2019 vs 2020



Некоторые индустрии

Рис. 19. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых индустриях



Во втором полугодии 2020 процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, вырос во всех представленных индустриях.

Анализ ситуации в инжиниринге опубликован в отдельном отчете.

География

Регионы

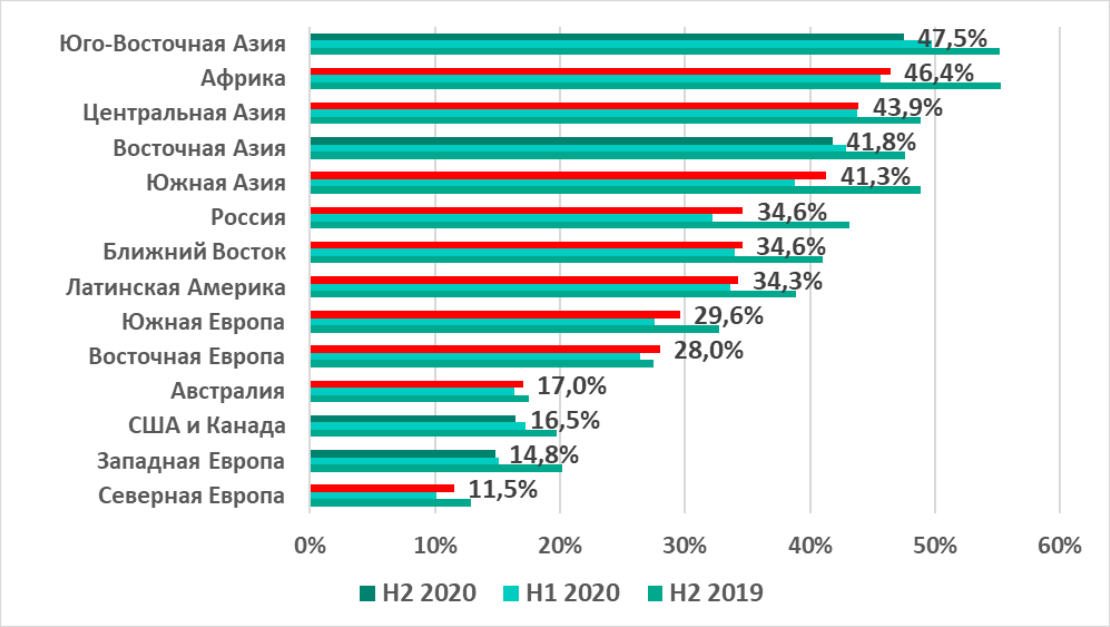
В рейтинге регионов мира по доле компьютеров АСУ, на которых была предотвращена вредоносная активность, по-прежнему лидируют регионы Азии и Африка.

В Юго-Восточной и Восточной Азии, как и в прошлые годы, процент атакованных компьютеров АСУ уменьшился по сравнению с предыдущим полугодием.

Небольшое уменьшение отмечено также в США и Канаде и Западной Европе, которые находятся в конце рейтинга.

Во всех остальных регионах мира процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, за полугодие увеличился, включая и самую благополучную по этому показателю Северную Европу.

Рис. 20. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионах мира

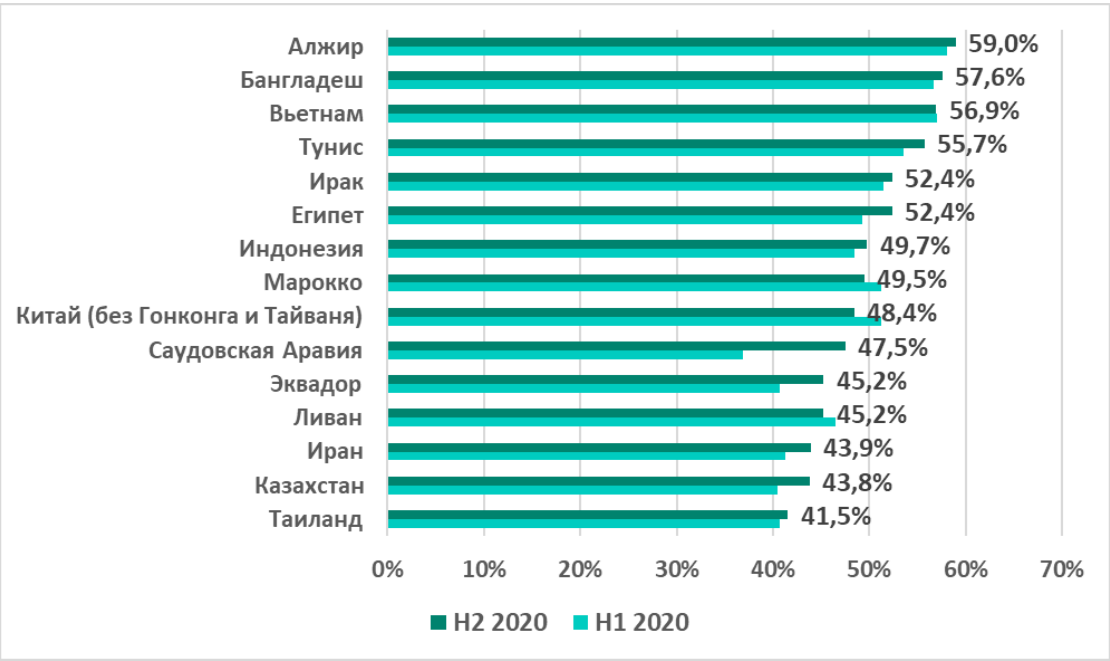


Россия прибавила 2,4 п.п. и заняла в рейтинге 6-е место — следующее после лидирующих и регионов Азии и Африки.

