ЦЕНТР КОМПЕТЕНЦИЙ
ПО ИМПОРТОЗАМЕЩЕНИЮ В СФЕРЕ ИКТ

ЦКИТ

АНАЛИТИЧЕСКИЙ ОТЧЕТ

Ландшафт российского рынка прикладного программного обеспечения и его сопоставление с мировым рынком и общими тенденциями (2019—2026)

Классы программного обеспечения: почтовые приложения, системы резервного копирования, системы виртуализации, облачные платформы

Москва, 2026 г.

ОГЛАВЛЕНИЕ

1. Введение

С 2019 по настоящее время во всём мире поступательно ужесточались требования к обработке персональных данных, целостности и сохранности данных. Наибольшее влияние на применение подобных мер оказали несколько факторов: пандемия COVID-19, стимулировавшая удалённую работу посредством информационных технологий; массовые хакерские атаки, блокирующие доступ к данным; и, как следствие, повышенные требования к сохранности и скорости восстановления данных.

Цифровая трансформация и переход на удалённую работу в период COVID-19 утроили долю облачных решений в мире и сделали ряд классов прикладного программного обеспечения — почтовые приложения, системы резервного копирования, системы виртуализации и облачные платформы — критическим элементом бизнес-процессов. К 2022 году до 95 % корпоративных серверов в России были виртуализированы (банки, телеком, госсектор, ОПК, транспорт, энергетика и пр.); электронная почта стала ключевым каналом взаимодействия с внешним миром; системы резервного копирования стали единственным барьером, отделяющим компании от полной потери данных при инцидентах с программами-вымогателями; облачные платформы превратились в базовую среду размещения приложений для подавляющего большинства корпоративных сценариев.

Все четыре класса прикладного программного обеспечения относятся к категории ПО с максимальным уровнем риска и для большинства предприятий являются полноценным объектом критической информационной инфраструктуры (КИИ) вне зависимости от отраслевой принадлежности.

Настоящий отчёт обобщает результаты анализа четырёх классов прикладного программного обеспечения — почтовые приложения, системы резервного копирования, системы виртуализации и облачные платформы — с точки зрения текущего ландшафта российского рынка, его сопоставления с мировым рынком, и систематизирует совокупность рисков, связанных с продолжением эксплуатации иностранных решений.

Процесс импортозамещения в сфере ИКТ в России стартовал в 2015 году с принятием соответствующих нормативных правовых актов и их последующим

ужесточением и распространением на все более широкий круг лиц. В ходе исследования акцент сделан на данные об использовании зарубежных решений в корпоративном секторе, компаниями — субъектами КИИ, крупными организациями, осуществляющими свою деятельность в ключевых отраслях экономики.

2. Почтовые приложения

2.1. Трансформация функционала почтовой системы

В 2018 году обязательные функции почтовой системы определялись как наличие:

- протоколов IMAP/POP3/SMTP;
- мобильных клиентов на iOS и Android;
- обеспечения функционала поиска и фильтров;
- антивирусной защиты;
- поддержки безопасного соединения TLS;
- веб-интерфейса;
- двухфакторной авторизации;
- поддержки Microsoft Active Directory и Exchange ActiveSync.

К 2026 году базовый функционал почтового приложения включает:

- полнофункциональный облачный сервер и клиент;
- интеграцию с облаком;
- приём вложений до 25—50 МБ напрямую и больших файлов через облачную ссылку;
- совместную работу: общие ящики, делегирование, общие календари, бронирование переговорных, интеграцию с офисным пакетом и видеоконференциями;
- ИИ-функции: семантический поиск, генерацию черновиков с настройкой тона, предложенные ответы в стиле автора, перевод, голосовой ввод и зарождающиеся ИИ-агенты (Microsoft Copilot Frontier, Gmail AI Overviews на Gemini 3, Apple Intelligence с iOS 18.1);
- для российского сегмента обязательным функционалом является полноценная поддержка российских операционных систем, аппаратных платформ и интеграция с российскими облачными сервисами.

Мировой рынок почтовых приложений к 2026 году завершает переход в вендорское облако, второй ключевой тенденцией становится использование искусственного интеллекта во всех компонентах почтовых систем.

К 2026 году почтовое приложение проникает во все процессы и обрастает большим количеством дополнительного функционала. Для многих компаний электронная почта — ключевой канал взаимодействия с внешним миром. Именно поэтому почтовые приложения классифицируются как ПО с максимальным уровнем риска.

2.2. Ключевые участники российского рынка

Иностранные вендоры, представленные на российском рынке:

- Microsoft (Exchange Server 2019 → Subscription Edition, M365/Exchange Online);
- Google (Gmail);
- HCL/IBM (Notes/Domino (v10—v14.5), HCL Verse, Sametime);
- Apple Mail;
- Mozilla Thunderbird;
- Yahoo Mail;
- Zimbra.

Российские вендоры:

- Группа Астра (RuPost + RuPost Desktop + Migration Tool);
- МойОфис / НОТ (МойОфис Почта (СМБ) + Mailion);
- АО «СБК» (CommuniGate Pro + Samoware);
- VK (mail.ru);
- VK Tech (VK WorkSpace);
- Яндекс (Яндекс 360);
- Р7 (Р7-Почта).

Безопасность почты в Российской Федерации обеспечивается следующими продуктами:

- Kaspersky Secure Mail Gateway;
- Positive Technologies;
- Solar (Ростелеком);

- InfoWatch Traffic Monitor, F.A.C.C.T.

Табл. 1. Объёмы мирового рынка почтовых приложений

Год	Почтовые сервисы, $ млрд	Безопасность почтовых приложений, $ млрд	Cloud-ящики, %
2018	46	2,8–3,1 (оценка)	50
2019	50	3,2	55
2020	53	3,5–4,0	63
2021	54,8	3,16–4,0	70
2022	63,6	4,25	75
2023	73,3	3,94–4,5	84
2024	84,2	5,17–6,94	86
2025	97,1	5,23–7,91	88
2026 (прогноз)	105,5	5,73–7,91	90

Табл. 2. Динамика российского рынка корпоративной почты, 2021–2025 гг.

Год	Рынок почтовых решений, всего (млн руб.)	Российские вендоры (млн руб.)	Зарубежные вендоры (млн руб.)	Доля российских
2021	5 513	561	4 952	10 %
2022	3 787	1 275	2 512	34 %
2023	4 360	1 457	2 903	33 %
2024	5 793	2 853	2 940	49 %
2025	6 979	4 052	2 927	58 %

Мировые показатели по использованию почтовых приложений демонстрируют двухкратный рост. За рассматриваемый период наблюдается значительное развитие

функциональных возможностей, решаемых задач и проникновение во все бизнес-процессы.

Вместе с тем в России не наблюдается существенных изменений в объёмах рынка, хотя очевидно его перераспределение в сторону приоритетного использования российских программных продуктов. Эти данные говорят об одном — большая часть корпоративных клиентов продолжают использовать почтовые приложения зарубежных вендоров, причём на уровне 40—50 % от общего объёма.

Действительно полный переход на российский продукт сопряжён с рядом технических сложностей, требует временных и финансовых затрат, однако задачей является оценка не только размера вложений, но и рисков, связанных с использованием иностранных почтовых сервисов.

Табл. 3. Доли вендоров на российском рынке корпоративной почты

Вендор	2018—2021	2022	2023	2024	2025
Microsoft Exchange / O365	70—80 %	~65 %	~60 %	~60 %	~50 %
HCL Domino / Lotus	5—10 %	5—8 %	3—5 %	~3 %	~2 %
Google Workspace	3—5 %	3—5 %	2—3 %	<2 %	<2 %
Российские вендоры (всего)	5—15 %	15—20 %	20—25 %	~30 %	~40 %

Формальная доля Microsoft в B2B-сегменте остаётся высокой (~50 %) при том, что продление лицензий и доступ к облаку прекращены. Это означает, что значительная часть пользователей продолжает работать на старых, давно не поддерживаемых или снятых с основной поддержки версиях Exchange Server, то есть в зоне критического риска.

Табл. 4. Доля иностранных решений по сегментам РФ (% иностранные / % российские, экспертная оценка)

Сегмент	2018	2020	2022	2023	2024	2025	2026
Госсектор	80/20	75/25	50/50	30/70	15/85	5/95	0/100

Сегмент	2018	2020	2022	2023	2024	2025	2026
Объекты КИИ	75/25	70/30	40/60	20/80	10/90	5/95	0/100
Крупный бизнес — банки	85/15	80/20	70/30	55/45	45/55	35/65	25/75
Крупный бизнес — нефтегаз	90/10	85/15	65/35	45/55	30/70	20/80	15/85
Крупный бизнес — ритейл	85/15	80/20	70/30	60/40	50/50	40/60	30/70
Средний бизнес	90/10	88/12	80/20	70/30	60/40	50/50	40/60
Малый бизнес	95/5	93/7	88/12	80/20	70/30	60/40	50/50
Образование	70/30	65/35	50/50	35/65	25/75	15/85	10/90

2.3. Примеры инцидентов в почтовых системах российских организаций

К 2025–2026 гг. в государственном секторе и на объектах КИИ доля иностранных решений формально приблизилась к нулю, но отдельные примеры свидетельствуют об иной фактической картине:

- Кампания BI.ZONE «security4real» (август 2022 — 2023, ProxyShell, CVE-2021-34473): десятки российских компаний СМБ-сегмента, эксфильтрация почтовых ящиков, шантаж публикацией данных под видом «аудита безопасности» (Habr/BI.ZONE).
- По данным Positive Technologies, в 2023 году 50 % всех расследованных атак на публично доступные приложения в РФ пришлись на Microsoft Exchange.
- В августе 2023 ФСТЭК России публично предупредила об уязвимости BDU:2023-07515 в Exchange, затрагивающей ~77 тыс. серверов в России.
- «Аэрофлот», 28 июля 2025 — группировки Silent Crow (Украина) и «Киберпартизаны BY» (Беларусь) уничтожили ~7 000 серверов и эксфильтрировали 12 ТБ баз данных, 8 ТБ файлов и 2 ТБ корпоративной почты; среди скомпрометированных систем явно названы Exchange, SharePoint, CREW, Sabre, КАСУД, Sirax, CRM, 1С, DLP.

- Positive Technologies и Kaspersky фиксируют устойчивые кластеры атак на российские цели через фишинг: Cloud Atlas, XDSpy, Scaly Wolf, Mysterious/Core/Sticky/Paper/Vortex Werewolf, Hellhounds, Dark River, Red Wolf, Head Mare, Silent Crow. Типовая схема — фишинговые письма от имени Минпромторга России, Роскомнадзора, СК РФ, Военной прокуратуры.
- «Ростелеком» (январь 2025, Silent Crow, утечка 154 тыс. email через подрядчика, РБК, «Ведомости»);
- «Доктор Веб» (октябрь 2024, DumpForums заявил о компрометации сервера корпоративной почты, Confluence, Redmine);
- «Россети» (2025, продажа дампа 3 ТБ с корпоративной перепиской на закрытом форуме);
- ВСК (ноябрь 2024, корпоративная почта выведена из строя на неделю);
- «Яндекс» (февраль 2023, утечка 45 Гб репозиториев — компания настаивает на инсайдерском характере);
- СДЭК (май 2024, шифровальщик Head Mare).

