УДК 004.056 **DOI: 10.18413/2518-1092-2022-7-3-0-2**

Маслова М.А.
Кузьминых Е.С.

ПРОБЛЕМЫ ОБЛАЧНЫХ СЕРВИСОВ И МЕТОДЫ ЗАЩИТЫ ОТ РИСКОВ И УГРОЗ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: mashechka-81@mail.ru, egor2014ru@mail.ru

Аннотация
Всё больше людей начинают пользоваться облачными сервисами для хранения, редактирования и передачи данных через интернет, ведь это очень удобно, не слишком дорого и не требует большой ресурсоёмкости. Помимо этого, с развитием удалённой работы почти все компании пользуются облачными сервисами, некоторые платят за услуги сервисов, иные создают свои собственные. На таких серверах порой хранятся очень важные данные, потеря которых привела бы в катастрофе и огромным финансовым потерям компаний. Поэтому необходимо не забывать о безопасности и необходимости защищать информацию качественно и непрерывно. В связи с мировыми переменами, в этом году популярность на облачные ИБ-сервисы очень выросла из-за резкого количества атак на различные российские информационные системы и ресурсы различных отраслей и поэтому стали все больше внимания и финансов уделять данному направлению и его защите в целом. В данной статье рассмотрим облачные сервисы, возможные риски, имеющиеся пути решения угроз, а также возможное развитие в данном направлении.
Ключевые слова: облако; облачные сервисы; облачные площадки; безопасность; безопасность облачных сервисов; информационная безопасность; безопасность облака; типы облачный сервисов; угрозы облачных сервисов; рынок облачных сервисов
Для цитирования: Маслова М.А., Кузьминых Е.С. Проблемы облачных сервисов и методы защиты от рисков и угроз // Научный результат. Информационные технологии. – Т.7, №3, 2022. – С. 14-22. DOI: 10.18413/2518-1092-2022-7-3-0-2

Maslova M.A.
Kuzminykh E.S.

PROBLEMS OF CLOUD SERVICES AND METHODS OF PROTECTION AGAINST RISKS AND THREATS

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: mashechka-81@mail.ru, egor2014ru@mail.ru

Abstract
More and more people are starting to use cloud services for storing, editing and transferring data via the Internet, because it is very convenient, not too expensive and does not require large resource intensity. In addition, with the development of remote work, almost all companies use cloud services, some pay for services, others create their own. Such servers sometimes store very important data, the loss of which would lead to disaster and huge financial losses for companies. Therefore, it is necessary not to forget about security and the need to protect information efficiently and continuously. In connection with world changes, this year the popularity of cloud information security services has grown very much due to the sharp number of attacks on various Russian information systems and resources of various industries, and therefore more and more attention and finances have been paid to this area and its protection in general. In this article, we will consider cloud services, possible risks, available ways to solve threats, as well as possible development in this direction.
Keywords: cloud; cloud services; cloud sites; security; cloud services security; information security; cloud security; types of cloud services; cloud service threats; cloud services market
For citation: Maslova M.A., Kuzminykh E.S. Problems of cloud services and methods of protection against risks and threats // Research result. Information technologies. – T.7, №3, 2022. – P. 14-22. DOI: 10.18413/2518-1092-2022-7-3-0-2

ВВЕДЕНИЕ

В настоящее время происходит ускоренная информатизация населения, но мало кто может похвастаться тем, что он разбирается в компьютере хотя бы на половину и может защитить данные, хранящиеся в нем на 100%. Если рассматривать обычных пользователей, то в процессе обмена информацией еще недавно были риски - «принести» вирусы на дисках, флешках и др. носителях, которыми пользовались для обмена информацией. В данный момент же информацию в основном хранят на компьютере и для ее обмена используют интернет или облачные хранилища. Всё это необходимо грамотно защищать, иначе информацию могут украсть, удалить или повредить.

Что касается предприятий или больших компаний, особенно если они относятся к государственным сервисам, КИИ, имеют корпоративную тайну, интернет вещам, то обязательно необходимо выстроить слаженную и четко взаимодействующую защищенную сеть и заранее просчитать, и предусмотреть все возможные риски, связанные с постоянным обменом информацией и пути их решения.