TOP стран

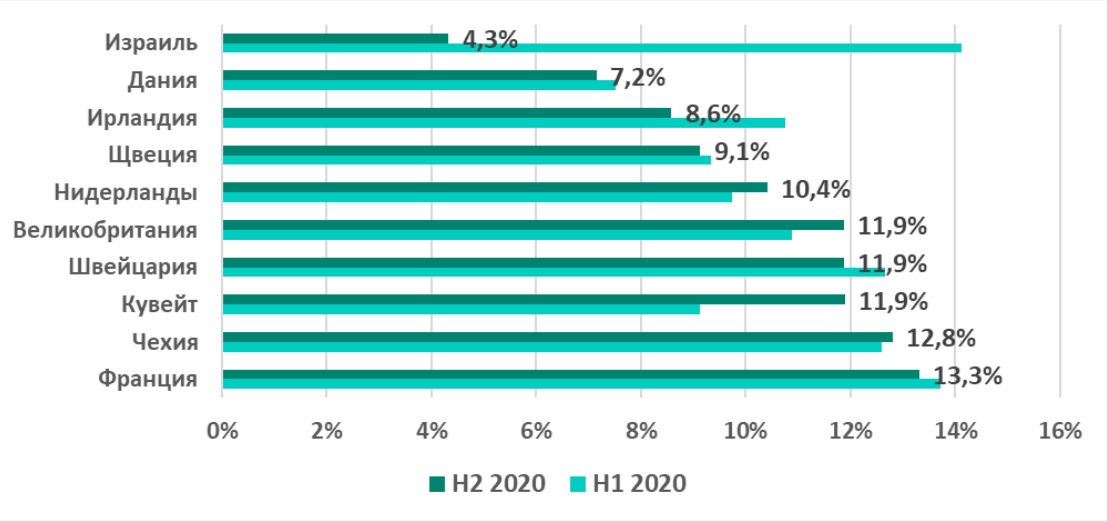
Во втором полугодии 2020 в TOP 15 стран и территорий по проценту атакованных компьютеров АСУ не попала ни одна европейская страна

Рис. 21. Топ-15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты. Второе полугодие 2020



Израиль занял первое место в списке десяти наиболее благополучных стран во втором полугодии 2020 с рекордными 4,3%.

Рис. 22. 10 стран и территорий с наименьшим процентом омпьютеров АСУ, на которых были заблокированы вредоносные объекты. Второе полугодие 2020



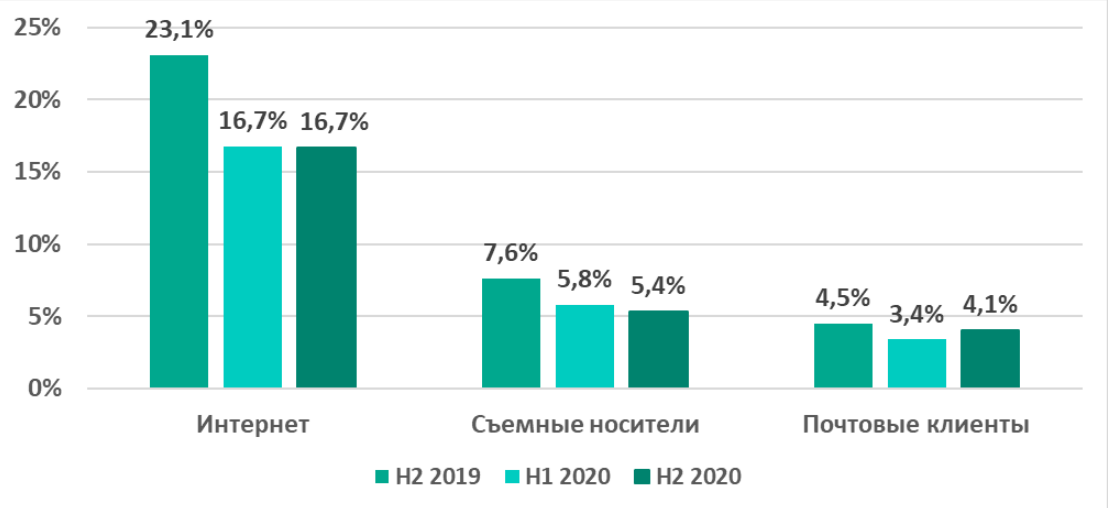
В TOP 10 стран с минимальным процентом атакованных компьютеров АСУ, как и в первом полугодии 2020, вошли Израиль и Кувейт. Остальные страны в десятке — европейские.

Основные источники угроз

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

Рис. 23. Основные источники угроз, заблокированных на компьютерах АСУ*

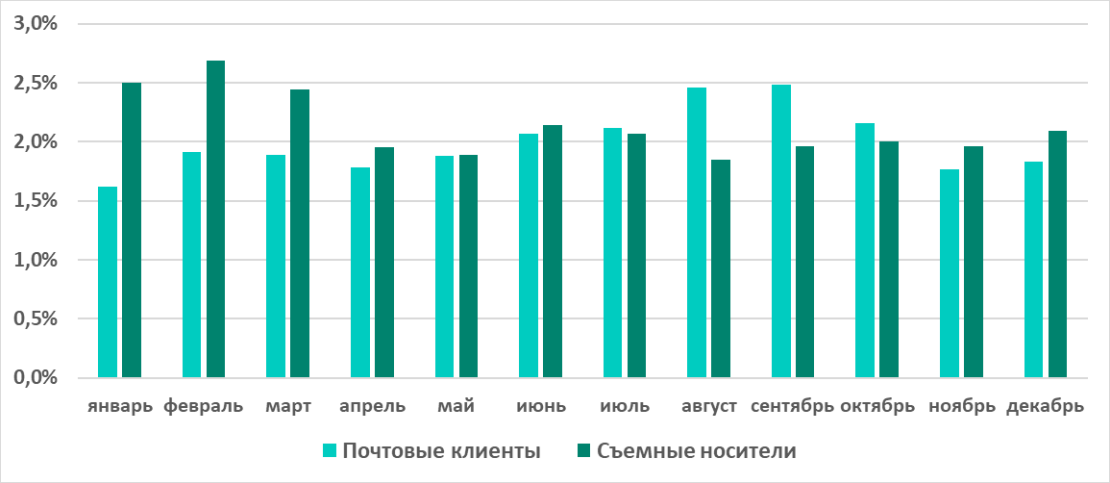
** процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников*



Во втором полугодии 2020:

- Показатели угроз из интернета не изменились.
- На 0,4 п.п. уменьшился процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей.
- На 0,7 п.п. увеличился процент компьютеров АСУ, на которых были заблокированы вредоносные вложения в электронных письмах.

