

## СОВРЕМЕННЫЕ РЕАЛИИ ЗАЩИТЫ ОБЛАЧНЫХ СЕРВИСОВ

### MODERN REALITIES OF PROTECTION OF CLOUD SERVICES

**O. Vysotin  
A. Vysotin  
A. Kuleshov  
V. Fedorova  
E. Zelentsova**

*Summary.* This article assesses the current situation in the market for services, ensuring the security of information and technical means related to cloud technologies, considers the options that are available in our country when most IT companies leave the Russian market. The components of information protection of cloud services are analyzed.

*Keywords:* cloud services, information protection, hardware, software, sanctions, import substitution, developer, vulnerabilities, comprehensive protection, crisis situation.

**Высотин Олег Валерьевич**

*К.т.н, профессор Академии военных наук,  
Федеральная служба по техническому и экспортному  
контролю ФСТЭК России  
visotin@mail.ru*

**Высотин Андрей Олегович**

*Московский государственный технический  
университет им. Н.Э. Баумана  
visotin\_andrey@mail.ru*

**Кулешов Алексей Игоревич**

*Московский государственный технический  
университет им. Н.Э. Баумана  
kuleshovai@student.bmstu.ru*

**Федорова Вероника Анатольевна**

*К.т.н., доцент, Московский государственный  
технический университет им. Н.Э.  
bmstukf@mail.ru*

**Зеленцова Екатерина Валентиновна**

*К.т.н., доцент, Московский государственный  
технический университет им. Н.Э. Баумана  
katez@mail.ru*

*Аннотация.* В данной статье оценивается текущая ситуация на рынке услуг, обеспечения безопасности информации и технических средств, связанных с облачными технологиями, рассматриваются варианты, которые доступны в нашей стране при уходе большинства IT-компаний с российского рынка. Проанализированы составляющие защиты информации облачных сервисов.

*Ключевые слова:* облачные сервисы, защита информации, технические средства, программное обеспечение, санкции, импортозамещение, разработчик, уязвимости, комплексная защита, кризисная ситуация.

### Введение

**З**а последние 5–10 лет в мире растет количество облачных сервисов, предлагающих пользователям широкий спектр услуг в повседневной или деловой деятельности. Эти сервисы облегчают использование функций, для которых требуются большие технические и экономические средства. Использование облачных сервисов позволяет рядовым пользователям не иметь дома или в офисе большие вычислительные возможности, и как следствие, считается лучшим вариантом для простых пользователей.

В настоящее время на рынке представления информационных услуг сложилась кризисная ситуация, что также влияет на обеспечение безопасности информации и технических средств, связанных с облачными

технологиями [9]. С учетом ухода большинства IT-компаний с российского рынка ситуация еще больше обостряется.

После введения санкций в IT-области возможно использовать только российские и китайские аналоги и следовательно, необходимо дорабатывать составляющие защиты информации облачных сервисов. Рассмотрим и сформулируем какие современные тенденции появляются в сфере защиты облачных сервисов. Сделаем предположение о дальнейшем развитии данной области в ближайшем будущем.

### Облачные сервисы

Облачные сервисы можно разделить на несколько типов по решаемым задачам [12]:

Таблица 1. Перечень компаний-производителей оборудования

Название	Страна	Направление деятельности
Dell	США	Крупнейшая компания в области производства компьютеров
HP	США	Поставщик аппаратного и программного обеспечения
Nvidia	США	Разработчик GPU и систем на чипе
IBM	США	Крупнейший производитель и поставщик аппаратного и программного обеспечения, а также IT-сервисов и консалтинговых услуг
Cisco Systems	США	Разрабатывающая и продающая сетевое оборудование, специализирующаяся в области высоких технологий
AMD	США	Производитель интегральной микросхемной электроники, один из крупнейших производителей CPU, GPU, адаптеров, материнских плат и чипсетов для них, а также твердотельных накопителей
Microsoft	США	Производитель проприетарного ПО для различного рода вычислительной техники
Qt Group	Норвегия	Производитель производству программного обеспечения
Ajax Systems	Украина	Разрабатывающая беспроводных и проводных систем безопасности полного цикла
Nokia	Финляндия	Производитель телекоммуникационного оборудования для мобильных, фиксированных, широкополосных и IP-сетей
TSMC	Китайская Республика (Тайвань)	Занимающаяся изучением и производством полупроводниковых изделий
Intel	США	Разработчик и производитель электронных устройств и компьютерных компонентов
Parallels	Россия	Специализируется на разработке программного обеспечения
Ericsson	Швеция	Производитель телекоммуникационного оборудования