Согласно статистике, формируемой вендорами в области информационной безопасности, почтовые приложения относятся к одному из наиболее уязвимых сегментов. По данным BI.ZONE — 68 % целевых атак начинаются с email; по данным Positive Technologies — в 79 % случаев доступ к защищённой информации, системам или физическим объектам, основанный на психологическом манипулировании людьми, осуществляется через почту, 92 % вредоносной доставки — электронная почта; по данным Kaspersky — 42 % начальных компрометаций происходит через уязвимости публичных приложений (преимущественно почтовых). По данным StopPhish и Forbes (2024), корпоративные email сотрудников 94 из 100 крупнейших российских компаний присутствуют в публичных утечках.

3. Системы резервного копирования

3.1. Состояние российского рынка

К 2021 году российский рынок был насыщен западными решениями в области резервного копирования. Число зарубежных компаний, представленных в классе «Системы резервного копирования», к 2021 году составляло более 30. Основную долю

рынка (более 90 %) занимали крупные западные решения; компания Veeam обладала долей в 50—60 % годового объёма всего российского рынка.

Табл. 5. Ключевые игроки российского рынка систем резервного копирования

Годы	Зарубежные компании, разработчики	Российские компании, разработчики
2019—2025	Veeam B&R; Veritas NetBackup/Commvault; Acronis Cyber Backup/Protect; Commvault® Backup & Recovery; Microsoft (DPM/Azure); HPE; Dell EMC; IBM; Arcserve; Micro Focus Data Protector.	ООО «Акронис-Инфозащита» — ООО «Киберпротект» («Кибер Бэкап»); ГК «Астра» («RuBackup»); ООО «Новософт Развитие» («Handy Backup»); ООО «Береста РК» («Береста»); ЗАО «МВП «СМЕВЕЛ» («Циркон-резерв»); ООО «ХАЙСТЕКС» («Хайстекс Акура»).

После марта 2022 года и до конца 2023 года практически все западные поставщики систем резервного копирования заявили о своём уходе и официально покинули российский рынок. Стоит отметить, что большинство иностранных решений поставлялось через локальных дистрибьюторов или партнёров, продукты были локализованы для российского рынка, для них были организованы службы поддержки пользователей, однако официальные представительства большинства зарубежных поставщиков в Российской Федерации открыты не были.

3.2. Оценка затрат российских компаний на приобретение систем резервного копирования

Распределение затрат на мировом и российском рынках систем резервного копирования с 2019 по 2025 годы выглядит в динамике следующим образом.

Табл. 6. Объёмы мирового и российского рынков СРК

Год	Мир, $ млрд (млрд руб.)	Россия, млрд руб.
2019	7,80 (504,9)	7,3
2020	8,60 (620,5)	8,4

Год	Мир, $ млрд (млрд руб.)	Россия, млрд руб.
2021	9,50 (699,7)	9,7
2022	10,50 (719,8)	5,6
2023	11,60 (988,9)	7,1
2024	12,90 (1 194,1)	8,5
2025	14,20 (1 187,4)	9,1

Согласно данным по оценке рынка, на 2021 год приходится пик объёма затрат на российском рынке систем резервного копирования — 9,7 млрд руб., при этом доля иностранных решений составила более 90 %.

К 2025 году на российском рынке сформированы и доступны зрелые российские решения, осуществляется масштабное внедрение на всех уровнях. По различным оценкам, объём российского рынка составил приблизительно 9,1 млрд руб. Доля российских решений на текущий момент превышает 60 %.

Табл. 7. Структура российского рынка СРК

Год	Объём общий, млрд руб.	Доля российских решений, %
2021	9,7	7
2022	5,6	35
2023	7,1	53
2024	8,5	63
2025	9,1	70 и более

Табл. 8. Объёмы продаж российских и иностранных решений по годам, млрд руб.

Показатель	2019	2020	2021	2022	2023	2024	2025
Российские решения	0,5	0,6	0,7	2,0	3,8	5,4	6,4

Показатель	2019	2020	2021	2022	2023	2024	2025
Иностранные решения	6,7	7,7	8,8	3,1	2,8	2,6	2,3
Закупки без идентификации продукта	0,1	0,1	0,2	0,5	0,5	0,5	0,4

Объём российского рынка на своём пике к 2021 году достигал примерно 9,7 млрд руб. в год, однако в 2022 году из-за санкций и официального ухода западных поставщиков сократился до 5,6—5,9 млрд руб. в год и не восстановился до сих пор.

Распределение российского рынка систем резервного копирования по лидерам выглядит следующим образом. Объём выручки ООО «Киберпротект» с решением «Кибер Бэкап» в 2024 году составил 4,21 млрд руб., в 2025 году — 5,33 млрд руб., что соответствует росту на 26 %. На российском рынке доля «Кибер Бэкап» составляет более 80 %, RuBackup от ГК «Астра» — 10 %. Другие российские системы резервного копирования занимают существенно меньшие доли рынка.

3.3. Российские альтернативы зарубежным решениям

Табл. 9. Зарубежные решения и их статус, российские альтернативы

Зарубежное решение	Статус в РФ	Российская альтернатива
Veeam Backup & Replication	Покинул российский рынок, лицензии блокируются с марта 2024 года	On-premise решения резервного копирования: «Кибер Бэкап»; «RuBackup»; «Handy Backup»; «Береста»; «Циркон-резерв»; «Хайстекс Акура». Защита виртуальных сред: Basis Virtual Protect. Облачные решения: Beeline Cloud Backup; «MWS Резервное копирование»;
Veeam Data Cloud for M365	Заблокирован после ухода Microsoft	
Veeam Kasten K10 (Kubernetes)	Покинул российский рынок	
Veritas NetBackup	Покинул российский рынок, поглощён Cohesity	

Зарубежное решение	Статус в РФ	Российская альтернатива
Commvault	Покинул российский рынок (07.03.2022)	«Selectel PK как услуга»; VK Cloud Backup; Yandex Cloud Backup.
Dell EMC PowerProtect / Avamar / NetWorker	Покинул российский рынок	
IBM Spectrum Protect (TSM)	Покинул российский рынок (07.06.2022)	
HPE StoreOnce / Data Protector	Покинул российский рынок (01.06.2022)	
Rubrik / Cohesity	Доля рынка крайне мала	
Acronis Cyber Protect	Прекратил продажи в РФ с 2017	
Arcserve	Доля рынка крайне мала, покинул российский рынок	
Quest NetVault / vRanger	Доля рынка крайне мала	
pgBackRest / Barman / Dell для Oracle	Поддержка прекращена	
Zerto	Покинул российский рынок с HPE	

С учётом совокупности данных о потребностях рынка, растущем функционале, увеличивающемся спросе, расширении законодательных требований, росте объёмов данных в различных секторах экономики и существенном увеличении рисков, потребность российских компаний в продуктах класса систем резервного копирования определённо растёт достаточно высокими темпами.

Вместе с тем, проводя сравнения с мировыми показателями рынка систем резервного копирования, продемонстрировавшими двухкратный рост, можно сделать

вывод, что рынок в России частично ушёл в «серую зону» и занял выжидательную позицию.

С учётом всё возрастающего спроса на системы резервного копирования несущественная разница в динамике объёмов затрат крупнейших российских потребителей с 2022 по 2025 годы может свидетельствовать о фактическом использовании ранее приобретённых иностранных решений вместо перехода на отечественные аналоги. Доля крупного бизнеса, продолжающего использование западных решений, закупленных в период до 2022 года, не менее 30 %.

3.4. Фактический статус ключевых зарубежных поставщиков

На сегодняшний день фактический статус ключевых зарубежных поставщиков систем резервного копирования следующий.

Компания Veeam Software прекратила продажи 4 марта 2022 года (заявление CEO Anand Eswaran), петербургский офис R&D был закрыт 24 мая 2022 года, в июне 2023 года ликвидированы ООО «Виэм Рус» и ООО «Эмаст Софтвер Корпорэйшн». 20—25 марта 2024 года началась массовая блокировка личных кабинетов российских клиентов со ссылкой на санкции ЕС 12-го пакета. До 2022 года Veeam обеспечивал более 50 % российского рынка резервного копирования, и даже сейчас примерно 30 % компаний продолжают эксплуатировать Veeam без поддержки. Основатели Андрей Баронов (декабрь 2023 года) и Ратмир Тимашев (январь 2024 года) отказались от российского гражданства, что косвенно подтверждает невозможность возврата.

Veritas Technologies прекратила все операции в России 7 марта 2022 года. Компания Commvault официально ушла с российского рынка 7 марта 2022 года. Dell EMC PowerProtect/Data Domain/Avamar/NetWorker — после закрытия в августе офисов Dell объявила полный уход 29 августа 2022 года. IBM Spectrum Protect (TSM/Storage Protect) — 7 июня 2022 года IBM объявила контролируемое прекращение деятельности российского представительства, российское юридическое лицо завершило коммерческую деятельность к концу 2022 года. HPE StoreOnce/Data Protector — 1 июня 2022 года объявлен организованный уход из России. Acronis прекратил прямые продажи в России ещё в 2017 году, российский партнёр «Акронис-Инфозащита» в 2022 году был преобразован в ООО «Киберпротект» и стал

технологически независимым. Arcserve и Quest Software (NetVault, vRanger) фактически прекратили работу через дистрибьюторов из-за санкций.

4. Системы виртуализации

4.1. Состояние российского рынка

Системы виртуализации являются основным элементом построения корпоративных систем как для внутреннего облака, так и для внешнего. К 2022 году до 95 % корпоративных серверов в России были виртуализированы (банки, телеком, госсектор, ОПК, транспорт, энергетика и пр.), причём около 80 % серверов работали на VMware vSphere.

К началу 2022 года ключевыми поставщиками российского рынка были следующие компании:

- VMware (vSphere, ESXi, vCenter, vCloud Director, NSX-T, vSAN, Horizon, Workspace ONE, vRealize, Tanzu/Pivotal Cloud Foundry после поглощения, vRA, SDDC Manager, VMware Cloud Foundation; лидер с инсталляционной базой ~80 тыс. хостов к концу 2021 г.);
- Microsoft (Hyper-V, Windows Server 2016/2019, System Center Virtual Machine Manager, Azure Stack HCI, Azure Stack Hub, Storage Spaces Direct);
- Citrix Systems (XenServer/Citrix Hypervisor, XenApp/XenDesktop → Citrix Virtual Apps and Desktops, NetScaler ADC/Citrix ADC, Citrix ADM, ShareFile, XenMobile);
- Red Hat (RHEL, Red Hat Virtualization RHV/RHEV, OpenShift Container Platform, Red Hat OpenStack Platform, Ceph Storage);
- Oracle (Oracle VM Server, VirtualBox, Oracle Linux Virtualization Manager OLVM, Oracle Cloud Native Environment);
- Nutanix (AHV, Prism, Nutanix Enterprise Cloud, Files, Era, Calm; представительство с 2014 г.);
- IBM (PowerVM, IBM Cloud Private, IBM Cloud Pak, Spectrum Virtualize, KVM for IBM z, z/VM; в 2019 г. купила Red Hat);
- HPE (SimpliVity, OneView, GreenLake, Synergy, Nimble, ProLiant);
- Huawei (FusionCompute, FusionSphere).

К 2025 году доля российских поставщиков в сегменте серверной виртуализации выросла до 80 %. Тем не менее парк виртуальных машин на VMware остаётся существенным, а в финансовом секторе и нефтегазовой отрасли — критическим.