Рис. 24. Процент компьютеров АСУ, на которых были вредоносные объекты из разных источников, по месяцам 2020 года



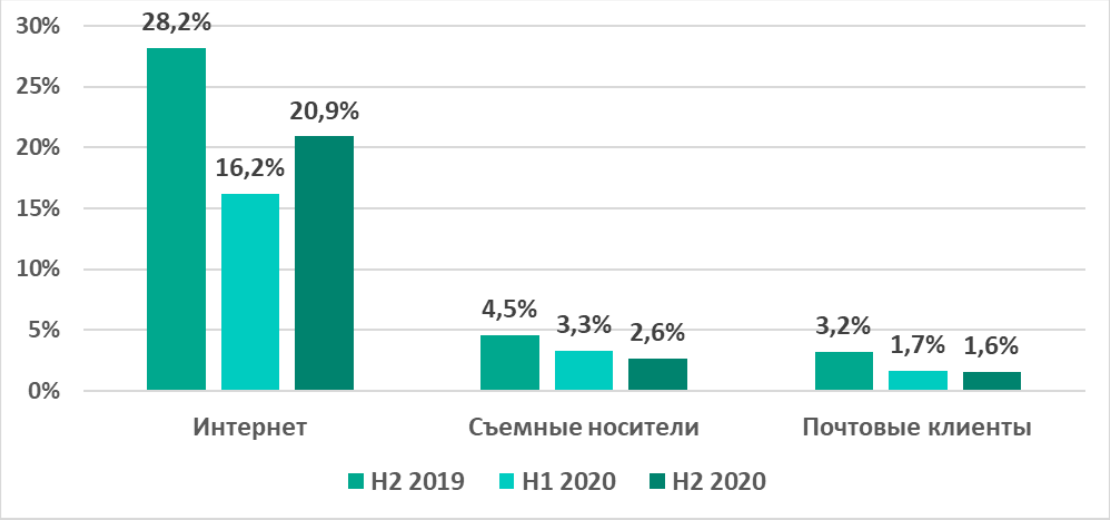
Пик угроз, заблокированных в почте, пришелся на август и сентябрь, угроз, которые были заблокированы при подключении съемных носителей, — на первый квартал 2020 года.

Россия

В России заметно (на 4,7 п.п.) вырос процент компьютеров АСУ, на которых заблокированы угрозы из интернета.

Рис. 25. Россия. Основные источники угроз, заблокированных на компьютерах АСУ*

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



Основные источники угроз: география

Во втором полугодии 2020 показатели по вредоносным почтовым вложениям превысили показатели по съемным носителям во всех регионах Европы, в США и Канаде, в Австралии и, в отличие от предыдущего полугодия, — в Латинской Америке.

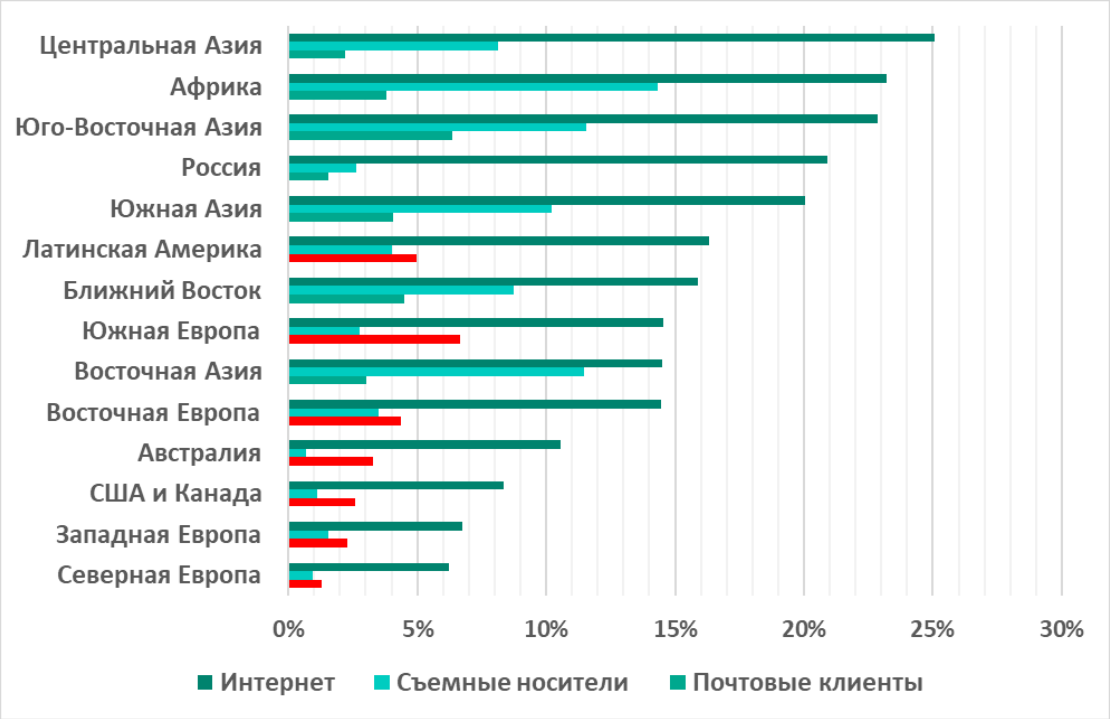


Рис. 26. Основные источники угроз, заблокированных на компьютерах АСУ*, в регионах, второе полугодие 2020

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

Как и в предыдущие годы, основным источником угроз остается интернет.

Интернет

Процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, уменьшался со второго полугодия 2019 года. Во второй половине 2020 он вырос сразу в нескольких регионах, включая Северную Европу, которая замыкает рейтинг по этому показателю.