IaaS («Инфраструктура как услуга») — представлено созданием виртуальных рабочих мест сотрудников и местом в сетевом хранилище данных. Пример сервисов: «VMware Horizon», «DigitalOcean», «vGate»;

PaaS («Платформа как услуга») — используется как виртуальный сервер для контейнеризации программных продуктов;

SaaS («Программное обеспечение как услуга») — программное обеспечение, используемое без установки его на пользовательское устройство. Примерами такого сервиса является «VK Cloud», «Яндекс.Диск», «Яндекс.Документы» [15].

#### Составляющие защиты информации облачных сервисов

Рассмотрим процесс функционирования облачных сервисов, в том числе систему защиты информации. Для обеспечения функционирования облачных сервисов используются центр обработки данных (далее — ЦОД) и его информационно-телекоммуникационная система (далее — ИТС) [14].

Разделим систему защиты информации на две составляющие [10], [17]:

1. Непосредственная защита (физическая) — защита здания ЦОД, реализация температурно-влажностного режима для обеспечения функционирования ИТС.

Данная составляющая включает в себя:

- ◆ наличие круглосуточной охраны на объекте (служба безопасности, сеть видеонаблюдения, датчики проникновения и т.д.);
- ◆ использование система контроля и управление доступом (далее — СКУД) (наличие турникетных ворот с защитой от обратного хода и т.д.);
- ◆ выполнение организационных мер;
- ◆ периодические проверки персонала, имеющего доступ к ЦОД;
- ◆ размещение ЦОД в местах, свободных от риска стихийных бедствий.

2. Защита технических и программных средств [19].

К защите технических средств относятся;

- ◆ минимизация трафика через выделенные залы обработки данных, помещения и ячейки;
- ◆ установка автономных дублирующих систем энергоснабжения;
- ◆ предварительная проверка используемого оборудования.
- ◆ К защите программных средств относятся:

Таблица 2. Остановленные облачные сервисы

Компания	Страна	Направление деятельности
Serpstat	Украина	SEO-платформа SaaS-модели
Heroku	США	Облачная PaaS-платформа, поддерживающая ряд языков программирования

Таблица 3. Системы физической защиты объектов

Компания	Страна	Направление деятельности
Assa Abloy (Electromechanical and Electronic Locks)	Швеция	Контроль доступа
Bosch Security Systems	Германия	Системы безопасности
Hanwha Techwin	Корея	Видеонаблюдение
Flir Systems (Commercial, Government and Defense)	США	Видеонаблюдение, контроль доступа

- ◆ использование трехфакторной аутентификации;
- ◆ системы разграничения доступа;
- ◆ ограничение доступа к ячейкам информации пользователей;

Организационные меры реализуются путем мониторинга действий и обеспечения безопасности их учетных данных, что влияет на снижение риска для инсайдеров.

Проблемной ситуацией в настоящее время является то, что большое количество облачных сервисов используют технические и программные средства иностранных разработчиков, а также средства физической защиты иностранного производства. Пример: для СКУД использовались и продолжают использоваться системы Cisco, IBM, Bosch Security Systems, коммутационное оборудование от компании Cisco или HP, серверное программное обеспечение Microsoft Windows Server.

Рассмотрим сложившуюся в 2022 году ситуацию на рынке услуг оказания облачных сервисов.

#### Анализ современных реалий защиты облачных сервисов в Российской Федерации

Иностранные компании-производители оборудования, которые остановили свою деятельность на территории Российской Федерации.

Рассмотрим компании, которые составляют систему облачных сервисов (таблица 1).

С учетом введения санкций в IT-области в отношении Российской Федерации остановлены облачные сервисы следующих типов (таблица 2):

Перечень системы физической защиты объектов приведен в таблице 3.

#### Уязвимости в используемом программном обеспечении

С учетом ухода иностранных компаний с территории Российской Федерации возникла еще одна проблемная ситуация — отсутствие обновления программного обеспечения.

В соответствии с ГОСТ 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» любой недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации называется уязвимостью. К уязвимостям относится и отсутствие обновления программного обеспечения.

В связи с тем, что иностранные компании больше не предоставляют услуги в Российской Федерации, то найденные уязвимости невозможно устранить, так как отсутствует доступ к серверам обновлений. Отсутствие данного доступа приводит к невозможности обновления и устранения недостатков у применяемых технических средств, а также их диагностики [4].