Российские альтернативы к 2026 году достигли функционального соответствия с VMware vSphere в большинстве сегментов:

- Базис (Basis Dynamix Standard/Enterprise/Cloud Control) — лидер по выручке (4,5 млрд руб. в 2024, 26–30 % рынка);
- zVirt от Orion soft — популярное решение для миграции с VMware vSphere/vCenter;
- vStack от ITGLOBAL.COM — гиперконвергентная платформа на FreeBSD/bhyve/ZFS;
- ROSA Virtualization;
- Скала^р МВ (Rubytech) — ПАК на базе Basis Dynamix + Deckhouse Kubernetes;
- ПК СВ «Брест» (Astra Linux) — для гостайны до уровня «совершенно секретно», единственное решение с 1 классом защиты;
- РЕД Виртуализация (Ред Софт) — oVirt + РЕД ОС.

Табл. 10. Объёмы мирового рынка ПО виртуализации

Год	Виртуализация ($ млрд)	Год к году
2019	~38–42	—
2020	~45–48	+12–14 %
2021	~52–58	+14–17 %
2022	~60–68	+12–17 %
2023	~70–75	+9–12 %
2024	~80–86	+14–16 %
2025	~95–96	+11–12 %
2026 (оценка)	~110	+13–15 %

4.2. Российский рынок — класс 02.04 (ПО виртуализации)

Российский рынок средств виртуализации прошёл за восемь лет траекторию от практически полной зависимости от западных вендоров до доминирования отечественных решений в новых продажах при сохранении огромной унаследованной зарубежной инсталляционной базы.

Табл. 11. Динамика российского рынка ПО виртуализации

Год	Рынок (₽ млрд)	Год к году	Доля иностр.	Доля росс.	Выручка росс. (₽ млрд)
2019	~9–11	н/д	~96 %	~4 %	~0,4
2020	~10–11	~5 %	~96 %	~4 %	~0,45
2021	10,73	+5–7 %	95–96 %	4–4,5 %	0,42–1,5
2022	7,37	−31 %	77–81 %	12–19 %	1,4
2023	10,08	+37 %	45 %	55 %	5,55
2024	13,83	+37 %	26 %	74 %	10,19
2025	~19,4	+37–40 %	~20 %	~80 %	~15–16

Установленная база VMware в России на конец 2021 года составляла примерно 80 000 серверов, а к концу 2024 года российские решения заняли 60,2 % развёртываний виртуализации у обследованных облачных провайдеров; VMware упал до 39 %.

Ключевая особенность ситуации к 2025–2026 годам: VMware всё ещё занимает 39 % серверов в эксплуатации, но новых лицензий практически не продаётся. Это означает, что компании продолжают эксплуатировать ранее купленный VMware vSphere без обновлений.

5. Облачные платформы

5.1. Состояние мирового и российского рынка

Облачные платформы (класс 02.03 — облачные и распределённые вычисления) к 2025—2026 годам стали базовой инфраструктурой для размещения корпоративных приложений всех рассмотренных выше классов: почтовых систем, систем резервного копирования и платформ виртуализации. Темпы роста мирового рынка облачных сервисов сохраняют двузначные значения, и российский рынок в этом тренде следует мировой динамике.

Табл. 12. Объёмы мирового рынка облачных и распределённых вычислений, $ млрд

Год	Всего	Год к году
2019	~96—97	~37 %
2020	129	~33 %
2021	178	~38 %
2022	227	~28 %
2023	270	~19 %
2024	330,4	~22 %
2025	419	~27 % (Q4 +30 %)

Российский рынок облачных сервисов вырос с приблизительно 68 млрд руб. в 2018 году до 416,5 млрд руб. в 2025 году — практически в шесть раз в рублях. При этом доля иностранных провайдеров обрушилась с 25—30 % до фактически нулевой к 2024—2025 годам согласно официальным данным. До 2022 года на российском рынке преимущественное присутствие имели западные провайдеры: AWS, Microsoft Azure, Google Cloud, Oracle, IBM и SAP.

Табл. 13. Объём российского рынка IaaS+PaaS

Год	IaaS+PaaS (₽ млрд)	Год к году
2019	~28,5 (оценка)	~25 %

Год	IaaS+PaaS (₽ млрд)	Год к году
2020	39,4	+38 %
2021	61,1	+53 %
2022	90,6	+47 %
2023	121,5	+33,9 %
2024	168,5	+36,3 %
2025	~235	~+40 %

Ключевая динамика российского рынка — замедление темпов роста: с пика +47 % в 2022 году рынок постепенно сходит к +29 % в 2025 году и ожидаемым +22–25 % в 2026 году. Темпы роста в целом соответствуют мировым показателям.

После 2022 года произошло последовательное замещение иностранных провайдеров в связи с уходом и/или приостановкой доступа западными компаниями. Ключевые решения, представленные на российском рынке: Cloud.ru, РТК-ЦОД, Yandex Cloud, Selectel, MWS, VK Cloud.

Табл. 14. Зависимость российского рынка от иностранных облачных провайдеров

Год	Объём рынка, млрд ₽	Доля иностранных провайдеров (оценка)	Лидер из иностранных
2018	68,4	~25–28 %	Microsoft Azure
2019	~86	~22–25 %	Microsoft Azure
2020	~96–104	~18–22 %	Microsoft + AWS
2021	~115–140	~15–20 %	Microsoft, AWS, GCP
2022	~180 (90,6 IaaS+PaaS)	резкое падение к 5–10 %	—
2023	~242	<3 % в IaaS/PaaS	—
2024	322,3	<1–2 % легально	—

Год	Объём рынка, млрд ₽	Доля иностранных провайдеров (оценка)	Лидер из иностранных
2025	416,5	<1 %	—

К началу 2026 года в России выстроена многоуровневая нормативная система, фактически делающая невозможным легальное использование иностранных облаков в большинстве серьёзных сценариев.

В настоящее время дата-центры подавляющего большинства российских облачных провайдеров находятся на территории Российской Федерации, имеют уровень надёжности Tier III и соответствуют требованиям регуляторов (УЗ-1/2, ГИС К1, 1Г и т.д.). Однако при этом сама инфраструктура ЦОДов для предоставления облачных услуг (не гостевые ОС и прикладное ПО) зачастую состоит из иностранных продуктов, включая проприетарные гипервизоры VMware, vSphere, либо гипервизоры на базе ПО с открытым кодом (KVM/QEMU), СУБД Oracle, MS SQL, операционные системы семейства Windows, балансировщики ALB NLB, резервное копирование Veeam и др., что существенно повышает степень ранее упомянутых рисков.

5.2. Ключевые российские облачные провайдеры

К 2025—2026 годам сформирован пул российских облачных провайдеров, обеспечивающих полный спектр услуг IaaS, PaaS и SaaS, включая аттестованные сегменты для размещения государственных информационных систем (ГИС) и систем, обрабатывающих персональные данные на уровне защищённости УЗ-1 и К1. Краткая характеристика ключевых провайдеров приведена ниже.

Selectel.

Облачная платформа на базе OpenStack (собственной сборки), отдельный продукт — «Облако на базе VMware» (vSphere/vCloud Director), а также аттестованный сегмент ЦОД и аттестованное облако (УЗ-1, ГИС К1). Средства защиты информации — сертифицированные ФСТЭК России (антивирус, СЗИ от несанкционированного доступа, доверенная загрузка по подписке). 6 собственных центров обработки данных в Российской Федерации.

Yandex Cloud.

Собственный гипервизор на базе KVM/QEMU (полностью собственная разработка, не VMware). Аттестат соответствия 152-ФЗ до УЗ-1 (от ООО «Кард Сек»), Приказ ФСТЭК России № 21. Object Storage — S3-совместимое хранилище.

VK Cloud (бывш. MCS / Mail.ru).

Платформа на базе OpenStack с собственными доработками. Отдельный продукт Secure Cloud для государственных информационных систем. Серверы Intel Xeon Gold 6230/6230R. ЦОДы уровня Tier III и IV расположены в России, SLA (соглашение об уровне обслуживания) — 99,95% с финансовыми гарантиями. Совместимость с отечественными ОС и типовыми x86-серверами, доверенные ПО и ПАК. Инфраструктура VK Cloud аттестована по требованиям 152-ФЗ (УЗ-1), К1 (ГИС), сертифицирована по PCI DSS, ГОСТ Р 57580.1, ФСТЭК России

Cloud.ru (бывш. SberCloud),

Несколько платформ: Cloud.ru Advanced (собственная), «Облако на базе VMware», ML Space. Все продукты аттестованы по 152-ФЗ УЗ-1. S3 объектное хранилище, DRaaS, резервное копирование.

MWS (MTC Web Services).

Аттестованный сегмент по 152-ФЗ УЗ-1/К1, заключение по ГОСТ Р 57580.1-2017. Активно продвигают медицинский кейс — публичный проект «Платформа обмена медицинскими данными».

Рег.облако (reg.cloud).

Аттестат ФСТЭК России УЗ-1 (информационные системы персональных данных и автоматизированные системы класса 1Г), включена в реестр российского ПО, S3-бакеты, GPU-серверы (A5000, A100).

DataLine Cloud-152.

Аттестат ФСТЭК России + PCI DSS + ISO/IEC 27001:2013. Совместимость с S3 — 98 %. Готовый продукт «Облачный диск для просмотра медицинских файлов».

Linx Cloud.

Облако на базе VMware с поддержкой S3 в соответствии с Федеральным законом № 152-ФЗ.

6. Карта рисков использования иностранного программного обеспечения

Анализ рисков, связанных с продолжением эксплуатации иностранного программного обеспечения четырёх рассматриваемых классов — почтовых приложений, систем резервного копирования, систем виртуализации и облачных платформ — показывает, что значительная часть угроз является общей для всех классов прикладного программного обеспечения и обусловлена единым санкционным контуром, единой регуляторной средой и едиными технологическими ограничениями. При этом каждый класс программного обеспечения имеет также собственные специфические риски, обусловленные функциональным назначением и архитектурой решений.

В целях системного представления риски разделены на две группы:

- общие риски, применимые ко всем четырём классам ПО (раздел 6.1);
- специфические риски, характерные для отдельного типа программного обеспечения (раздел 6.2).

6.1. Общие риски, применимые ко всем классам ПО

Группа общих рисков охватывает шесть основных категорий: технологические, экономические, киберугрозы, юридические и регуляторные, операционные и репутационные. Каждая из них в равной мере проявляется во всех четырёх классах прикладного программного обеспечения, рассматриваемых в настоящем отчёте.

6.1.1. Технологические риски

1. Прекращение обновлений и патчей безопасности.

После ухода западных вендоров российские клиенты теряют доступ к репозиториям обновлений: Veeam с марта 2024 года блокирует личные кабинеты, Microsoft 20 марта 2024 года отключила более 50 облачных сервисов, Cisco в марте 2022 года деактивировала Smart-аккаунты в течение 24 часов. С сентября 2023 года российские организации не получают обновлений Microsoft. Любой обнаруженный CVE превращается в уязвимость нулевого дня для российского пользователя. Возможность легального получения патча отсутствует. Получение патчей через

посредников в третьих юрисдикциях уязвимо с точки зрения возможной загрузки бэкдора, специально созданного для России.

2. Истечение лицензий и невозможность их продления.

Лицензии Veeam, Commvault, Veritas, VMware и Microsoft требуют ежегодного продления с активацией через серверы вендора. Параллельный импорт (Постановление Правительства Российской Федерации от 29.03.2022 № 506) формально касается товаров, а не SaaS-лицензий. Активация требует онлайн-связи с инфраструктурой вендора, заблокированной для российских IP-адресов и реквизитов. Перманентные лицензии ряда продуктов продолжают работать, но без обновлений; существует сценарий полного аннулирования даже постоянных ключей.