ОСНОВНАЯ ЧАСТЬ

В нашем компьютере находится жёсткий диск (HHD), или же твердотельный накопитель (SSD), которые хранят данные пользователя в себе. Облачные сервисы включают в себя множество таких мощных компьютеров-серверов, которые за дополнительную плату позволяют использовать свои ресурсы другим пользователям и хранить там свои данные, которые грамотно зашифрованы и защищены. Помимо хранения данных, с ними можно взаимодействовать, редактировать, делиться и так далее, образно говоря, облачный сервис, это определенная онлайн-программа, позволяющая удалённо работать с данными.

Так чем же пользоваться, чтоб сохранить данные в целостности и каких правил необходимо придерживаться для безопасной работы и передачи информации? У каждого сервиса свои плюсы, так же они делятся на разные типы предоставления услуг, некоторые предоставляют только виртуальную папку, иные же предоставляют возможность собрать свой виртуальный компьютер, или же выделяют целый сервер с большими возможностями работы. Но всегда остается вопрос в конфиденциальности и сохранности информации, что не всегда предоставляется всеми сервисами.

Облачные вычисления почти 20 лет применяют в коммерческих целях и почти 95% компаний утверждают, что у них есть облачная стратегия. Хранение информации на «облаке» набирает все большего размаха, т.к. это очень удобно и мобильно.

Помимо обычных пользователей не стоит забывать про компании, предприятия в любой из которых сотрудники делятся между собой информацией, будь то конфиденциальная, или же обычная, но помимо этого её необходимо где-то хранить. Для таких случаев существуют облачные сервисы, для обычных пользователей возможно использование обычных известных сервисов, Яндекс.Диск, Dropbox, Google Диск и так далее. Крупные компании же создают свои внутренние облачные сервера и хранят там свои данные, ведь лучше защищать самому свою «тайную комнату», чем надеяться на надёжную защиту неизвестно кого.

Рост рисков, связанных непосредственно с киберугрозами и касающиеся предприятий, компаний, интернет вещей - все больше набирает обороты и становиться предметом наживы. Все больше стало распространено использование облачных хранилищ и обмена информацией с их помощью, но на защиту данных сервисов не всегда хотят тратить дополнительно и поэтому все больше утекает логинов, паролей, личной и корпоративной информации, а вслед за этим идут большие финансовые потери, ущербы и репутационные риски для компаний. Но это не останавливает компании и пользователей хранить данные на «облаке», а наоборот, рост объёма рынка облачных услуг продолжает расти (рис. 1).

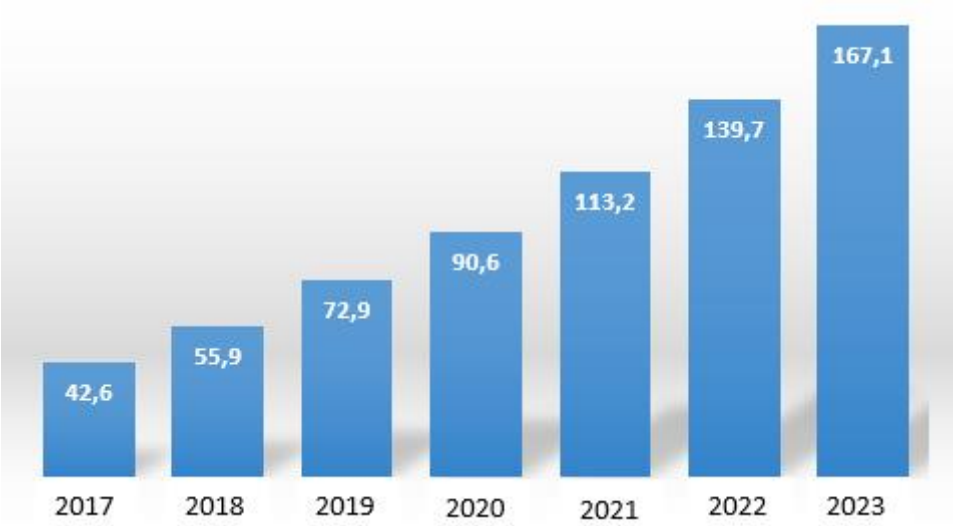

Рис. 1. Объём рынка облачных услуг в РФ 2017-2023, млрд.руб.
Fig. 1. Volume of the market of cloud services in the Russian Federation 2017-2023, billion rubles

Облачные сервисы делятся на следующие типы: публичные, частные и гибридные [1].