Таблица 4. Выявленные уязвимости, ушедших иностранных компаний-производителей

Номер уязвимости	Выявленная уязвимость	Дата размещения на сайте БДУ
BDU:2022–06634 [7]	Уязвимость режима рендеринга Vulkan браузеров Google Chrome и Microsoft Edge, позволяющая нарушителю выполнить произвольный код	25.10.2022
BDU:2022–06632 [7]	Уязвимость компонента Upload программного средства для работы с веб-приложениями Oracle Web Applications Desktop Integrator, позволяющая нарушителю получить полный контроль над приложением	18.10.2022
BDU:2022–06631 [7]	Уязвимость исполняемого файла iscsicpl.exe операционной системы Windows, позволяющая нарушителю выполнить произвольный код	27.07.2022

Таблица 5. Разработчики оборудования отечественного производства

Название	Направление деятельности
Eltex	Разработчик и производитель телекоммуникационного оборудования
Название	Направление деятельности
Ангстрем	Разработчик полного цикла по производству микросхем и силовых полупроводниковых приборов
QTECH	Производитель телекоммуникационного и IT-оборудования
Network Systems Group	Производитель оборудования для сетей передачи данных
ООО «НПО «Рапира»	Разработчик и производитель телекоммуникационного оборудования, занимается проектированием инфраструктуры беспроводных сетей, их построению и вводу в эксплуатацию.
PicoCell	Разработчик и производитель оборудования сотовой связи
ООО «Радиокомп»	Разработчик, производитель, радиоэлектронной продукции для наземных, авиационных и космических сфер промышленности
НТЦ «СГЭП»	Разработчик и производитель промышленных систем электропитания
АО НПП «Полигон»	Производитель высокотехнологичного радиоэлектронного и телекоммуникационного оборудования для нужд операторов связи, ведомственных структур, органов государственной власти и других заказчиков
ООО «Спецстрой-связь»	Разработчик и производитель собственного телекоммуникационного и сотового оборудования, систем беспроводной сети, программного обеспечения для различных продуктов, систем безопасности, оповещения
«Овен»	Разработчик и производитель контрольно-измерительных приборов и средств автоматизации для различных отраслей промышленности
АО «Микрон»	Производитель интегральных схем для защищенных носителей данных, идентификационных, платежных и транспортных документов, управления питанием и RFID-маркировки для различных отраслей цифровой экономики
ЗАО «Институт сетевых технологий»	Собственные программные и программно-аппаратные продукты, реализующие передовые информационно-телекоммуникационные технологии и обеспечивающие соблюдение требований руководящих документов Российской Федерации по защите информации

Кроме этого, нет возможность коммерческой разработки программного обеспечения из-за отсутствия сред разработки.

Приведём примеры найденных уязвимостей (таблица 4).

Полный перечень выявленных уязвимостей размещен на официальном сайте Банка данных угроз безопасности информации и его Телеграмм-канале.

### Российские аналоги технических средств и программного обеспечения

В сложившейся ситуации, представляется возможным реализация решений на базе технических и программных средств российского производства, являющихся аналогами ушедших средств иностранного производства, которые также можно использовать, и для облачных сервисов.

Таблица 6. Разработчики отечественного программного обеспечения

Название	Направление деятельности
ГК «Astra Linux» (ООО «РусБИТех-Астра»)	Разработка операционной системы «Astra Linux»
«БазАльт СПО»	Разработка операционной системы «Альт»
«Ред Софт»	Разработка операционной системы «РЕД ОС»
«Новые облачные технологии»	Офисные решения для общения и совместной работы с документами «МойОфис»
ООО «НПП «ЭЛКОМ»	Фильтр сетевой помехоподавляющий ФСПК-10-220-99-УХЛ4
ЗАО «ОКБ САПР»	Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ»
ООО «Фактор-ТС»	Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall» (модификации «DioNIS TS/FW 16000», «DioNIS TS/FW 160FD», «DioNIS TS/FW 1600R», «DioNIS TS/FW 1600V»)

Таблица 8. Ключевые компании КНР — поставщики оборудования

Название	Направление деятельности
Huawei	Производитель телекоммуникационного и ИТ-оборудования
Tr-Link	Производитель телекоммуникационного и ИТ-оборудования
Mercusys	Производитель телекоммуникационного и ИТ-оборудования

Рассмотрим отечественные компании — разработчики оборудования отечественного производства (таблица 5), отечественного программного обеспечения (таблица 6) и отечественных средств защиты информации (таблица 7).