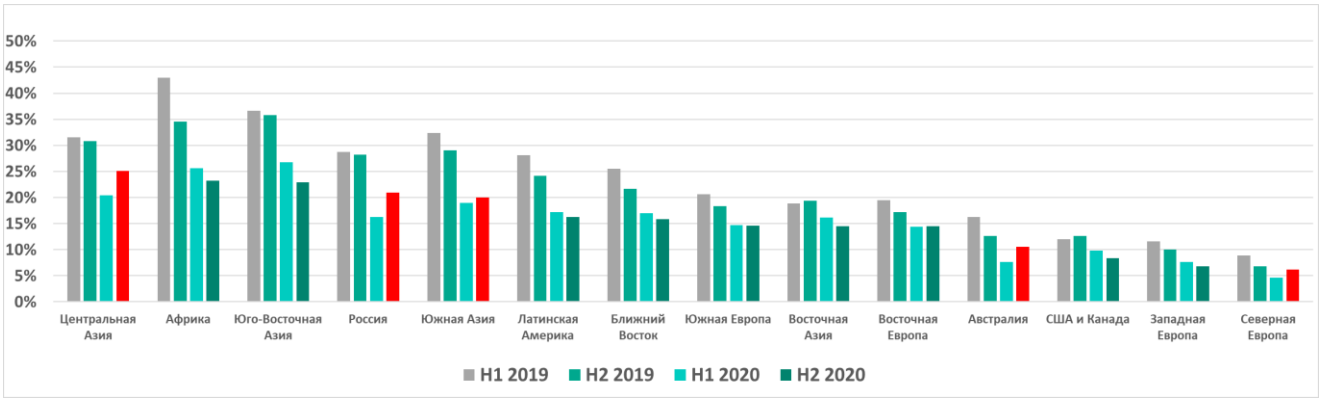
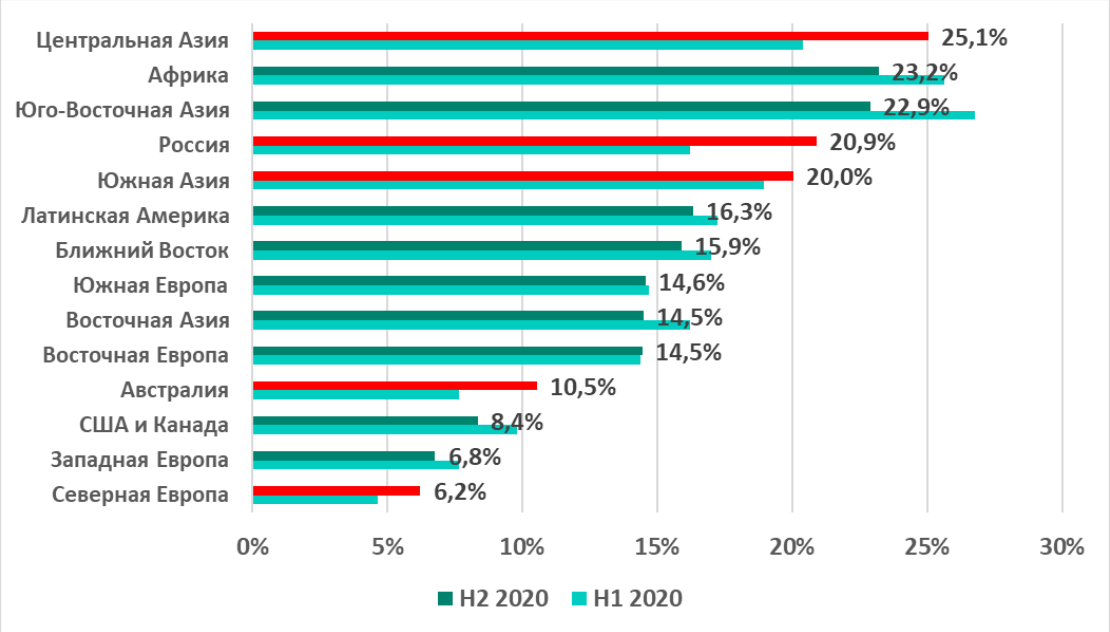


Рис. 27. Процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, по полугодиям 2019 — 2020

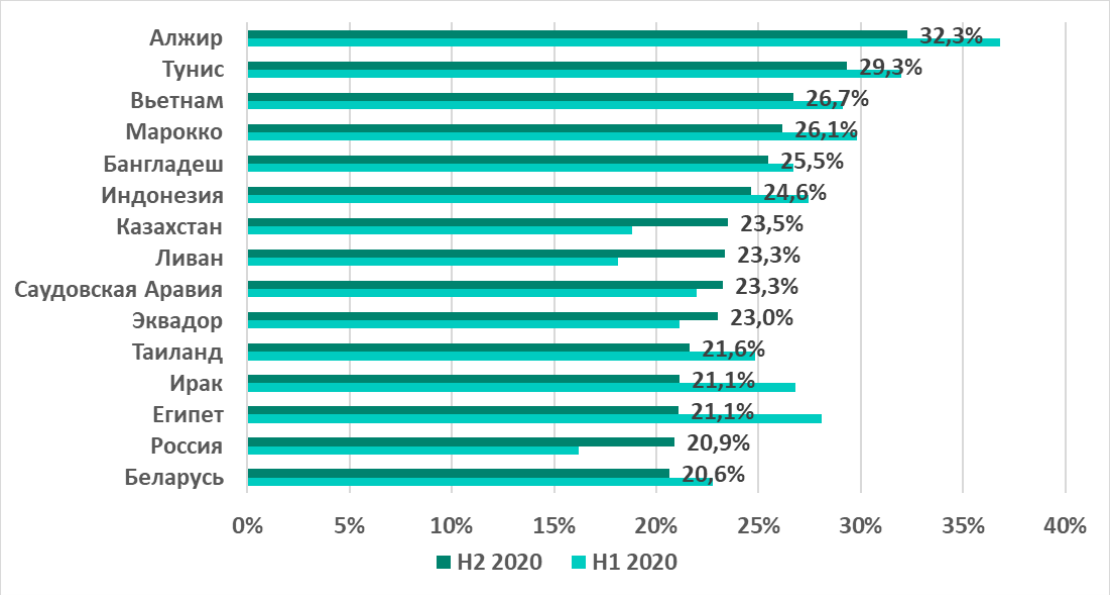
Рис. 28. Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2020



Во втором полугодии 2020 года процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, вырос в 39% стран. Аналогичный показатель второго полугодия 2019 — 14,5%.

Максимальный прирост зафиксирован в Казахстане и в России — на 4,7 п.п. В результате Россия вернулась в TOP 15 стран по этому показателю.

Рис. 29.
ТОР 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2020



Съемные носители

Процент компьютеров АСУ, на которых при подключении съемных носителей было заблокировано вредоносное ПО, увеличился в Восточной Азии, на Ближнем Востоке и не намного — в Западной и Северной Европе.