3. Дистанционное отключение и блокировка облачных сервисов.

Cisco Meraki в октябре—ноябре 2022 года удалённо переконфигурировала точки доступа клиентов из России, переключив их на открытый SSID с надписью «12345-Sanctions». Microsoft 20—31 марта 2024 года массово отключил более 50 облачных сервисов российским юридическим лицам по EU 2023/2873. SAP 20 марта 2024 года отключил облачные сервисы российских клиентов. Veeam с 20—25 марта 2024 года блокирует личные кабинеты с 30-дневным grace-периодом для подписочных ключей. Отключение может произойти в момент критического инцидента, когда требуется восстановление. Пользователь не владеет своими данными — владелец сервиса может удалить аккаунт без объяснения причин.

4. Несовместимость с российскими операционными системами и инфраструктурой.

Постановлением Правительства Российской Федерации от 28.11.2025 № 1937 введена с 01.01.2026 обязательная совместимость средств защиты информации, СУБД и средств виртуализации с двумя российскими ОС (Astra Linux, RED OS, ALT Linux). Зарубежные системы сертифицированы для Windows Server, RHEL, SLES, ESXi/vSphere, но не для Astra Linux SE, «Брест», zVirt, RUSTACK. По мере миграции инфраструктуры на отечественные платформы зарубежные продукты теряют совместимость. Многие российские государственные порталы (Госуслуги), системы сдачи отчётности (ФНС, Социальный фонд) и банковские шлюзы работают через

отечественные криптографические стандарты (ГОСТ); иностранные сервисы могут не соответствовать данным требованиям.

5. Невозможность миграции при разрыве.

Иностранные системы используют закрытые проприетарные технологии, которые не всегда совместимы с другими решениями. Миграция — это сложный процесс переноса огромных массивов информации из одной структуры хранения в другую; глубокая интеграция с проприетарными технологиями VMware, Veeam, Microsoft Exchange делает миграцию сложной и дорогой и создаёт потенциальные риски для непрерывности бизнеса в случае блокировки или прекращения поддержки.

6.1.2. Риски кибербезопасности

1. Эксплуатация неустранённых CVE.

Зарубежное программное обеспечение во всех четырёх рассматриваемых классах является приоритетной мишенью вредоносных программ. Российские пользователи без обновлений уязвимы постоянно. Ключевые активно эксплуатируемые уязвимости включают:

- Veeam CVE-2023-27532 (раскрытие учётных данных через TCP 9401) — патч 07.03.2023, в CISA KEV с 22.08.2023; эксплуатируется FIN7, Cuba, Akira, Qilin, EstateRansomware, BlackCat, BlackMatter.
- Veeam CVE-2024-40711 (CVSS 9.8, RCE через десериализацию) — патч 04.09.2024, в CISA KEV с 17.10.2024; Sophos X-Ops зафиксировал минимум 4 атаки Akira/Fog в течение месяца после публикации PoC.
- Veeam CVE-2025-23120 (CVSS 9.9, RCE для domain-joined серверов) — патч в 12.3.1 (март 2025).
- Commvault CVE-2025-3928 (zero-day, эксплуатировался государственными хакерами с февраля 2025 для взлома самой Microsoft Azure-среды Commvault).
- Commvault CVE-2025-34028 (pre-auth RCE) — патч 10.04.2025, в CISA KEV с 02.05.2025.
- Цепочка Commvault CVE-2025-57788/57789/57790/57791 (август 2025, bypass auth + privilege escalation + RCE через webshell).

- VMware CVE-2021-21974 (ESXiArgs) — массовая кампания, более 3 800 серверов зашифровано в феврале 2023 года.
- Citrix CVE-2023-4966 (CitrixBleed) — активно эксплуатируется LockBit 3.0.
- Microsoft Exchange — уязвимость BDU:2023-07515, по предупреждению ФСТЭК России затронула ~77 тыс. серверов в России.

2. Невозможность сертификации ФСТЭК России и отсутствие проверки на НДВ.

Компании уровня Google, Microsoft, VMware, Veeam никогда не откроют свой исходный код для российских регуляторов. Это их главная коммерческая тайна и интеллектуальная собственность. Без анализа кода полноценная сертификация невозможна. Проверка только «чёрного ящика» (готового продукта) не даёт гарантий отсутствия скрытых функций. Зарубежное ПО не проходит проверку ФСБ России/ФСТЭК России на отсутствие недокументированных возможностей (НДВ).

3. Закладки, недокументированные функции и недоверенный код.

Получение обновлений через посредников из третьих стран (Дубай, Армения, Казахстан) уязвимо с точки зрения возможной загрузки бэкдора, специально созданного для России. Существуют так называемые «спящие» (sleep) уязвимости — о них знают только хакеры или спецслужбы; они могут использоваться годами. Если компания не обновляет программы, такие «дыры» в безопасности остаются открытыми.

4. Атаки шифровальщиков на инфраструктуру.

Согласно статистическим данным, в 2024 году «Лаборатория Касперского» отразила более 500 тысяч атак вирусов-шифровальщиков на российские компании. Целые группировки (Crypt Ghouls, Twelve, HeadMare, Comet, Werewolves, CyberSec's и другие) специализируются на полном уничтожении ИТ-инфраструктуры, включая виртуализацию, почту и резервные копии. Современные группы шифровальщиков целенаправленно уничтожают резервные копии перед шифрованием основного блока данных.

5. Шпионаж иностранных спецслужб.

Как только данные (особенно персональные) попадают на сервер в США или Европе, они попадают под действие законов этих стран (например, CLOUD Act в США). Это означает, что иностранные спецслужбы могут получить к ним доступ легально, без

уведомления компании-владельца данных. Невозможность отзыва данных с зарубежных серверов с гарантией 100 %: копии могут остаться в кэшах, бэкапах или логах провайдера.

6. Утечка телеметрии за рубеж.

Современные зарубежные продукты по умолчанию отправляют телеметрию в юрисдикции США, ЕС или Израиля: VMware vSphere CEIP, Microsoft Diagnostic Data, Oracle Configuration Manager. Содержание передаваемых данных не контролируется пользователем и может включать сведения о конфигурации, версиях, идентификаторах. Дополнительной угрозой являются мисконфигурации провайдера: в 2023 году публично раскрыт инцидент с Microsoft 38 TB leak — утечка через мисконфигурацию SAS-токена в Azure.

7. Атаки через цепочку поставок (supply chain).

Зарубежное программное обеспечение неоднократно использовалось как вектор атаки через цепочку поставок: SolarWinds SUNBURST в декабре 2020 года (18 000 организаций, APT29), Kaseya VSA REvil в июле 2021 года, 3CX в марте 2023 года (Lazarus), MOVEit в мае 2023 года (Cl0p, 93,3 млн человек), мейнтейнерская закладка xz-utils CVE-2024-3094 в марте 2024 года. Заражение происходит через легитимные обновления, которые проходят все средства проверки. Известны и более ранние случаи — Juniper ScreenOS CVE-2015-7755/7756 (изменение Q в Dual_EC_DRBG, NSA-связанный бэкдор), уязвимости Pulse Secure (эксплуатировались APT5/APT15 в 2020—2024 годах).

8. Криптографическое несоответствие ГОСТ.

Зарубежные платформы не реализуют российские криптографические стандарты ГОСТ. Сервисы управления ключами (BYOK/HYOK) Azure Key Vault, AWS KMS не поддерживают ГОСТ. Шифрование томов и объектов в зарубежных продуктах (vSAN encryption AES-256/XTS, S3 encryption) формально не соответствует требованиям к КИИ и значимым ГИС.

9. Зависимость от зарубежных CDN/DNS и сетевой инфраструктуры.

Роскомнадзор 7 ноября 2024 года рекомендовал отказаться от использования Cloudflare; с 9 июня 2025 года введены DPI-ограничения, в результате которых трафик к Cloudflare упал более чем на 50 %. 15 апреля 2024 года заблокирован AWS.

Зависимость от зарубежных CDN/DNS-провайдеров создаёт риск внезапной недоступности сервисов.

6.1.3. Юридические и регуляторные риски

1. Нарушение Указа Президента Российской Федерации № 166.

С 1 января 2025 года использование иностранного программного обеспечения на значимых объектах критической информационной инфраструктуры (ЗОКИИ) для государственных органов и заказчиков 223-ФЗ — прямое нарушение Указа Президента РФ. Федеральный закон № 58-ФЗ от 07.04.2025 (вступил в силу 01.09.2025) дополнительно закрепил требования к ПО на уровне федерального закона. Федеральный закон № 325-ФЗ от 31.07.2025 (с 01.03.2026) ввёл реестр доверенного ПО для КИИ. По данным ФСТЭК России, в 2025 году возбуждено более 400 дел по ст. 19.7.15 КоАП.

2. Нарушение Указа Президента Российской Федерации № 250.

Запрет средств защиты информации из недружественных стран действует с 01.01.2025. Системы всех четырёх рассматриваемых классов могут квалифицироваться как СЗИ: backup-системы — по сертификации ФСТЭК России (категория «Средства резервного копирования»), почтовые системы — через встроенные функции антивирусной защиты и DLP, средства виртуализации — через интегрированные модули защиты гипервизора, облачные платформы — через интегрированные СЗИ от НСД, антивирусные средства и средства доверенной загрузки. Изменения Указом № 500 от 13.06.2024 распространили запрет на услуги и работы по защите информации.

3. Нарушение требований по КИИ (ФЗ-187).

Использование иностранных продуктов в критических отраслях (энергетика, транспорт, финансы) создаёт идеальный канал для промышленного шпионажа (кража чертежей, планов), сбора данных для подготовки кибератак, дестабилизации работы инфраструктуры через компрометацию учётных записей администраторов.

4. Нарушение локализации персональных данных (ст. 18 ФЗ-152).

Персональные данные граждан Российской Федерации запрещено хранить и обрабатывать на серверах, находящихся за пределами РФ. Это требование напрямую затрагивает почтовые системы (содержат большие массивы ПДн), системы резервного

копирования (хранят их копии) и системы виртуализации (обеспечивают работу систем, обрабатывающих ПДн).

5. Уголовная ответственность по ст. 274.1 УК РФ.

«Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» — до 10 лет лишения свободы при тяжких последствиях. Если из-за необновлённого зарубежного решения на ЗОКИИ произойдёт инцидент (ransomware, утечка), при экспертизе ФСБ России установит нарушение правил эксплуатации (ч. 3 ст. 274.1) — 2–5 лет лишения свободы; при тяжких последствиях по ч. 5 — до 10 лет. Реальные приговоры: Самара (ВНИИ «Сигнал», 2023), Кировская область (инженер «дочки» Россетей, 2024 — отключение 38 населённых пунктов).

6. Оборотные штрафы за утечки ПДн (ФЗ № 420-ФЗ от 30.11.2024).

С 30 мая 2025 года действуют новые штрафы по ст. 13.11 КоАП: утечка более 100 000 субъектов или более 1 млн идентификаторов — 10–15 млн руб.; биометрия — 15–20 млн руб.; повторная утечка — 1–3 % годовой выручки, минимум 20 млн — максимум 500 млн руб. Дела рассматривает арбитражный суд. Федеральный закон № 421-ФЗ (с 11.12.2024) ввёл уголовную ответственность до 10 лет лишения свободы. Если утечка происходит через скомпрометированное зарубежное ПО без обновлений — это отягчающее обстоятельство (заведомо ненадлежащая защита).