Полный перечень сертифицированных средств защиты приведен в Государственном реестре сертифицированных средств защиты информации, размещенном на официальном сайте ФСТЭК России.

Российские технические и программные средства имеют достаточно мощные системные требования, однако в большинстве случаев необходимо реализовать более комплексное взаимодействие между компаниями для обеспечения комплексной защиты и поддержки аналогичных российских продуктов.

По результатам анализа можно установить, что в нашей стране достаточно много производителей технических и программных средств, которые могут составить конкуренцию или заменить продукты ушедших иностранных ИТ-компаний.

Пока нет подробной статистики по импортозамещению, но предложенные решения данных предприятий позволяют закрыть оставшиеся пустыми ниши рынка и восстановить возможности отечественной сетевой безопасности на должный уровень.

#### Китайские аналоги программного обеспечения и технических средств

В качестве альтернативы имеется возможность использовать технические и программные средства из Китайской Народной Республики. Почти все оборудование, доступное на рынке, прошло проверку на соответствие требованиям защиты информации и может быть установлено на предприятиях/в компаниях для дальнейшей настройки и использования.

Имеются свои специфики работы в виде специализированного программного обеспечения, технических характеристик и ограничений, но большая часть аппаратуры может быть интегрирована в отечественные локальные сети и информационные системы (открытого доступа) без особых проблем.

Список ключевых компаний КНР — поставщиков оборудования приведен в таблице 8.

### Направления развития облачных сервисов в Российской Федерации

С учетом проведенного в статье анализа можно сформулировать некоторые направления развития облачных сервисов.

Рынок развивается очень стремительно, и количество используемых сервисов будет только увеличиваться. Ожидается заход на российский рынок китайских компаний, которые готовы закрыть потребности пользователей в различных сферах. Для предприятий малого и среднего бизнеса экономически не выгодно покупка систем, им достаточно аренда.

С точки зрения защиты информации российские компании могут закрывать возникающие проблемы в программном обеспечении и технических средствах, так как им доступны уязвимости, которые появляются в системе и доступны критические обновления или поставка устройств, закрывающих технические уязвимости [9].

Кроме этого, для устранения проблем с ремонтом и поставками комплектующих для оборудования иностранного производства, израсходования страхового запаса комплектующих, а также необходимости обновления оставшегося иностранного программного обеспечения предлагается наладить производство всего необходимого оборудования и компонентов на территории Российской Федерации, осуществить интеграцию информационных ресурсов производства и компаний в российские телекоммуникационные системы и отечественные большие хранилища данных [4], [5].

Устранение проблем с программным обеспечением предлагается решать путем приоритетной разработки и внедрения отечественного программного обеспечения, в том числе в директивном порядке, по аналогии с объектами критической информационной инфраструктуры, которое будет на том же уровне, а где-то и лучше, зарубежных аналогов для упрощения процесса импортозамещения.

### Заключение

В настоящее время очень сложно сделать какие-то конкретные выводы из текущей ситуации на рынке, за исключением нескольких вещей [19]:

1. Исход или временная приостановка деятельности иностранных компаний с российского рынка будет продолжаться еще какое-то время;
2. Предложения по рынку оборудования и программного обеспечения будет временно уменьшаться, пока не наладится производство и выпуск оборудования отечественного производства или аналогов иностранных технических и программных средств;
3. Часть компаний, ушедших летом, будет поставлять свою продукцию либо через т.н. «параллельный импорт», либо через местные филиалы;
4. Стоит рассматривать продукцию, представленную азиатским или ближневосточным рынком (Иран, Китай, Вьетнам, Индия и др.), как альтернативу недоступному (отсутствующему) оборудованию и программному обеспечению, предварительно изменяя их под нужды российских заказчиков;
5. Требуется наладить производство оборудования и программного обеспечения в нашей стране, так как это критически необходимо для дальнейшей работоспособности многих отраслей деятельности.