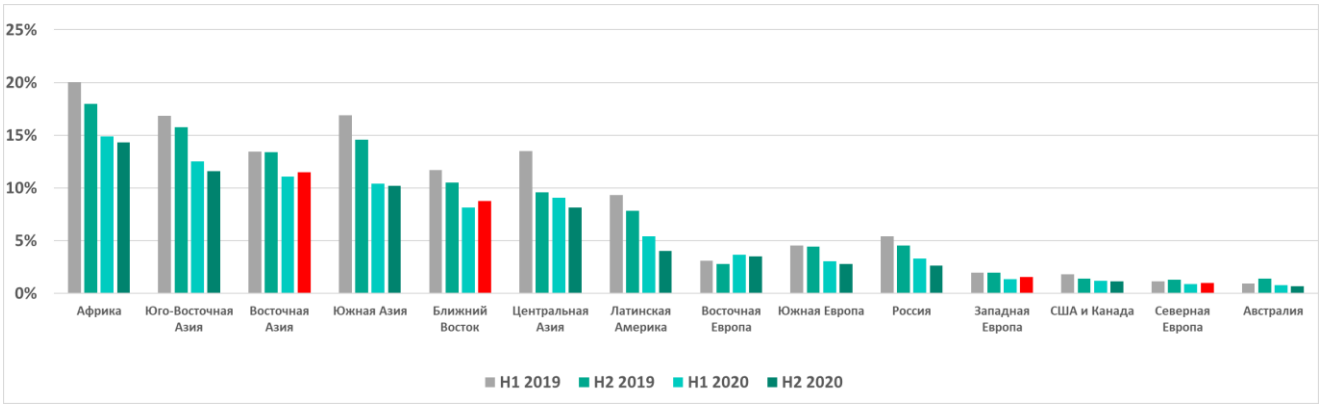
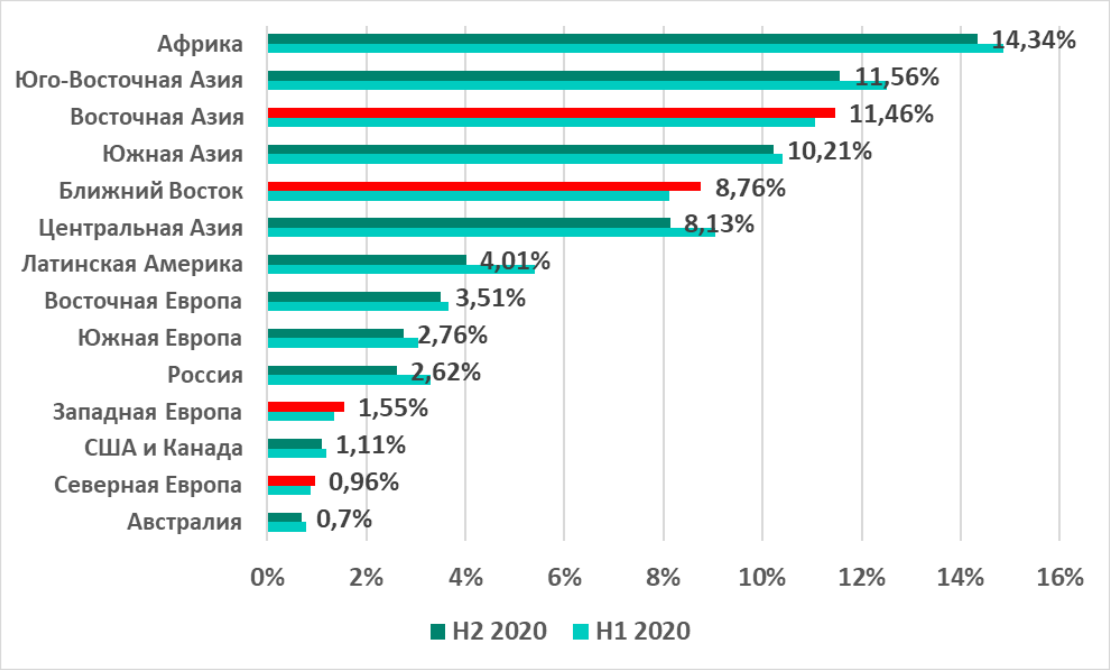


Рис. 30. Процент компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей

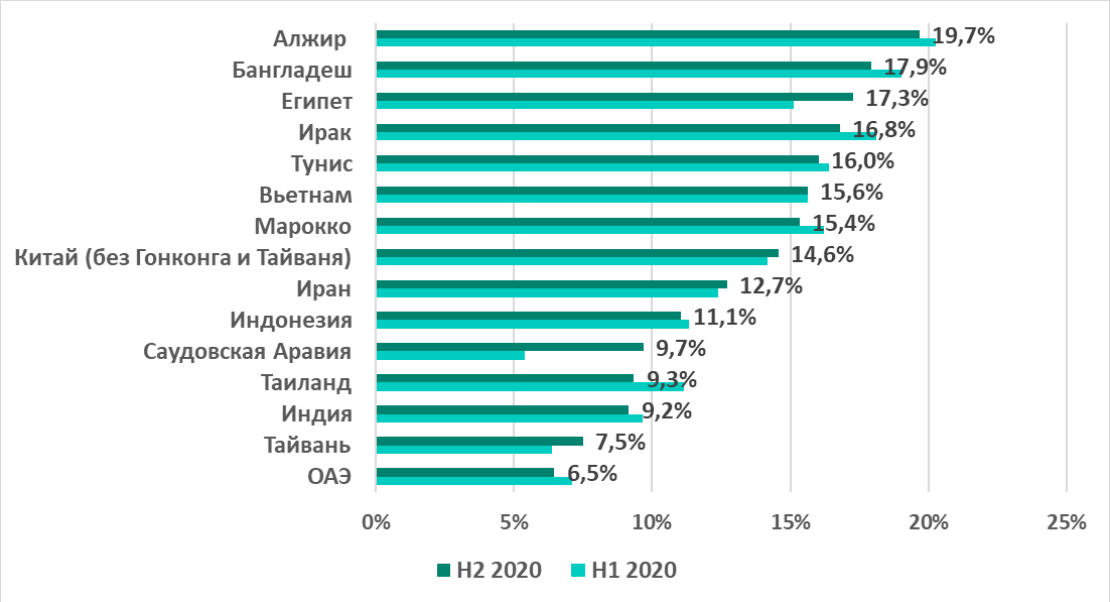
Рис. 31. Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, второе полугодие 2020



Во втором полугодии 2020 процент компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, вырос в 39% стран (во втором полугодии 2019 таких стран было 30,9%).

Среди всех стран наибольший рост этого показателя был отмечен в Саудовской Аравии — на 4,3 п.п.

Рис. 32. Топ-15 стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, второе полугодие 2020



Как и в первой половине 2020 года, по итогам второго полугодия в этот список не попали страны Северной Америки, Европы и Австралия.

Почтовые клиенты

Процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, во втором полугодии 2020 вырос во всех регионах, кроме Восточной Азии, США и Канады, Западной Европы и России.