7. Санкционные риски для контрагентов и руководителей.

При закупке через серый импорт компания и её руководители рискуют попасть под вторичные санкции OFAC (расширены 12.06.2024) и EU criminal liability через Directive 2024/1226. Иностранные банки и компании, через которые российские компании обходят санкции, сами попадают под вторичные санкции США и ЕС.

6.1.4. Операционные риски

1. Падение качества технической поддержки и серый импорт.

Реальная техническая поддержка отсутствует с 2022 года. Поддержка через интеграторов в Армении, Казахстане, ОАЭ — вне SLA, не покрывает критические инциденты, не имеет SLA-гарантий. Активация лицензий через третьи юрисдикции попадает под вторичные санкции OFAC после расширения 12.06.2024. В случае

серьёзного сбоя или взлома обратиться в официальную поддержку невозможно. Администратору приходится искать решение на форумах или в сообществах, что неэффективно при критических инцидентах.

2. Зависимость от ключевых специалистов и потеря компетенций.

Уход вендоров привёл к закрытию российских R&D-центров и тренинг-центров. Учебные центры VMware, Citrix, Veeam закрыты, новые специалисты не проходят сертификацию. Сертифицированные VMCE-инженеры (Veeam Certified Engineer), VCP (VMware Certified Professional) сертификации не получают, экспертиза устаревает. Произошёл отток опытных инженеров. Через 2—3 года компетенция полностью исчезнет. Специалисты по западным системам не могут сразу работать с российскими аналогами (zVirt, «Базис», RuBackup, RuPost) — рынок таких экспертов пока не насыщен.

3. Сложности интеграции с российской инфраструктурой.

При миграции инфраструктуры на Astra Linux, РЕД ОС, zVirt, «Брест», Postgres Pro зарубежные агенты резервного копирования, почтовые серверы и системы виртуализации не имеют официальной поддержки. Тестирование совместимости компании проводят на свой страх и риск.

4. Финансовые потери от простоев.

При отказе системы и невозможности восстановления данных у предприятий возникают прямые финансовые потери. Примеры:

- «Винлаб»/Novabev (14.07.2025): простой более 4 суток, 2 000+ магазинов парализованы, оценка убытков более 1 млрд руб., акции упали на 5,5 %. По данным «Неэлектронной коммерции», 1 день простоя ритейлера стоил 100 млн руб.
- СДЭК (26.05.2024): остановка 3—4 суток на выручке 34 млрд руб./год; уничтожены бэкапы (по заявлению хакеров, администраторы делали РК «раз в полгода»).
- RuTube (9 мая 2022): атака Anonymous, уничтожено 75 % баз и около 90 % резервных копий и кластеров для восстановления БД. Восстановление заняло несколько суток, оценка ущерба — 100—150 млн руб. (Forbes).

- ВСК (12.11.2025): массированная атака на страховую компанию, нарушена работа сайта и приложений, корпоративная почта выведена из строя на неделю.

5. Падение надёжности.

Без официальной поддержки (hot-fix) при сбоях приходится искать решения на форумах. Для крупных компаний это означает снижение доступности сервисов с 99,99 % до 99,9 % и ниже, что соответствует увеличению допустимого простоя в десятки раз.

6.1.5. Экономические риски

1. Потеря инвестиций в существующие лицензии.

Корпоративные клиенты ранее заплатили за многолетние лицензии Veeam, Commvault, Veritas, VMware, Microsoft Exchange (стоимость для крупного банка — десятки и сотни миллионов рублей). С прекращением поддержки и блокировкой обновлений экономическая ценность падает практически до нуля при необходимости срочной замены.

2. Стоимость экстренной миграции.

Сроки полной замены крупной инфраструктуры составляют от 12—24 месяцев, бюджет — от десятков до сотен миллионов рублей в зависимости от класса ПО и масштаба пользовательской базы (см. таблицу 5 для оценки миграции почтовой инфраструктуры). Полноценная миграция требует не менее года.

3. Рост стоимости параллельного импорта и серых каналов.

Конечная стоимость лицензий, приобретаемых через третьи страны, может превышать стоимость официальной на 30—100 %. Увеличение происходит и за счёт затрат на посредников в цепочке продаж, валютных рисков, а также дополнительных правил продаж — вторичных санкций для контрагентов из Турции, Казахстана, ОАЭ после расширения OFAC от 12.06.2024. В 2022 году наценки доходили до 20—30 %.

4. Курсовые риски ₽/$ и высокая стоимость.

Вендоры или их официальные партнёры транслируют цену напрямую по текущему курсу. Российские клиенты ранее получали предложения по специальной цене и с защитой от колебаний курса; с 2022 года такие условия не предоставляются, и все цены в долларах или евро пересчитываются в рубли по текущему курсу.

5. Двойные затраты.

Компания продолжает нести все расходы, связанные с иностранным вендором, и одновременно начинает нести новые расходы на внедрение и лицензирование российских аналогов. Это создаёт «бюджетные ножницы» в период миграции.

6. Рост стоимости лицензий и принуждение к подписке.

Бесплатные тарифы часто имеют ограничения (по объёму ящика или количеству писем). Сервис может перевести организацию на платную подписку или отключить функции, что потребует незапланированных трат из бюджета.

7. Stranded assets — потеря инвестиций в инфраструктуру.

Помимо лицензий, обесценивается смежное оборудование и инвестиции в инфраструктуру. Cisco в 2022 году списала оборудование на ₽3 млрд. Перевод инсталляций VMware в legacy-режим де-факто означает амортизацию выделенных под них серверных мощностей с пониженной отдачей и невозможность развития платформы. Аналогичные эффекты возникают по всем рассматриваемым классам ПО.

8. Невозможность взыскания компенсаций с ушедших вендоров.

Юридическая защита прав в отношении ушедших вендоров крайне ограничена. К ООО «Виэмваре Рус» (ликвидируемое юридическое лицо) подано лишь два иска (на ₽1 тыс. и ₽224,6 тыс.). Ряд частичных побед — арест ₽778 млн по делу «Талмер» / «Делл», ₽73,2 млн по делу «АСАП софт» / SAP — не образует устойчивой практики. Серый импорт по Постановлению Правительства РФ № 506 формально не покрывает облачные лицензии, что создаёт риск исков по ст. 14.10 КоАП и ст. 1252 ГК.

6.1.6. Репутационные риски

Репутационные риски в условиях санкционного давления и регуляторного контроля приобретают особое значение, поскольку их реализация одновременно затрагивает несколько контуров: общественное доверие, отношения с контрагентами, доступ к финансовым рынкам и капитализацию компании.

1. Публичный инцидент с раскрытием использования зарубежного ПО на КИИ.

Инцидент через зарубежное программное обеспечение на ЗОКИИ — двойной репутационный удар: общественный (утечка/простой) и регуляторный (нарушение Указа № 166). СМИ освещают такие случаи особенно остро (RuTube, СДЭК, «Винлаб»,

«Аэрофлот»). Инциденты на иностранном ПО после 1 января 2025 года вызывают двойной негатив: за сам сбой и за использование запрещённого софта.

2. Потеря доверия клиентов после утечки персональных данных.

После утечек «Яндекс.Еды», «Гемотеста», СДЭК зафиксированы коллективные иски (33 заявителя по 100 тыс. руб. к «Яндекс.Еде»). С 30.05.2025 действуют оборотные штрафы до 500 млн руб. Финтех-сегмент особенно чувствителен: после крупной утечки клиенты массово закрывают счета. Утечки данных ведут к оттоку клиентов в B2C-сегменте.

3. Отказ контрагентов работать с компанией, не выполнившей импортозамещение.

Всё чаще государственные компании, государственные корпорации, значимые банки требуют подтверждения полной независимости от иностранных средств защиты информации. Отсутствие такого подтверждения ведёт к отказу в заключении договора, что особенно критично для подрядчиков и поставщиков.

4. Негативное освещение в отраслевых средствах массовой информации.

CNews, TAdviser, Anti-Malware.ru, SecurityLab публикуют разборы инцидентов с указанием вендоров. Использование «ушедшего» Veeam в финансовом секторе или эксплуатация Microsoft Exchange без обновлений — повод для критической публикации.

5. Снижение инвестиционной привлекательности и доверия акционеров.

Использование иностранного программного обеспечения, не соответствующего требованиям регулятора, отражается в отчётности компании как существенный непрорезервированный регуляторный и операционный риск. Раскрытие этого риска в ходе комплексной проверки бизнеса или независимого аудита приводит к снижению доверия акционеров, особенно институциональных, и негативно сказывается на оценке корпоративного управления (ESG/корпоративные рейтинги). В практике крупных публичных компаний раскрытие подобных фактов сопровождается кратковременным, но ощутимым снижением котировок.

6. Падение рыночной стоимости бизнеса.

Регуляторное несоответствие, утечки данных и громкие инциденты непосредственно отражаются на рыночной капитализации публичных компаний и

оценке частных. Кейс «Винлаб»/Novabev (14.07.2025) показателен: после атаки и простоя котировки акций упали на 5,5 % за один день. Накопленный эффект серии инцидентов в отрасли может приводить к структурному переоцениванию рыночной стоимости компаний, продолжающих эксплуатировать неподдерживаемое зарубежное программное обеспечение, причём дисконт сохраняется и после устранения непосредственных последствий инцидента.

7. Увеличение стоимости заёмного капитала.

Кредитные организации и инвесторы при оценке заёмщика учитывают регуляторные и операционные риски, включая сертификационные требования по информационной безопасности. Компании, не соответствующие требованиям Указов № 166 и № 250, требованиям 187-ФЗ и положений ЦБ РФ (716-П, 779-П, 850-П, 851-П, 757-П), относятся к категории повышенного риска. Это приводит к удорожанию кредитов, требованию дополнительного обеспечения, а в отдельных случаях — к прямому отказу в кредитовании. Для эмитентов облигаций — к снижению кредитного рейтинга и росту премии за риск (спреду к ОФЗ).

8. Расширенные риски для бизнеса.

Совокупность репутационных факторов формирует системный риск для бизнеса в целом:

- отказ страховых компаний от заключения договоров киберстрахования или существенное удорожание страховых премий по причине эксплуатации не обновляемого зарубежного ПО;
- снижение позиций в отраслевых рейтингах надёжности и устойчивости;
- ограничение возможностей для слияний и поглощений: контрагент учитывает регуляторное несоответствие как существенный фактор при структурировании сделки и определении цены;
- ухудшение условий взаимодействия с международными партнёрами, осторожно относящимися к компаниям, замешанным в санкционных или регуляторных нарушениях.

6.2. Специфические риски, характерные для отдельных классов программного обеспечения

Помимо общих рисков, описанных в разделе 6.1, каждый из рассматриваемых классов программного обеспечения обладает рисками, обусловленными его функциональным назначением, архитектурой и положением в инфраструктуре предприятия.

6.2.1. Специфические риски почтовых приложений

1. Электронная почта как основная точка входа для целевых атак.

По данным BI.ZONE, 68 % целевых атак начинаются с электронной почты; по данным Positive Technologies — 92 % вредоносной доставки происходит через электронную почту, в 79 % случаев доступ к защищённой информации осуществляется через почту, основанную на психологическом манипулировании людьми; по данным Kaspersky — 42 % начальных компрометаций происходит через уязвимости публичных приложений (преимущественно почтовых). Почтовая система — единственный класс ПО среди рассматриваемых, который ежедневно открыт для миллионов внешних входящих сообщений и таким образом является постоянной целью.