Публичные облака распространены в использовании, т.к. их применяют для работы в компаниях, в которых закупают нужные мощности у провайдеров и сдают их в аренду.

Частные же облака принадлежат одной компании и работа происходит на ее оборудовании, которыми пользуются сотрудники. Такую информацию легко контролировать и защищать; не надо оборудование обслуживать и администрировать его, что очень удобно и финансово выгодно.

Гибридные облака они содержат как публичные, так и частные облака или содержатся на физических носителях.

Основным направлением развития корпоративных IT-инфраструктур является гибридное облако, так как оно является оптимальным решением для бизнеса и составляет 80% спроса. Так же компании выбирают пути размещения критичных IT-систем следующим образом (см. рис. 2), приватное облако предназначено для внутренних ресурсов и различных процессов компании, а частное находится на арендованном или собственном оборудовании компании [2].

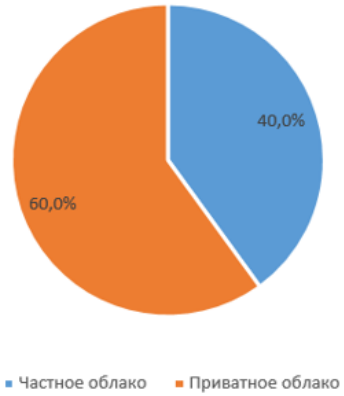

Рис. 2. Размещение критичных IT-систем компаний
Fig. 2. Placement of critical IT systems of companies

Так же облачные сервисы делят на виды услуг: Infrastructure as a Service (IaaS); Platform as a Service (PaaS); Software as a Service (SaaS) [2].

В большинстве случаев используется SaaS, так как IaaS и PaaS используется людьми, которые разбираются в этом, а именно, системные администраторы и разработчики, а SaaS больше подходит для обычных пользователей, или штатных сотрудников компаний [9].

Плюсы использования данных сервисов: удобность, практичность, удалённый доступ, постоянные улучшения, хорошая защита, дешевизна. Благодаря удобству и плюсам использования компании готовы инвестировать в защищенные облака.

В настоящее время происходит импортозамещение, поэтому уже мало кто пользуется услугами иностранных сервисов, особенно учитывая то, что цены на их услуги растут во много раз больше, чем на отечественные. А те, кто хотят быть уверены в защищённости своих данных, доверяют только отечественному производителю (табл. 1).

Таблица 1

Общемировые расходы и рост облачных сервисов

Table 1

Global Spending and Cloud Growth

Сервис	**Расходы в 2020 г., $млн**	**Расходы в 2021 г., $млн**	**Рост 2020/ 2021, %**	**Расходы в 2022 г, $млн**	**Рост 2021/ 2022, %**	**Расходы в 2023 г., $млн**	**Рост 2022/ 2023, %**
ПО как сервис (SaaS)	120686	152184	26,1%	176622	16,1%	208080	17,8%
Инфраструктура как сервис (IaaS)	64286	91642	42,6%	119717	30,6%	156276	30,5%
Платформа как сервис (PaaS)	58917	86943	47,6%	109623	26,1%	136404	24,4%
Бизнес-процессы как сервис (BPaaS)	46066	51410	11,6%	55598	8,1%	60619	9,0%
Услуги по управлению облаком и обеспечению безопасности	22664	26665	17,7%	30471	14,3%	35218	15,6%
Рабочий стол как сервис (DaaS)	1235	2072	67,8%	2,623	26,6%	3244	23,7%
Итого:	313853	410916	30,9%	494654	20,4%	599841	21,3%

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Углубимся в структуру облачных сервисов, чтобы разобраться в их проблемах и рисках. Рассмотрим плюсы и минусы 3-х видов услуг облачных сервисов (табл.2), которые рассмотрены в [3, 10].