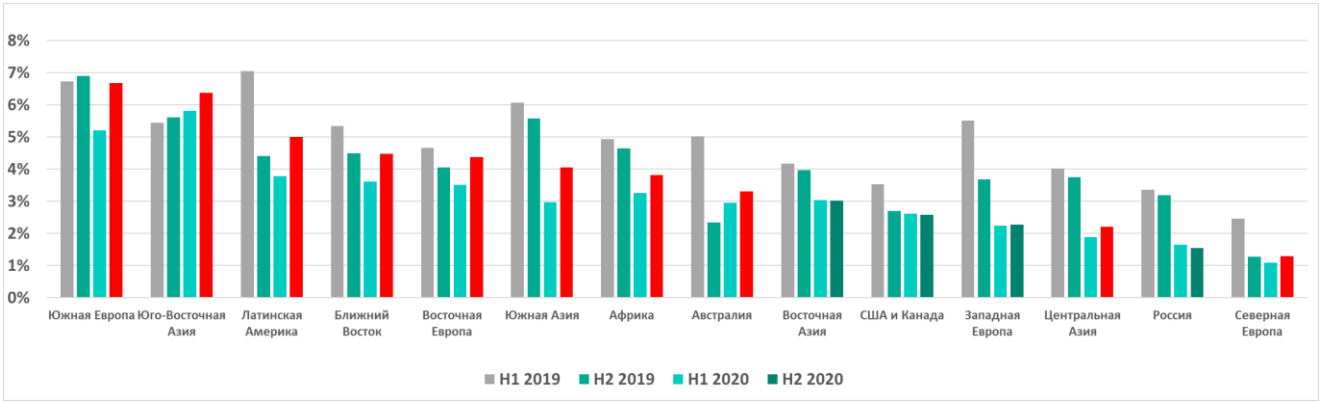
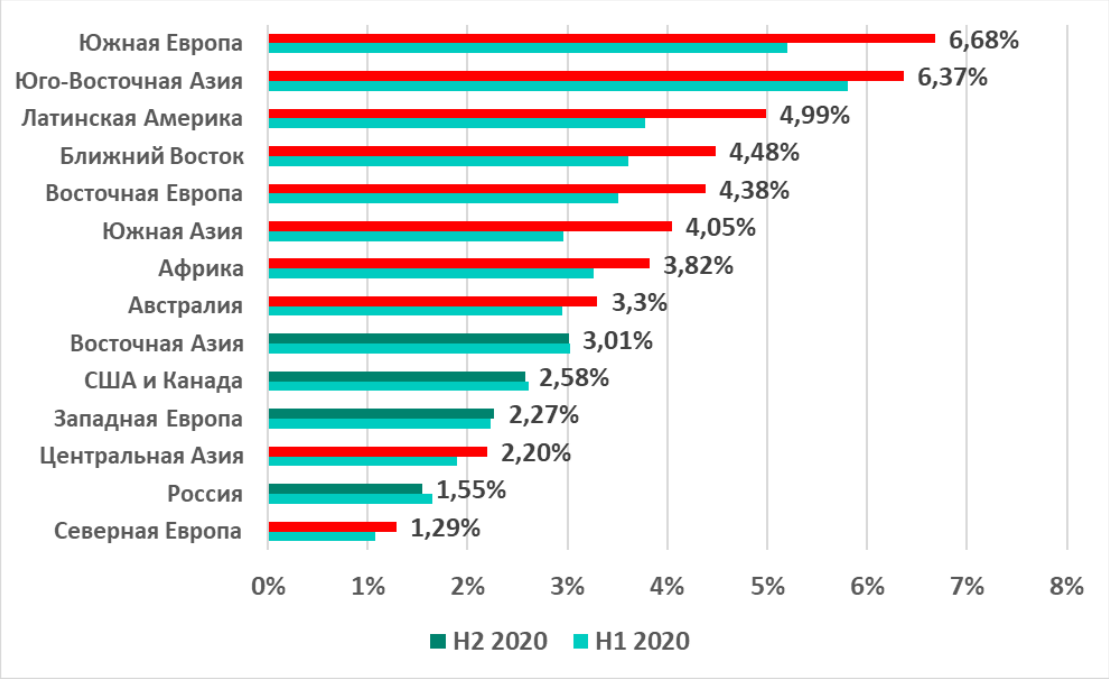


Рис. 33. Процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения

Рейтинг регионов по этому показателю по итогам полугодия вновь возглавила Юго-Восточная Азия.

Россия по этому показателю оказалась в числе наиболее благополучных регионов и заняла предпоследнее место в рейтинге.

Рис. 34. Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, второе полугодие 2020

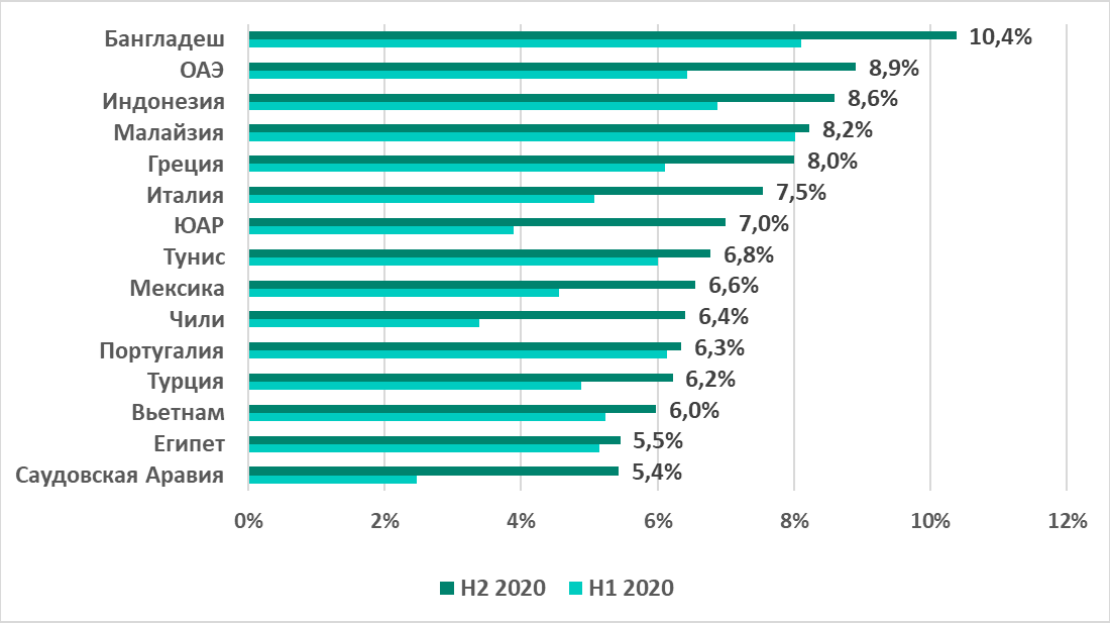


В случае вредоносных почтовых вложений изменения ситуации в разных странах мира, пожалуй, наиболее драматичны. Во втором полугодии 2020

года процент компьютеров АСУ, на которых были заблокированы почтовые вложения, вырос в 73,4% всех стран. Это втрое больше аналогичного показателя 2019 года (23,6%).

Во всех странах, попавших в TOP 15 по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, показатель вырос.