2. Утечка корпоративной переписки и шантаж публикацией.

Корпоративная почта содержит уникальный массив чувствительной информации: коммерческие переговоры, юридически значимые документы, договорные обязательства, кадровые решения, финансовые транзакции. Утечка такого массива не только нарушает законодательство о ПДн, но и наносит прямой ущерб конкурентоспособности. Кампания BI.ZONE «security4real» (август 2022 — 2023) с эксплуатацией ProxyShell (CVE-2021-34473) — характерный пример: десятки российских компаний СМБ-сегмента подверглись эксфильтрации почтовых ящиков с последующим шантажом публикацией данных под видом «аудита безопасности».

3. Фишинг и социальная инженерия.

Иностранные почтовые сервисы являются главной целью мошенников. Злоумышленники рассылают письма от имени руководителей или технической поддержки с просьбой перейти по ссылке или скачать файл. Такие письма часто содержат вирусы-шифровальщики (Medusa, Akira и др.) или программы для кражи

паролей. Positive Technologies и Kaspersky фиксируют устойчивые кластеры атак на российские цели через фишинг от имени Минпромторга, Роскомнадзора, Следственного комитета РФ, Военной прокуратуры. Группировки: Cloud Atlas, XDSpy, Scaly Wolf, Mysterious/Core/Sticky/Paper/Vortex Werewolf, Hellhounds, Dark River, Red Wolf, Head Mare, Silent Crow.

4. Зависимость от почты как канала юридически значимых документов.

Многие российские государственные порталы (Госуслуги), системы сдачи отчётности (ФНС, Социальный фонд) и банковские шлюзы работают через отечественные криптографические стандарты (ГОСТ). Иностранная почта может не обеспечивать поддержку этих стандартов, что приводит к невозможности отправки юридически значимых документов или отчётности прямо из интерфейса почты. Требуются дополнительные манипуляции и стороннее ПО.

5. Потеря исторических архивов.

Иностранные провайдеры подчиняются законодательству своей страны. Они могут предоставить доступ к архивам (даже без уведомления) правоохранительным органам или спецслужбам своей юрисдикции либо ограничить доступ пользователя. Для объекта КИИ это означает потерю контроля над технологическими процессами, историей согласований и критически важной документацией.

6. Взлом аккаунтов и почтовый компромат.

Личные аккаунты, например, сотрудников образовательных учреждений, защищены слабее корпоративных. При компрометации пароля (например, из-за утечки базы данных) злоумышленник получает доступ ко всей переписке, спискам контактов, документам. Он может рассылать письма от имени сотрудника, вымогая деньги или распространяя вредоносные программы. Корпоративные почты сотрудников 94 из 100 крупнейших российских компаний присутствуют в публичных утечках (StopPhish, Forbes, 2024).

6.2.2. Специфические риски систем резервного копирования

1. Невозможность восстановления при крупном инциденте.

Без техподдержки вендора при сложных сценариях восстановления (повреждённая БД, нестандартный сценарий ransomware, проблемы с дедупликацией)

восстановление может оказаться невозможным. Кейс RuTube — 90 % бэкапов уничтожено, восстановление заняло несколько суток без поддержки Veeam/Veritas. У СДЭК — практически полная потеря данных. Это специфический риск именно для систем резервного копирования: их единственное назначение — восстановить данные, и невозможность этого делает их бесполезными.

2. Целенаправленные атаки на резервные копии.

Современные группы шифровальщиков целенаправленно уничтожают резервные копии перед шифрованием основного блока данных. Это специфика, отличающая backup-системы от других классов ПО:

- RuTube (9 мая 2022) — атака Anonymous: уничтожено 75 % баз и около 90 % резервных копий и кластеров для восстановления БД.
- СДЭК (26—29 мая 2024) — группа Head Mare; зашифрованы виртуальные машины на гипервизоре, уничтожены бэкапы.
- Российские группы Comet/Twelve, Werewolves, Head Mare, CyberSec's — двойного назначения: вымогательство + диверсия.

3. Утечки данных через незащищённые backup.

Резервные копии часто содержат персональные данные в открытом виде и хранятся без должного контроля доступа:

- «Яндекс.Еда» (01.03.2022) — утечка 49,4 млн строк (3 SQL-дампа) с ФИО, телефонами, адресами, кодами домофонов.
- «Гемотест» (май 2022) — 30 млн строк ПДн + результаты медицинских анализов, более 300 Гб скачано через скомпрометированную учётную запись сотрудника.
- «Сберлогистика» (2025) — 20,3 млн уникальных телефонов, 17,1 млн e-mail.
- По данным DLBI, в 2024 году в РФ зафиксировано 382 утечки на 438 млн телефонов и 227 млн e-mail (+70 %). За 2023—2025 годы суммарно украдено около 4,5 млрд записей ПДн (TAdviser).

Для зарубежного backup-софта без обновлений риск утечки усиливается через CVE и невозможность применить современные функции защиты (immutable backup, шифрование с актуальными библиотеками).

4. Деградация SLA и нарушение требований ЦБ РФ к RTO/RPO.

Положение ЦБ РФ 779-П вводит порог инцидента в 5 минут; Положение 850-П (с 01.10.2025) требует контрольных показателей деградации, лимитов простоя; инцидент = деградация >5 минут. Положение 757-П требует сертификации прикладного ПО по ОУД4; зарубежные продукты сертификаты потеряли. Без современных функций (mirror-репликация, immutable backup, ML-анализ аномалий) недостижимы целевые RTO/RPO критичных бизнес-процессов. Это специфический регуляторный риск именно для систем резервного копирования в финансовом секторе.

5. Закрытие R&D и потеря узкоспециализированных компетенций.

Уход вендоров привёл к закрытию российских R&D-центров и тренинг-центров. Сертифицированные VMCE-инженеры (Veeam Certified Engineer) сертификации не получают; экспертиза устаревает. Это специфика именно для backup: класс ПО является высокотехнической нишей с длинным циклом подготовки специалистов; через 2—3 года компетенция полностью исчезнет.

6. Несоответствие положениям ЦБ РФ.

Несоответствие Положениям ЦБ РФ 716-П, 779-П, 850-П, 851-П, 757-П специфично для финансового сектора. Положение 850-П (вступило 03.05.2025) с 01.10.2025 требует установки сигнальных и контрольных показателей деградации, лимитов простоя; инцидент определяется как деградация >5 минут. Использование зарубежного backup без поддержки делает невозможной гарантию RTO/RPO. Штрафы по ст. 13.12 КоАП — 10—30 тыс. руб. + приостановка деятельности до 3 мес.; для банков ЦБ может применять предписания, ограничения, штрафы по 86-ФЗ.

6.2.3. Специфические риски систем виртуализации

1. Резкий рост стоимости лицензий VMware после поглощения Broadcom.

После того как VMware была куплена компанией Broadcom, стоимость лицензий резко выросла по всему миру. С апреля 2025 года покупать лицензии стало ещё сложнее:

- минимальный объём покупки увеличен с 16 до 72 ядер процессора;
- на текущий момент лицензии считаются по ядрам (per-core), а не по процессорам (per-CPU);

- введены штрафы за несвоевременное продление лицензии.

С 2024 года Broadcom ввела строгую лицензионную политику. В случае истечения срока действия подписки (поддержки/обновлений) пользователь попадает в категорию «просрочивших продление» (lapsed renewal). Штрафной период (Grace Period) составляет 30 дней с момента окончания подписки для продления на обычных условиях. В течение указанного периода ПО продолжает работать, стоимость стандартная. В случае отсутствия продления лицензии в течение этих 30 дней включается штраф, который составляет +20 % к стоимости продления за каждый год просрочки. Это специфика именно для виртуализации после поглощения Broadcom.

2. Массовая инсталляционная база VMware ESXi с открытыми критическими уязвимостями.

Эксперты по безопасности подтверждают масштаб проблемы: в апреле 2025 года было обнаружено более 40 тысяч серверов VMware ESXi, доступных из интернета и имевших критические уязвимости. Кампания ESXiArgs (февраль 2023) использовала уязвимость CVE-2021-21974 в VMware ESXi: исправление существовало уже два года, но многие компании его не установили — в результате по всему миру было зашифровано более 3 800 серверов. Уязвимость CitrixBleed (CVE-2023-4966, октябрь 2023) активно использовалась группировкой LockBit 3.0; разведка велась с российских IP-адресов. Поскольку Citrix и VMware ушли из России, пользователи не могли получить патч и остались без необходимой защиты.

3. Глубокая интеграция с проприетарными технологиями VMware.

Глубокая интеграция с проприетарными технологиями VMware и зависимость от облачных сервисов активации делают миграцию сложной и дорогой и создают потенциальные риски для непрерывности бизнеса. В отличие от почтовых протоколов (SMTP/IMAP) или форматов данных backup, которые имеют относительно стандартизованные интерфейсы, экосистема VMware (vSphere, vCenter, NSX, vSAN, Tanzu) обеспечивает плотную взаимосвязь компонентов, и разрыв этой экосистемы при миграции на отечественные платформы требует существенной доработки.

4. Атаки шифровальщиков на гипервизоры.

Атака на российскую компанию (группа Muliaka, январь 2024): группировка зашифровала и Windows-серверы, и виртуальную инфраструктуру на базе VMware

ESXi. Атаки группы MorLock (2024) — не менее 9 крупных и средних российских компаний, шифровальщики. Самый крупный публичный инцидент: «Аэрофлот» (июль 2025) — группировки Silent Crow и «Киберпартизаны BY» уничтожили около 7 тысяч серверов «Аэрофлота» (как физических, так и виртуальных) и украли от 12 до 22 ТБ данных. Они взломали контроллер домена, базы данных, почту и гипервизоры. Виртуализация — цель особой ценности, поскольку компрометация одного гипервизора одновременно компрометирует десятки виртуальных машин.

5. Падение надёжности доступности до уровней ниже отраслевых стандартов.

Без официальной поддержки (hot-fix) при сбоях приходится искать решения на форумах. Для крупных компаний это означает снижение доступности сервисов с 99,99 % (52 минуты простоя в год) до 99,9 % (8,76 часа простоя в год) и ниже. В контексте требований ЦБ РФ к финансовым организациям и SLA-обязательств перед клиентами это превращается в постоянное технологическое нарушение.

6. Дефицит специалистов VMware и Citrix.

Учебные центры VMware и Citrix закрыты, новые специалисты не проходят сертификацию. Произошёл отток опытных инженеров. Специалисты по западным системам не могут сразу работать с российскими аналогами (zVirt, «Базис», ROSA Virtualization, «Брест») — рынок таких экспертов пока не насыщен.

6.2.4. Специфические риски облачных платформ

1. Дистанционная деактивация и блокировка аккаунтов.

Для облачных платформ риск удалённого отзыва лицензий и прекращения работоспособности продукта (remote kill switch) реализуется в наиболее острой форме, поскольку платформа полностью находится под контролем вендора. Документированные случаи: Autodesk — массовая блокировка AutoCAD/3ds Max/Revit 17–18 апреля 2024 года (включая бессрочные лицензии); Cisco — деактивация аккаунтов в 2022 году; Adobe — аннулирование ключей; VMware — частичная деактивация аккаунтов под санкциями. С 1 ноября 2025 года VMware VCF 9 и License Portability работают только через 40 Certified Cloud Services провайдеров, среди которых нет российских.