Таблица 2

Преимущества и недостатки облачных сервисов

Table 2

Advantages and disadvantages of cloud services

Видов услуг облачных сервисов	**Преимущества**	**Недостатки**
SaaS — ПО как услуга	– технический спектр полностью скрыт и пользователь ничего не узнает, обновления происходят сами, пользователь видит готовый продукт; – легкодоступность, заказал и пользуешься.	– не всё может быть доступно по техническим причинам; – отсутствие возможности редактировать глобальные настройки; – ограниченные возможности по редактированию своих файлов; – всё зависит от поставщика, качество и эффективность; – стоимость бывает дороже остальных вариантов.
PaaS — платформа как услуга	– можно собрать любой виртуальный компьютер и пользоваться как желаешь; – оплата по факту, сколько ресурсов затратил, за то и платишь; – возможно подключить дополнительные услуги от Microsoft, Google и т.д.; – поставщики услуг имеют огромные территориальные распределения, что даёт очень быстро функционировать.	– для функционирования нужно разобраться в самом компьютере, чтобы собрать виртуальную машину; – очень дорогая базовая стоимость; – на каждой платформе свои ограничения, бывают довольно серьёзные.
IaaS — инфраструктура как услуга	– при покупке сервера его всегда можно обновлять и дополнять за небольшую плату; – низкие цены, большие возможности; – лёгкая настройка и возможность в любое время регулировать производительностью; – полная свобода действий.	– необходим специалист для настройки; – часто имеется специальная привязка к характеристикам из-за чего теряется гибкость.

Рассмотрим облачные сервисы и выясним их проблемы и угрозы безопасности, которые подробно рассмотрены в статье [4, 8].

Основные проблемы:

– машины довольно динамичны, создать, перезапустить, переместить можно за короткое время, однако такая динамичность вредит разработке целостности и со временем появляются уязвимости;

– уязвимость находятся в виртуальной среде;

– даже при выключенном состоянии машина подвержена заражению;

– во время использования облачных вычислений сеть по периметру «размывается» и тогда общий уровень защищенности влияет на защиту менее защищенной части сети;

Так же огромную роль играют всевозможные атаки на программное обеспечение, на конкретные элементы облака, на клиента, на гипервизор, на систему управления. В - первом случае их можно избежать благодаря установке: межсетевых экранов, firewall, антивирусов и т.д. Во - втором же случае если это веб-сервер, тогда необходимо установить контроль целостности страниц, для прокси-сервера - защита от DoS-атак, для системы хранения данных – установка

разграничения доступа и бэкапы, для СУБД - установка защиты от SQL-инъекций, а для сервера приложений – экран уровня приложений. В – третьем, происходят угрозы в виде утечки паролей, перехват веб-сессий за счет уязвимостей при подключении через браузер. В – четвертых – атаки на гипервизор возможны за счет разделения ресурсов между виртуальными машинами, которые начнут видеть файлы другой машины. Для устранения необходимо использовать: политики сложности и изменения устаревших паролей, внедрение постоянного применения встроенных брандмауэров хоста виртуализации, применения специальных продуктов для виртуальных сред и использование интеграции хост-серверов со службой каталога Active Directory. В – пятых это атаки на системы управления так называемых машин «невидимок», с помощью которых можно блокировать одни и подставлять др. виртуальные машины.

Применяются следующие способы защиты этих данных на облачных сервисах – это в первую очередь аутентификация с хорошей защитой сложным паролем; возможность использования личной виртуальной сети и машины; применение шифрования данных и передача данных с помощью шифрования с использованием аутентификации [5].