Рис. 35. Топ-15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, второе полугодие 2020

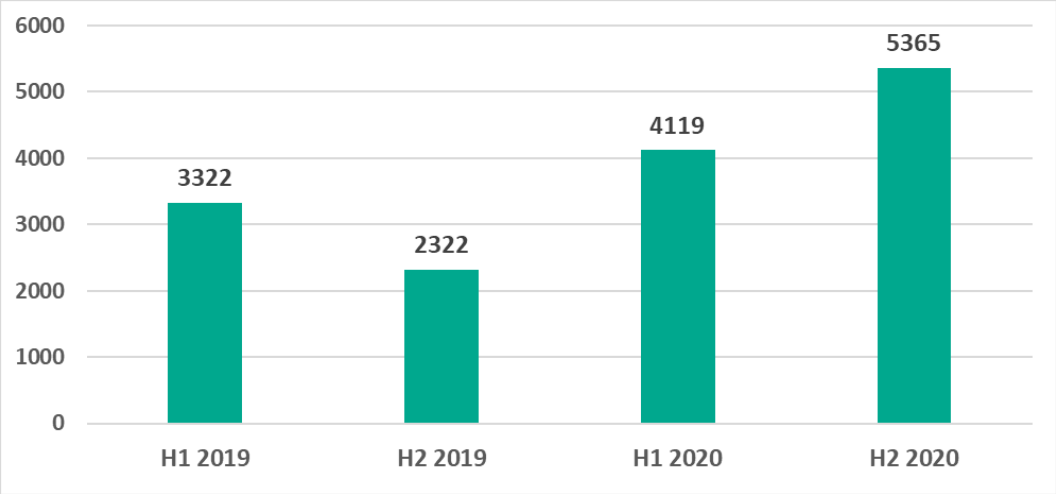


Отметим присутствие в этом рейтинге стран Южной Европы — Португалии, Греции и Италии.

Разнообразие обнаруженного вредоносного ПО

Во втором полугодии 2020 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 19,4 тысяч модификаций вредоносного ПО из 5365 различных семейств.

Рис. 36. Количество семейств вредоносного ПО, заблокированного на компьютерах АСУ, по полугодиям 2019 — 2020



После уменьшения показателя во второй половине 2019 года в 2020 году количество семейств вредоносного ПО увеличивалось. Стало заметно больше семейств бэкдоров, троянцев-шпионов, вредоносных скриптов и документов, а также вредоносного ПО на платформе .NET.

Категории вредоносных объектов

Результаты нашего детального анализа дали следующие оценки процента компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий:

Рис. 37. 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.

Во втором полугодии 2020 года вырос процент компьютеров АСУ, на которых были заблокированы:

- угрозы из интернета — веб-ресурсы, задействованные в распространении или управлении вредоносным ПО, и зловредные скрипты и перенаправления на веб-ресурсах (JS и Html) — на 2,5 п.п. и 1,6 п.п. соответственно;
- типичные угрозы, распространяемы по электронной почте — вредоносные документы MSOffice и PDF — на 1,2 п.п.
- шпионское ПО — троянцы-шпионы, бэкдоры и кейлоггеры — на 1,4 п.п.
- майнеры — исполняемые файлы для ОС Windows — на 0,7 п.п.

Краткое описание каждого типа угроз представлено в отдельном документе.

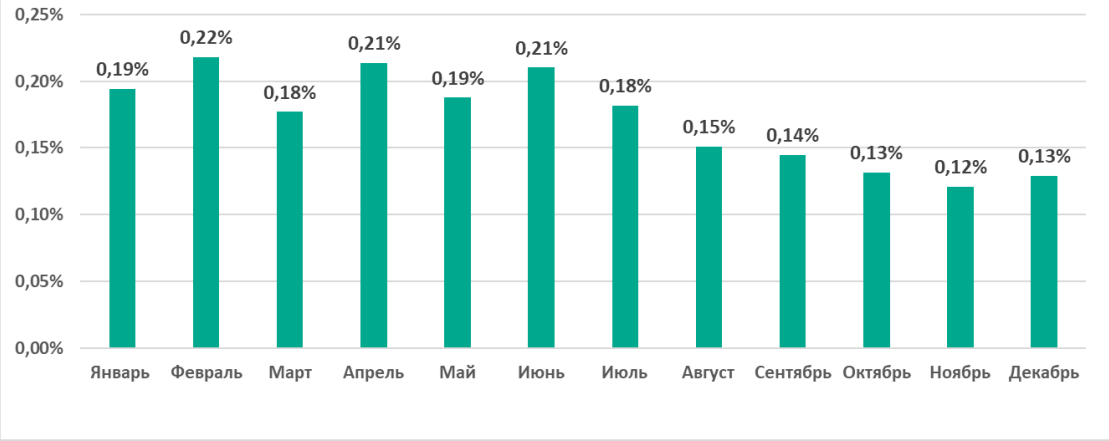
Программы — вымогатели

По итогам 2020 года процент компьютеров АСУ, на которых были заблокированы попытки заражения вредоносными программами-вымогателями, составил 0,77%.

В первом полугодии 2020 года такое вредоносное ПО было заблокировано на 0,63% компьютеров АСУ, во втором — на 0,49%.

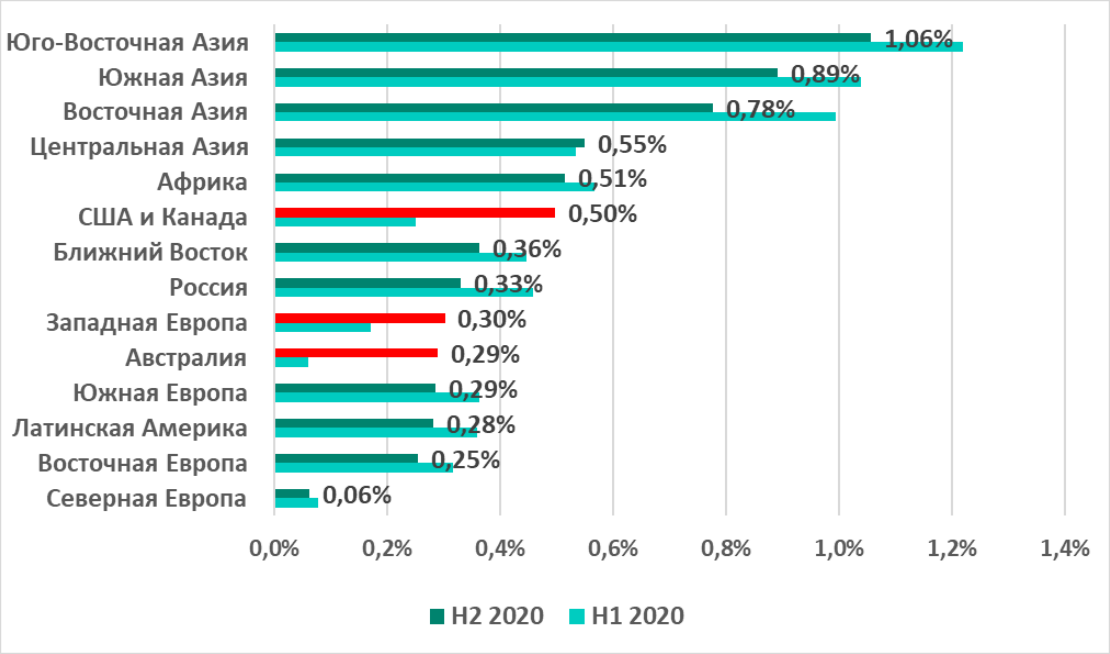
Этот показатель колебался от 0,18% до 0,22% в первой половине года, а во второй плавно уменьшился до 0,12% в ноябре и 0,13% в декабре.