2. Зависимость от облачных регионов и вендорских CDN/DNS.

Облачные сервисы могут быть отключены санкциями быстрее любых on-premise решений: Oracle Cloud для Российской Федерации отключён 12 марта 2022 года; AWS заблокирован Роскомнадзором 15 апреля 2024 года; Google Cloud Platform прекратил регистрацию 10 марта 2022 года; Microsoft Azure отключил 9 сервисов 12 сентября 2024 года. Параллельно: Роскомнадзор 7 ноября 2024 года рекомендовал отказаться от Cloudflare; с 9 июня 2025 года введены DPI-ограничения, в результате которых трафик к Cloudflare упал более чем на 50 %.

3. Зависимость от зарубежных репозиториев и реестров образов.

Массовая загрузка контейнерных образов из зарубежных регистров (Docker Hub, AWS ECR Public, Google Container Registry) для российских пользователей часто оказывается невозможной, что делает невозможной нормальную DevOps-эксплуатацию. Разработчики переходят на российские и китайские альтернативы, что требует адаптации CI/CD-процессов.

4. Прямое нарушение Положений ЦБ для финансового сектора при размещении в иностранных облаках.

Размещение данных финансовых организаций в зарубежных облаках напрямую противоречит положениям ЦБ РФ. Возможные меры регулятора: предписания, увеличение резервов, ограничение операций; в крайнем случае — отзыв лицензии (ст. 74 ФЗ-86). Кроме того, размещение государственных информационных систем в иностранных облаках исключает возможность аттестации по Приказу ФСТЭК России № 17/117 — обязательной сертификации СЗИ для классов К1, К2.

5. Трансграничная передача персональных данных через зарубежные облака.

Размещение информационных систем, обрабатывающих персональные данные, в зарубежных облаках квалифицируется как трансграничная передача ПДн со всеми вытекающими ограничениями. Штрафы по ст. 13.11 ч. 8 КоАП — до ₽6 млн (повторно до ₽18 млн); оборотные штрафы до 3 % выручки. Частный риск облачного сценария по сравнению с on-premise.

6. Невозможность интеграции с ГосСОПКА и НКЦКИ.

Российские системы мониторинга и реагирования на инциденты (SIEM-системы MaxPatrol, KUMA, RuSIEM, KOMRAD) имеют ограниченную поддержку парсеров для новых версий VMware vSphere и других зарубежных облачных платформ.

Шифрованные каналы передачи в ГосСОПКА требуют использования сертификатов Минцифры России (НУЦ), не поддерживаемых зарубежными облаками штатно. Коннекторы устаревают и не обновляются.

7. Эксплуатируемые критические CVE без возможности патчей.

Облачные продукты являются приоритетной мишенью атак с использованием неустранённых уязвимостей: CVE-2024-37085 эксплуатировалась группировками Black Basta и Akira; CVE-2023-34048 — 0-day от UNC3886, эксплуатировалась около 2 лет; Citrix Bleed CVE-2023-4966 (LockBit на Boeing, ICBC, DP World). Для российских пользователей зарубежных облачных продуктов получение патчей через customerconnect и аналогичные порталы недоступно.

8. Прекращение жизненного цикла продуктов (EOL/EOS) и принудительный отказ.

Зарубежные облачные платформы регулярно объявляют о прекращении жизненного цикла продуктов: Red Hat Virtualization EOL 31 августа 2026 года; vSphere 7.0 — End of General Support 2 апреля 2025 года; oVirt upstream закрыт Red Hat в мае 2024 года; Red Hat HCI for Virtualization EOL 31 октября 2024 года. После EOL пользователь юридически и технически не имеет права на эксплуатацию продукта, либо лишается базовой технической поддержки.

9. Отказ интеграторов от обслуживания зарубежных облачных решений.

Крупные российские интеграторы — «Т1 Интеграция», «Крок», IBS, «Инфосистемы Джет» — переориентируются на российские продукты в 2023—2025 годах. Экспертиза по новым версиям VMware vSphere 8 / VCF 9 не наращивается. Для облачных проектов это означает невозможность найти подрядчика для миграции, апгрейда или поддержки.

10. Невозможность взыскания компенсаций по SLA.

ВТБ, Сбер, Газпром фактически работают без вендорских SLA с 2022 года. ООО «Виэмваре Рус» в ликвидации; иски подаются на символические суммы (₽1 тыс., ₽224,6 тыс.). Это специфическая для облачных сервисов проблема: модель IaaS/PaaS/SaaS изначально построена на гарантиях провайдера, и потеря этих гарантий обесценивает экономическую модель сервиса.

11. Двойное финансирование и масштаб переходных бюджетов.

Для облачной миграции крупных потребителей характерны существенные параллельные бюджеты: ВТБ — ₽90 млрд за 4 года, в том числе более ₽50 млрд в 2024 году; Yandex Cloud — ₽42 млрд в 2025–2026 годах; «Базис» — ₽700 млн на R&D. Это специфика облачной миграции: одновременная закупка иностранных и российских мощностей с длительным периодом параллельной эксплуатации.

12. Сложность экстренного восстановления при инцидентах.

Кейсы массовых инцидентов в облачной инфраструктуре особенно показательны: ESXiArgs (февраль 2023) — массовые потери данных; Storm-0506 (атаки через CVE-2024-37085 в 2024–2025 годах). Для российских клиентов отсутствует возможность обращения в Premier Support вендора, что делает восстановление принципиально сложнее. Кейс ICL Group: миграция Nutanix → zVirt требует выключения виртуальных машин (downtime 7–10 минут на ВМ).

13. Утрата доверия клиентов при компрометации данных в облаке.

Снижение доверия особенно выражено в облачных сервисах: Snowflake-Ticketmaster — 560 млн записей; Snowflake-AT&T — выкуп $370 000 плюс многомиллиардные иски. Поскольку облачная модель строится на доверии к провайдеру, репутационный ущерб от компрометации существенно превышает аналогичный для on-premise решений.

6.3. Сводная матрица рисков по классам программного обеспечения

Сводное представление рисков с разбиением на общие и специфические для каждого класса прикладного программного обеспечения приведено в таблице 15.

Табл. 15. Сводная матрица рисков по категориям и классам ПО

Категория	Риск	Почта	СРК	Виртуализация	Облака
Технологический	Прекращение обновлений и патчей	✓	✓	✓	✓
	Истечение лицензий, невозможность продления	✓	✓	✓	✓

Категория	Риск	Почта	СРК	Виртуализация	Облака
	Дистанционное отключение, блокировка облачных сервисов	✓	✓	✓	✓
	Несовместимость с российскими ОС/инфраструктурой	✓	✓	✓	✓
	Невозможность миграции при разрыве, vendor lock-in	✓	✓	✓	✓
	Зависимость от ГОСТ-криптографии для юридически значимых документов	✓	—	—	—
	Глубокая интеграция с проприетарной экосистемой VMware	—	—	✓	—
	Зависимость от зарубежных репозиториев и реестров образов	—	—	—	✓
	Прекращение жизненного цикла продукта (EOL/EOS), принудительный отказ	—	—	—	✓
Кибербезопасности	Эксплуатация неустранённых CVE	✓	✓	✓	✓

Категория	Риск	Почта	СРК	Виртуализация	Облака
	Невозможность сертификации ФСТЭК России / НДВ	✓	✓	✓	✓
	Закладки, недокументированные функции, supply chain	✓	✓	✓	✓
	Атаки шифровальщиков на инфраструктуру	✓	✓	✓	✓
	Шпионаж иностранных спецслужб (CLOUD Act, PRISM)	✓	✓	✓	✓
	Утечка телеметрии за рубеж (CEIP, Diagnostic Data)	✓	✓	✓	✓
	Криптографическое несоответствие ГОСТ	✓	✓	✓	✓
	Зависимость от зарубежных CDN/DNS (Cloudflare, AWS)	✓	✓	✓	✓
	Электронная почта как точка входа для целевых атак (68 %)	✓	—	—	—
	Шантаж публикацией корпоративной переписки	✓	—	—	—

Категория	Риск	Почта	СРК	Виртуализация	Облака
	Фишинг и социальная инженерия	✓	—	—	—
	Целенаправленные атаки на резервные копии (уничтожение бэкапов)	—	✓	—	—
	Утечки ПДн через незащищённые backup	—	✓	—	—
	Атаки шифровальщиков на гипервизоры (компрометация всех ВМ)	—	—	✓	—
	Массовая инсталлбаза ESXi с открытыми CVE (ESXiArgs, CitrixBleed)	—	—	✓	—
	Невозможность интеграции с ГосСОПКА / НКЦКИ	—	—	—	✓
Юридический и регуляторный	Нарушение Указа № 166 (запрет иностранного ПО на ЗОКИИ)	✓	✓	✓	✓
	Нарушение Указа № 250 (запрет СЗИ из недружественных стран)	✓	✓	✓	✓

Категория	Риск	Почта	СРК	Виртуализация	Облака
	Нарушение требований по КИИ (ФЗ-187)	✓	✓	✓	✓
	Нарушение локализации ПДн (ст. 18 ФЗ-152)	✓	✓	✓	✓
	Уголовная ответственность ст. 274.1 УК РФ	✓	✓	✓	✓
	Оборотные штрафы за утечки ПДн (ФЗ-420)	✓	✓	✓	✓
	Санкционные риски (вторичные санкции OFAC, EU)	✓	✓	✓	✓
	Несоответствие Положениям ЦБ РФ 716-П, 779-П, 850-П, 851-П, 757-П	—	✓	—	✓
	Невозможность аттестации ГИС (Приказ ФСТЭК России № 17/117)	—	—	—	✓
	Трансграничная передача ПДн через зарубежные облака	—	—	—	✓
	Нарушение лицензионного соглашения Broadcom	—	—	✓	✓

Категория	Риск	Почта	СРК	Виртуализация	Облака
	(EULA), деавторизация				
	Невозможность защиты прав в иностранных юрисдикциях	✓	✓	✓	✓
Операционный	Падение качества техподдержки и серый импорт	✓	✓	✓	✓
	Зависимость от ключевых специалистов и потеря компетенций	✓	✓	✓	✓
	Сложности интеграции с российской инфраструктурой	✓	✓	✓	✓
	Финансовые потери от простоев	✓	✓	✓	✓
	Падение надёжности (с 99,99 % до 99,9 % и ниже)	✓	✓	✓	✓
	Деградация SLA и нарушение требований ЦБ к RTO/RPO	—	✓	—	—

Категория	Риск	Почта	СРК	Виртуализация	Облака
	Невозможность восстановления при крупном инциденте	—	✓	—	✓
	Потеря исторических архивов корпоративной переписки	✓	—	—	—
	Зависимость от облачных регионов, отключаемых санкциями	—	—	—	✓
	Невозможность взыскания компенсаций по SLA	✓	✓	✓	✓
	Отказ интеграторов от обслуживания зарубежных решений	✓	✓	✓	✓
Экономический	Потеря инвестиций в существующие лицензии	✓	✓	✓	✓
	Stranded assets — потеря инвестиций в инфраструктуру	✓	✓	✓	✓
	Стоимость экстренной миграции (12–24 мес.)	✓	✓	✓	✓
	Рост стоимости параллельного импорта (+30–100 %)	✓	✓	✓	✓

Категория	Риск	Почта	СРК	Виртуализация	Облака
	Курсовые риски ₽/$, высокая стоимость	✓	✓	✓	✓
	Двойные затраты в период миграции	✓	✓	✓	✓
	Невозможность взыскания компенсаций с ушедших вендоров	✓	✓	✓	✓
	Резкий рост стоимости лицензий Broadcom (per-core, мин. 72 ядра, штрафы +20 %/год)	—	—	✓	✓
	Двойное финансирование облачных миграций (масштабные параллельные бюджеты)	—	—	—	✓
Репутационный	Публичный инцидент с раскрытием иностранного ПО на КИИ	✓	✓	✓	✓
	Потеря доверия клиентов после утечки ПДн	✓	✓	✓	✓
	Отказ контрагентов работать с компанией	✓	✓	✓	✓

Категория	Риск	Почта	СРК	Виртуализация	Облака
	без импортозамещения				
	Негативное освещение в отраслевых СМИ	✓	✓	✓	✓
	Снижение инвестиционной привлекательности и доверия акционеров	✓	✓	✓	✓
	Падение рыночной стоимости бизнеса	✓	✓	✓	✓
	Увеличение стоимости заёмного капитала	✓	✓	✓	✓
	Расширенные риски для бизнеса (страхование, рейтинги, M&A)	✓	✓	✓	✓

Условные обозначения: «✓» — риск проявляется одинаково во всех четырёх классах ПО; «✓» — риск имеет специфический характер для данного класса; «—» — риск не характерен для данного класса либо проявляется опосредованно через общие риски.