На (рис. 3) предоставлено графическое изображение того, что же необходимо улучшить в сфере облачных сервисов. Больше всего конечно же людей интересует безопасность, ведь самое важное, это сохранность данных. На втором же месте управление, необходима возможность управлять своими файлами и средой хранения файлов. Остальные же 2 пункта уже не так важны, но всё равно желательны в обновлении [6].

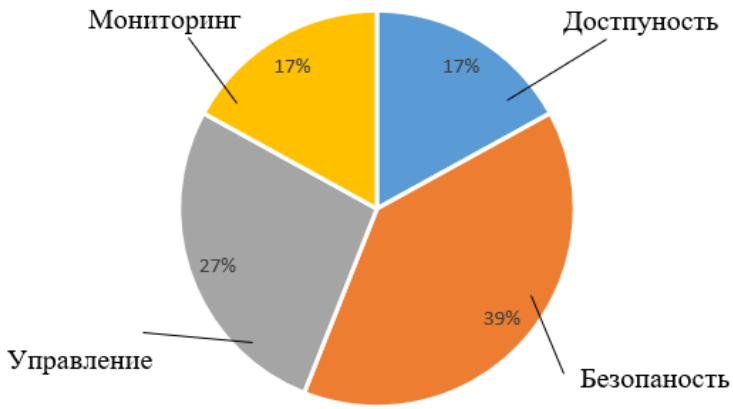

Рис. 3. Облачные вычисления: что необходимо улучшить
Fig. 3. Cloud computing: what needs to be improved

Так же существуют следующие риски, например:

– человеческий фактор, неосторожный или умышленный «слив» информации в сети, неправильные настройки доступа и т.д.,

– действия злоумышленников извне, такие как фишинговые, DDoS-атаки,

– использование несовместимых устаревших систем и сбои сторонних услуг хранения данных,

– онлайн-доступ и другие услуги хранения данных, например, во время сбоев электроэнергии или интернета,

– сети, через которые злоумышленники проникают в незащищенные учетные записи пользователей;

– отсутствие периметра для облака, так как обычно киберзащита обеспечивает безопасность периметра, а облачные среды непосредственно связаны и, следовательно, небезопасны интерфейсы программирования приложений и как следствие утечка и кража учетных записей пользователей [4];

– отказ от работы, запрет на использование, невозможность оплаты или реорганизации зарубежных облачных сервисов на российском рынке из-за санкций, введенных в 2022 г. [7];

Необходимо организовать качественную, защищенную и стабильную работу устройств и сети, в которой обрабатывается и передается вся информация, циркулирующая в сети предприятия и передающая извне. Для этого применяют: конкретные спец. средства для обеспечения локальной и сетевой защиты с большим диапазоном проверки, а также использование средств контроля трафика протоколов и систем, соответствующим тем, которые используются в данный момент; что касается например интернета вещей, то для определенного выделенного программного обеспечения его необходимо устанавливать на само устройство для контроля всех коммуникаций и работой с внешними системами, защитой этих устройств от воздействия внешних угроз. Также важно помнить об обязательной защите от различных угроз и утечек данных при взаимодействии с провайдерами облачных услуг. Тут важна защита коммуникаций инфраструктуры, реализуемая между провайдером и клиентом. Необходимо обращать внимание какие меры и сервисы предлагает вам провайдер облачных услуг, на сколько высокий уровень защиты они имеют и для чего используются, так как защита для обычного пользователя, использования интернета вещей, предприятий или КИИ значительно должна различаться [2].

Существуют определенные основные принципы для защиты систем от утечек, краж и появления рисков, которые обязательно необходимо придерживаться:

– во-первых – это постоянная защита от неправомерного доступа;

– во-вторых, один из главных факторов, чтобы стоимость защиты не превышала доходности компании;

– в-третьих – надежность, т.е. на всех этапах защиты информации она должна быть надежной;

– в-четвертых – многоступенчатость. Для хорошей защиты необходимо построить многоступенчатую систему защиты, т.е. начальная защита защищает менее важную информацию и самая глубокая – самую важную соответственно;

– в-пятых, система защиты должна быть комплексной. В данной системе необходимо предусмотреть различные возможные меры защиты от уязвимостей, краж и нанесения ущерба предприятий как внутри ее, так и извне, проанализировав, и защитив все возможные каналы утечек и возможных краж непосредственно для данной области ее применения и важно, чтобы одна защита перекрывала другую.