Рис. 38. Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь — декабрь 2020



Юго-Восточная, Южная и Восточная Азия с большим отрывом от других регионов лидируют в рейтинге регионов по проценту атакованных вымогателями компьютеров АСУ.

Рис. 39. Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2020



В большинстве регионов, как и в целом по миру, во втором полугодии 2020 процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, уменьшился.

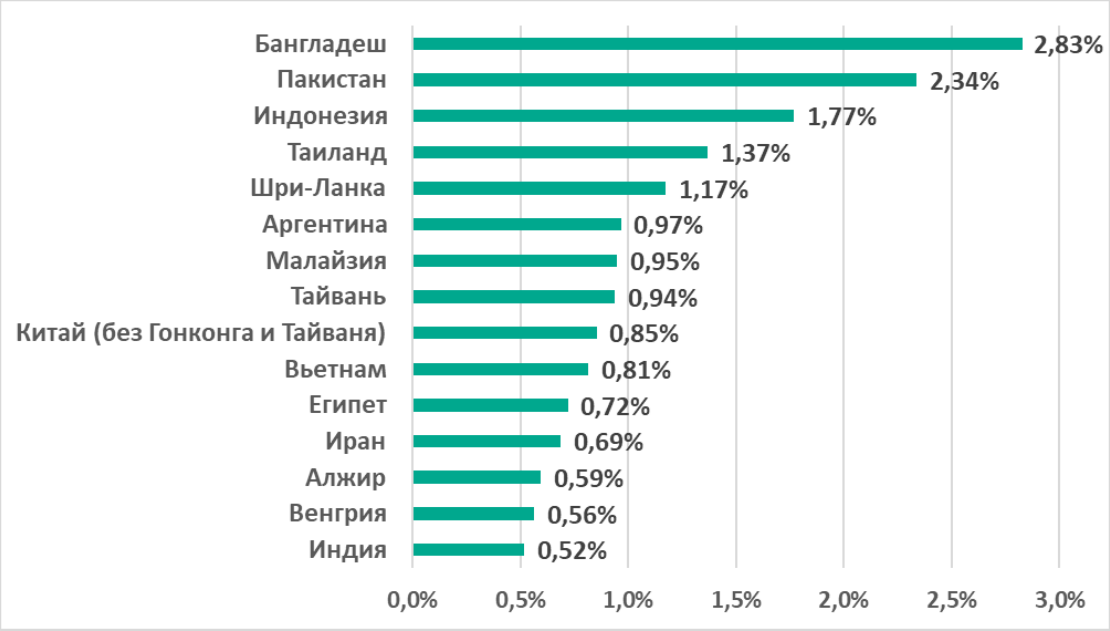
Однако есть несколько регионов, где этот показатель заметно увеличился:

- США и Канада — на 0,25 п.п.
- Австралия — на 0,23 п.п.
- Западная Европа — на 0,13 п.п.

Страны в этих регионах традиционно относят к развитым, и в аналогичных рейтингах они никогда не поднимались так высоко, как во втором полугодии 2020 года.

Большинство стран в TOP 15 по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, по-прежнему азиатские.

Рис. 40.
ТОР 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2020

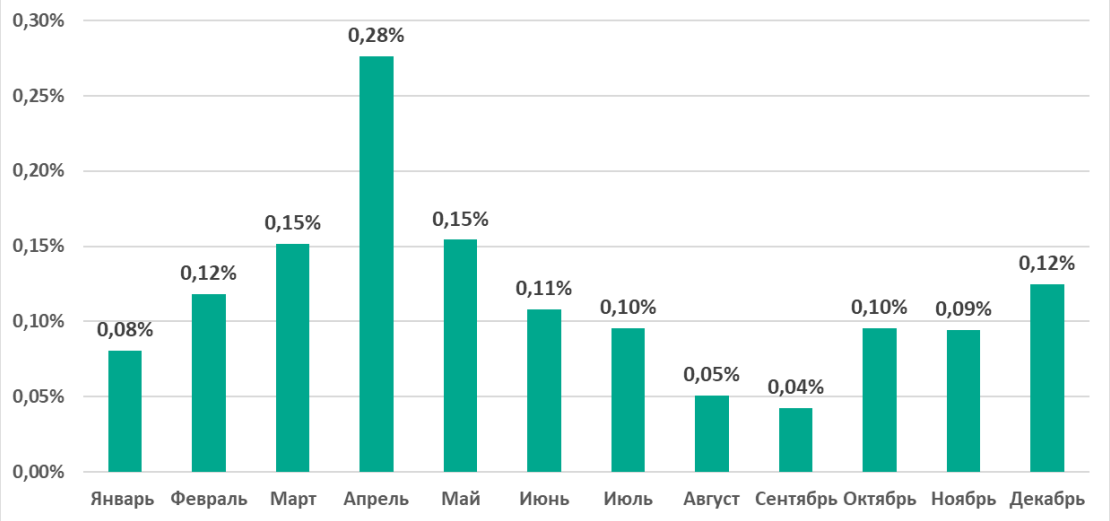


Единственная европейская страна — Венгрия — впервые попала в ТОР 15.

Россия

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, в России во втором полугодии 2020 уменьшился с 0,46% до 0,33%.

Рис. 41.
Россия. Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь — декабрь 2020



Как видно на графике, процент атакованных программами-вымогателями компьютеров АСУ в России увеличивался с января и достиг максимума в апреле (0,28%).

Далее он уменьшался с мая до сентября, когда было зафиксировано минимальное значение (0,04%). В четвертом квартале 2020 этот показатель вновь подрос до 0,12%.

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