7. Заключение и общие выводы

7.1. Положение российского рынка по четырём классам ПО

Анализ четырёх классов прикладного программного обеспечения — почтовых приложений, систем резервного копирования, систем виртуализации и облачных платформ — за период 2019–2026 годов показывает общую закономерность развития российского рынка.

До 2022 года все четыре рассматриваемых класса характеризовались доминированием зарубежных решений: до 90 % рынка систем резервного копирования (Veeam — более 50 %), до 95—96 % рынка виртуализации (VMware — около 80 % серверной базы, ~80 тыс. хостов), 70—80 % рынка корпоративной почты (Microsoft Exchange/O365), 25—30 % рынка облачных сервисов в 2018 году занимали зарубежные провайдеры (Microsoft Azure, AWS, Google Cloud). Российские решения занимали маргинальные доли, играли роль нишевых продуктов и не рассматривались как полноценная альтернатива.

После марта 2022 года практически все западные поставщики систем резервного копирования и виртуализации, крупнейшие облачные сервисы Microsoft и Google и большинство западных IaaS/PaaS-провайдеров заявили о своём уходе и официально покинули российский рынок. Это привело к радикальному перераспределению структуры рынка, ускорило развитие российских решений и создало новый класс рисков, связанных с продолжением эксплуатации зарубежных продуктов в условиях полного отсутствия легальной поддержки.

К 2025—2026 годам российские решения достигли функционального соответствия с зарубежными аналогами:

- на рынке систем резервного копирования доля российских решений превысила 70 %, лидер «Кибер Бэкап» занимает более 80 % сегмента;
- на рынке систем виртуализации доля российских поставщиков выросла до 80 % в новых продажах, при этом VMware всё ещё занимает около 40 % серверов в эксплуатации;
- на рынке корпоративной почты доля российских вендоров достигла 58 %, при этом Microsoft Exchange сохраняет ~50 % инсталляционной базы;
- на рынке облачных платформ доля иностранных провайдеров обрушилась с 25—30 % до менее 1 % к 2025 году; сформирован пул зрелых российских провайдеров (Cloud.ru, Yandex Cloud, Selectel, MWS, VK Cloud, РТК-ЦОД, Рег.облако, DataLine, Linx Cloud) с аттестациями ФСТЭК России до УЗ-1 и К1.

7.2. Унаследованная инсталляционная база как основной источник риска

Ключевая особенность ситуации к 2025—2026 годам, общая для всех четырёх классов программного обеспечения, состоит в одновременном сосуществовании двух процессов:

- активного роста доли российских решений в новых продажах;
- сохранения значительной унаследованной зарубежной инсталляционной базы, эксплуатируемой без официальных обновлений и поддержки.

По всем четырём классам прикладного программного обеспечения совокупная доля крупного бизнеса, продолжающего использование западных решений, закупленных в период до 2022 года, составляет не менее 30 % (для облачного сегмента доля неофициального использования зарубежных платформ оценивается до 20 %, причём лидирует ИТ-сфера и разработка). Несущественная разница в динамике объёмов затрат крупнейших российских потребителей с 2022 по 2025 годы может свидетельствовать о фактическом использовании ранее приобретённых иностранных решений вместо перехода на отечественные аналоги. Это особенно показательно в сравнении с мировыми показателями, демонстрировавшими двухкратный рост за тот же период.

7.3. Совокупная картина рисков

С учётом текущего статуса зарубежных решений и вендоров, эксплуатация неподдерживаемых иностранных решений во всех четырёх классах прикладного программного обеспечения влечёт за собой существенные риски, носящие системный характер. Шесть категорий рисков — технологические, кибербезопасности, юридические и регуляторные, операционные, экономические, репутационные — реализуются одновременно и взаимно усиливают друг друга.

Общий каркас рисков един для всех классов: невозможность получения обновлений, отсутствие легальной техподдержки, прямое нарушение требований Указов Президента РФ № 166 и № 250, потенциальная уголовная ответственность по ст. 274.1 УК РФ, оборотные штрафы по ФЗ-420, санкционные риски, удорожание заёмного капитала и падение рыночной стоимости бизнеса. Этот каркас одинаково

применим к компаниям, эксплуатирующим Microsoft Exchange, Veeam Backup & Replication, VMware vSphere и зарубежные облачные сервисы.

При этом каждый класс программного обеспечения добавляет к общему каркасу набор специфических рисков:

- для почтовых приложений — особая роль электронной почты как точки входа для целевых атак (68 % атак начинаются с email), риск шантажа публикацией корпоративной переписки, фишинговая ориентированность и зависимость от поддержки ГОСТ-криптографии для юридически значимых документов;
- для систем резервного копирования — невозможность восстановления при крупном инциденте, целенаправленные атаки на резервные копии перед основным шифрованием, утечки персональных данных через незащищённые backup, несоответствие положениям ЦБ РФ 716-П, 779-П, 850-П, 851-П, 757-П, потеря узкоспециализированных компетенций (VMCE);
- для систем виртуализации — резкий рост стоимости лицензий после поглощения VMware компанией Broadcom (per-core лицензирование, минимум 72 ядра, штрафы +20 %/год), массовая инсталлбаза ESXi с открытыми критическими уязвимостями (более 40 тыс. серверов в апреле 2025 года), глубокая интеграция с проприетарной экосистемой VMware, особая ценность гипервизора как мишени (компрометация одного гипервизора означает компрометацию десятков виртуальных машин);
- для облачных платформ — наиболее острая форма дистанционного отключения (remote kill switch), зависимость от облачных регионов и зарубежных CDN/DNS (AWS, Cloudflare), невозможность аттестации ГИС в зарубежных облаках, прямой запрет трансграничной передачи персональных данных через ст. 13.11 КоАП, невозможность интеграции с ГосСОПКА и НКЦКИ, отказ интеграторов от обслуживания зарубежных облачных решений, масштабное двойное финансирование облачной миграции (от десятков до сотен млрд руб. для крупных игроков).

7.4. Регуляторное давление и временной горизонт

В период 2024—2026 годов регуляторное давление на использование иностранного программного обеспечения существенно усилилось:

- Указ Президента РФ № 166 — запрет иностранного ПО на ЗОКИИ с 01.01.2025;
- Указ Президента РФ № 250 — запрет СЗИ из недружественных стран с 01.01.2025; Указ № 500 от 13.06.2024 распространил запрет на услуги/работы по защите информации;
- Федеральный закон № 58-ФЗ от 07.04.2025 (вступил 01.09.2025) — закрепление требований к ПО на уровне федерального закона;
- Федеральный закон № 325-ФЗ от 31.07.2025 (с 01.03.2026) — реестр доверенного ПО для КИИ;
- Федеральный закон № 420-ФЗ и № 421-ФЗ — оборотные штрафы за утечки ПДн до 500 млн руб. и уголовная ответственность до 10 лет лишения свободы;
- Постановление Правительства РФ от 28.11.2025 № 1937 — обязательная совместимость СЗИ, СУБД, средств виртуализации с российскими ОС с 01.01.2026;
- Положения ЦБ РФ 716-П, 779-П, 850-П (с 01.10.2025), 851-П, 757-П — требования к надёжности, RTO/RPO, ОУД4-сертификации для финансового сектора.

По данным ФСТЭК России, в 2025 году уже возбуждено более 400 дел по ст. 19.7.15 КоАП. Вынесены реальные приговоры по ст. 274.1 УК РФ (Самара, ВНИИ «Сигнал», 2023 год; Кировская область, 2024 год). Это означает, что регуляторный риск перестал быть теоретическим и трансформировался в практический.

7.5. Итоговый вывод

Положение российского рынка прикладного программного обеспечения в четырёх рассматриваемых классах — почтовые приложения, системы резервного копирования, системы виртуализации и облачные платформы — характеризуется завершением переходного периода: российские решения достигли функциональной зрелости и доминируют в новых продажах, однако значительная унаследованная инсталляционная база зарубежных продуктов продолжает эксплуатироваться без

поддержки и обновлений в условиях растущего регуляторного давления и усиления киберугроз.

Эксплуатация неподдерживаемого иностранного программного обеспечения во всех четырёх классах одновременно создаёт системный риск, не сводящийся к сумме отдельных категорий рисков. Реализация одного риска (например, успешная атака шифровальщика через неустранённую CVE) последовательно активирует другие категории — операционные потери от простоя, юридические последствия по ст. 274.1 УК РФ, оборотные штрафы по ФЗ-420, репутационный ущерб, рост стоимости заёмного капитала и падение рыночной стоимости бизнеса.

Сценарий «продолжать эксплуатацию до отказа» становится экономически неоправданным. Накопленная стоимость рисков (потенциальные штрафы, простои, утечки, уголовная ответственность руководителей, удорожание кредитов) превышает стоимость планомерной миграции на отечественные решения по большинству сценариев.

Для снижения влияния указанных рисков рекомендуется обеспечить планомерный переход на российские решения по всем четырём рассматриваемым классам прикладного программного обеспечения, включая:

- инвентаризацию зависимостей и составление дорожной карты миграции с приоритезацией объектов критической информационной инфраструктуры;
- тестирование предлагаемых на отечественном рынке решений и выбор наиболее подходящих по совокупности технических и экономических критериев;
- поэтапное внедрение российских продуктов с параллельной эксплуатацией зарубежных решений в переходный период с минимизацией двойных затрат;
- полный отказ от использования иностранных недоверенных решений, особенно на объектах критической информационной инфраструктуры, в установленные регуляторами сроки;
- формирование внутренних центров компетенций по российским продуктам и переподготовка специалистов, ранее работавших с зарубежными системами;

- регулярную оценку остаточных рисков по всем шести категориям с обновлением плана миграции по мере изменения регуляторной среды и появления новых уязвимостей в эксплуатируемых зарубежных продуктах.

Настоящий вывод применим в равной мере ко всем четырём рассматриваемым классам прикладного программного обеспечения и определяет общий вектор стратегии информационных технологий российских организаций на горизонте 2026—2028 годов.