### ЛИТЕРАТУРА

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ // [Электронный ресурс] URL: <http://www.kremlin.ru/acts/bank/24154> Дата обращения: 16.09.2022.
2. «Требования к средствам криптографической защиты информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведения, составляющих государственную тайну» ФСБ России от 17 сентября 2019 г. // [Электронный ресурс] URL: <http://www.fsb.ru/fsb/science/single.htm%21id%3D10437338%40fsbResearchart.html> Дата обращения: 18.09.2022.
3. Выписка из «Требований к средствам криптографической защиты информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведения, составляющих государственную тайну» ФСБ России от 23 сентября 2019 г. // [Электронный ресурс] URL: [http://www.fsb.ru/files/fsbdoc/project\\_normakt/vipiska.doc](http://www.fsb.ru/files/fsbdoc/project_normakt/vipiska.doc) Дата обращения: 18.09.2022.
4. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 // [Электронный ресурс] URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702> Дата обращения: 15.09.2022.
5. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 // [Электронный ресурс] URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> Дата обращения: 15.09.2022.
6. Приказ ФСТЭК России от 14 марта 2014 г. № 31 // [Электронный ресурс] URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31> Дата обращения: 15.09.2022.
7. «Банк данных угроз безопасности ФСТЭК России» // [Электронный ресурс] URL: <https://bdu.fstec.ru/threat-section> Дата обращения: 17.09.2022.

8. «Best Data Protection Solutions: our top picks» // [Электронный ресурс] URL: <https://cybernews.com/resources/best-data-protection-solutions/> Дата обращения: 20.10.2022.
9. «Как оценить, надежно ли защищено облако?» // [Электронный ресурс] URL: <https://www.itsec.ru/articles/kak-ocenit-nadezhno-li-zashchishcheno-oblako> Дата обращения: 05.09.2022.
10. «Информационная безопасность облаков» // [Электронный ресурс] URL: <https://www.itsec.ru/articles/informacionnaya-bezopasnost-oblakov> Дата обращения: 05.09.2022
11. «Сравнение Cloud-Native подходов к обеспечению безопасности облачных сервисов» // [Электронный ресурс] URL: <https://www.itsec.ru/articles/sravnenie-cloud-native-podhodov-k-obespecheniyu-bezopasnosti-oblachnyh-servisov> Дата обращения: 11.09.2022.
12. «Разница между Iaas, Paas и Saas» // [Электронный ресурс] URL: <https://mcs.mail.ru/blog/raznica-mezhdu-iaas-paas-saas-statya-ob-oblakah-v-internete> Дата обращения: 15.09.2022.
13. «Облачно, возможны осадки в виде атак» // [Электронный ресурс] URL: <https://habr.com/ru/post/533144/> Дата обращения: 19.09.2022.
14. «Что такое безопасность облака?» // [Электронный ресурс] URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security> Дата обращения: 19.09.2022.
15. «Безопасность в облаках. Изучаем безопасность облачных сервисов на примере инфраструктуры Яндекс» // [Электронный ресурс] URL: <https://xaker.ru/2019/08/14/yandex-cloud/> Дата обращения: 19.09.2022.
16. «Защита инфраструктуры облачных платформ Cloud» // [Электронный ресурс] URL: [https://docs.sbercloud.ru/overview/security-introduction/topics/architecture-principles\\_\\_infrastruture-protection.html](https://docs.sbercloud.ru/overview/security-introduction/topics/architecture-principles__infrastruture-protection.html) Дата обращения: 23.09.2022.
17. «Решения для обеспечения безопасности облака» // [Электронный ресурс] URL: <https://www.microsoft.com/ru-ru/security/business/solutions/cloud-security> Дата обращения: 23.09.2022.
18. «Кибербезопасность в облачной среде. CASB и другие технологии» // [Электронный ресурс] URL: <https://cloud.softline.ru/news/article/kiberbezopasnost-v-oblachnoj-srede/> Дата обращения: 02.10.2022.
19. «Защита облачных сервисов и приложений» // [Электронный ресурс] URL: <https://www.it-world.ru/cionews/security/149716.html> Дата обращения: 02.10.2022.
20. «Защита сред в публичном облаке: как не попасть в заголовки новостей» // [Электронный ресурс] URL: <https://www.securitylab.ru/analytics/514108.php> Дата обращения: 02.10.2022.

---

© Высотин Олег Валерьевич ( visotin@mail.ru ), Высотин Андрей Олегович ( visotin\_andrey@mail.ru ),  
Кулешов Алексей Игоревич ( kuleshovai@student.bmstu.ru ), Федорова Вероника Анатольевна ( bmstuf@mail.ru ),  
Зеленцова Екатерина Валентиновна ( katez@mail.ru ).  
Журнал «Современная наука: актуальные проблемы теории и практики»