Так же необходимо помнить о DDoS-атаках используя внешние утилиты, блокируя, например, в определенный момент доступ во время подозрительных одновременных и превышающих трафик запросов и т.д. Но помимо действий определения, блокировки, защиты необходимо обязательно позаботиться о резервном, постоянном и своевременном копировании информации на какие-либо носители или на «облако» и установить постоянно дублирование информации. Данные действия должны выполняться обязательно для важной информации регулярно или с определенным промежутком времени [5].

Важным этапом для каждого предприятия является заранее предусмотренные и разработанные действия если все же не удалось своевременно предупредить какие-либо атаки, вмешательства. Т.е. необходимо разработать быстрый и четкий план действий по ликвидации последствий вмешательства или блокировки при подозрительных действиях. И помнить, что все данные, что размещены в IT-инфрастуктуре не должны выйти за ее пределы.

Ни одна система не может дать 100% гарантию защиты, поэтому чтобы защитить хранящиеся данные в облаке и снизить риски до минимума, необходимо придерживаться основных правил:

– определить конфиденциальные данные и установить для них соответствующую защиту;

– разработать политику контроля доступа и только после этого давать права на пользование, редактирование, перемещение и копирование данных в облако и с него;

– внедрение современного криптографического решения компании до загрузки на облако с собственными ключами;

– постоянный мониторинг по устранению внутренних угроз облачной безопасности,

– контролировать использование облачных сервисов работниками компании и установить конкретные для работы в компании;

– запретить пользование личными устройствами для перемещения данных на облачные решения и постоянно выполнять проверку безопасности при скачивании;

– установить список безопасных сервисов, браузеров и облачных приложений для работы в компании, а также разрешенные данные для размещения на облаке,

– проводить постоянное обновление браузеров, ПО;

– установить автоматическое обновление политики веб-доступа, благодаря информации о профиле риска разных сервисов, с блокировкой и предупреждением сотрудника о запрете использования данного облака,

– установка защиты от некомпетентных сотрудников и злоумышленников,

– установка двухфакторной аутентификации для облачного доступа к документам с высоким риском потери и искажения,

– установка дополнительных мер аутентификации при входе в облако с нового устройства,

– выбирать такие облачные хранилища, которые соответствуют хорошей защите данных и имеют соответствие нормативным законам и актам государства и выполнения всех стандартов и правил, которые должны быть выполнены в применяемой отрасли,

– разработать четкий и комплексный план управления авторизацией и идентификацией в облачных сервисах,

– выбирать только надежные облачные услуги, поставщики которых соблюдают стандарты, политики и имеют сертификаты (самые распространённые сертификаты это ISO 27001 и SAS 70 Type II),

– перед заключением договоров ознакомиться с существующими защитными мерами, просмотреть статистику утечек и слабых сторон в данной системе безопасности.

– придерживаться правила, что все, что данные хранящиеся в IT-инфраструктуре компании не должны передаваться за ее пределы.

Правила и меры по обеспечению ИБ в компании необходимо постоянно разрабатываться, обновляться, реализовываться беспрерывно и комплексно, и только тогда это снизить до минимума потерю и повреждение данных компании и не придется потом тратить деньги на борьбу с последствиями.

ЗАКЛЮЧЕНИЕ

Облачные сервисы становятся всё популярнее и обществу необходимо где-то хранить данные с быстрым ее обменом. Это стало еще актуальнее при внедрении удалённой работы предприятий.

Всегда в любой системе или услуге есть как плюсы, там и минусы, необходимо сделать правильный выбор облачных сервисов, работы и защиты их. Необходимо обращать внимание и сравнивать не только денежные затраты, но и многие другие пункты, такие как: удобность, актуальность, возможность настройки большинства факторов, существующие уязвимости, угрозы, риски и главное предоставляемую защищенность. Для организации грамотной работы необходимо придерживаться перечисленных основных правил организации защиты и наличие грамотных сотрудников в области ИТ-инфраструктуры и информационной безопасности.

Список литературы

1. Как вести бизнес через облачные сервисы. URL: https://secrets.tinkoff.ru/razvitie/oblachnye-servisy/
2. Нестеренко В.Р., Маслова М.А. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними // Научный результат. Информационные технологии. – Т.6, №1, 2021. – С. 48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6, URL: http://rrinformation.ru/journal/annotation/2375/.
3. Обзор IT-рынка облачных решений для бизнеса. URL: https://habr.com/ru/post/417193/
4. Угрозы облачных вычислений и методы их защиты. URL: https://habr.com/ru/post/183168/
5. Миронова, А.О., Применение методики оценки угроз безопасности информации / А.О. Миронова, Ю.Ю. Гончаренко, А.С. Гоголь, А.Н. Фролова // Энергетические установки и технологии. – 2021. – Т. 7. № 4. – С. 71-75.
6. Облачные сервисы. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.09ae7991-62ebba87-8aa16fe0-74722d776562/https/corporatefinanceinstitute.com/resources/knowledge/data-analysis/cloud-services/
7. Ожиганова, М.И. Методы и средства проведения анализа угроз локальной вычислительной сети предприятия / М.И. Ожиганова, А.О. Шейко, Е.М. Исакова, А.О. Миронова // в сборнике: цифровая трансформация науки и образования. Сборник научных трудов II Международной научно-практической конференции. 2021. С. 264-270.
8. Простыми словами: Разбираемся с «облачными» услугами. URL: https://habr.com/ru/company/1cloud/blog/280376/
9. Облачные сервисы (рынок России). URL: https://www.tadviser.ru/index.php/Статья:Облачные_сервисы_(рынок_России)
10. Облачные сервисы 2022. URL: https://www.cnews.ru/reviews/oblachnye_servisy_2022/articles/spros_na_iaas_i_saas_ustojchivo_rastet

References

1. How to do business through cloud services. URL: https://secrets.tinkoff.ru/razvitie/oblachnye-servisy/
2. Nesterenko R.V., Maslova M.A. Modern challenges and threats information security public cloud making and methods of work with them // Research result. Information technologies. – T.6, №1, 2021. – P. 48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6, URL: http://rrinformation.ru/en/journal/annotation/2375/.
3. Overview of the IT market of cloud solutions for business. URL: https://habr.com/ru/post/417193/
4. Threats of cloud computing and methods of their protection. URL: https://habr.com/en/post/183168/
5. Mironova A.O., Goncharenko Y.Y., Gogol A.S., Frolova A.N. Application of the methodology for assessing threats to information security // Power plants and technologies. - 2021. - V. 7. No. 4. - P. 71-75.
6. Cloud services. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.09ae7991-62ebba87-8aa16fe0-74722d776562/https/corporatefinanceinstitute.com/resources/knowledge/data-analysis/cloud-services/
7. Ozhiganova, M.I. Methods and tools for analyzing threats to a local computer network of an enterprise / M.I. Ozhiganova, A.O. Sheiko, E.M. Isakova, A.O. Mironova // in the collection: digital transformation of science and education. Collection of scientific papers of the II International Scientific and Practical Conference. 2021. P. 264-270.
8. In simple words: Dealing with "cloud" services. URL: https://habr.com/ru/company/1cloud/blog/280376/
9. Cloud services (market of Russia). URL: https://www.tadviser.ru/index.php/Article: Cloud_services_(market_of Russia)
10. Cloud services 2022. URL: https://www.cnews.ru/reviews/oblachnye_servisy_2022/articles/spros_na_iaas_i_saas_ustojchivo_rastet

Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Кузьминых Егор Сергеевич, студент третьего курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Maslova Maria Alexandrovna, Senior Lecturer of the Department Information security, Institute of Radioelectronics and Information security
Kuzminykh Yegor Sergeevich, Third-year Student of the Department Information security, Institute of Radioelectronics and Information security