

INTERNATIONAL SCIENCE REVIEWS



№1 (5) 2024

Natural Sciences and
Technologies series





INTERNATIONAL SCIENCE REVIEWS

Natural Sciences and Technologies series

Has been published since 2020

№1 (5) 2024

Astana

INTERNATIONAL SCIENCE REVIEWS. NATURAL SCIENCES AND TECHNOLOGIES SERIES ЖУРНАЛЫНЫҢ РЕДАКЦИЯСЫ

БАС РЕДАКТОР

Қалимолдаев Мақсат Нұрадилович, техникалық ғылымдар докторы, ҚР ҰҒА академигі, профессор, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты» бас директорының кеңесшісі, бас ғылыми қызметкері (Қазақстан)

БАС РЕДАКТОРДЫҢ ОРЫНБАСАРЫ

Мырзағалиева Анар Базаровна, биология ғылымдарының докторы, профессор, бірінші вице-президент, Астана халықаралық университеті (Қазақстан);

РЕДАКТОРЛАР:

- **Сейткан Айнура Сейтканқызы**, техника ғылымдарының кандидаты, PhD, жаратылыстану ғылымдары жоғары мектебінің деканы, Астана халықаралық университеті (Қазақстан);

- **Муканова Асель Сериковна**, PhD, Ақпараттық технологиялар және инженерия жоғары мектебінің деканы, Астана халықаралық университеті (Қазақстан);

- **Абдилдаева Асель Асылбековна**, PhD, қауымдастырылған профессор, Әл-Фараби атындағы ҚазҰУ (Қазақстан);

- **Хлахула Иржи** PhD, профессор, Познаньдағы Адам Мицкевич атындағы университет (Польша);

- **Редферн Саймон А.Т.**, PhD, профессор, Наньян технологиялық университеті (Сингапур);

- **Сяолей Фенг**, PhD, Наньян технологиялық университеті (Сингапур);

- **Шуджаул Мулк Хан**, PhD, профессор, Каид-және-Азам университеті (Пакистан);

- **Базарнова Наталья Григорьевна**, химия ғылымдарының докторы, профессор, Химия және химиялық-фармацевтикалық технологиялар институты (Ресей);

- **Черёмушкина Вера Алексеевна**, биология ғылымдарының докторы, профессор, РҒА СБ Орталық Сібір ботаникалық бағы (Ресей);

- **Тасболатұлы Нұрболат**, PhD, Ақпараттық технологиялар және инженерия жоғары мектебі деканының орынбасары, Астана халықаралық университеті (Қазақстан);

- **Байшоланов Сакен Советович**, география ғылымдарының кандидаты, доцент, Астана халықаралық университеті (Қазақстан);

- **Нуркенов Серик Амангельдинович**, PhD, қауымдастырылған профессор, Астана халықаралық университеті (Қазақстан).

**РЕДАКЦИЯ ЖУРНАЛА INTERNATIONAL SCIENCE REVIEWS.
NATURAL SCIENCES AND TECHNOLOGIES SERIES**

ГЛАВНЫЙ РЕДАКТОР

Калимолдаев Максат Нурадилович, доктор технических наук, академик НАН РК, профессор, ГНС, советник генерального директора Института информационных и вычислительных технологии КН МНВО РК (*Казахстан*)

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА

Мырзагалиева Анар Базаровна, доктор биологических наук, профессор, первый вице-президент, Международный университет Астана (*Казахстан*)

РЕДАКТОРЫ:

- **Сейткан Айнур Сейтканкызы**, кандидат технических наук, PhD, декан высшей школы естественных наук, Международный университет Астана (*Казахстан*);

- **Муканова Асель Сериковна**, PhD, декан Высшей школы информационных технологии и инженерии, Международный университет Астана (*Казахстан*);

- **Абдилдаева Асель Асылбековна**, PhD, ассоциированный профессор, Казахский национальный университет имени Аль-Фараби (*Казахстан*);

- **Хлахула Иржи** PhD, профессор, Университет имени Адама Мицкевича в Познани (*Польша*);

- **Редферн Саймон А.Т.**, PhD, профессор, Наньянский технологический университет (*Сингапур*);

- **Фенг Сяoley**, PhD, Наньянский технологический университет (*Сингапур*);

- **Шуджаул Мулк Хан**, PhD, профессор, Университет Каид-и Азама (*Пакистан*);

- **Базарнова Наталья Григорьевна**, доктор химических наук, профессор, Институт химии и химико-фармацевтических технологий (*Россия*);

- **Черёмушкина Вера Алексеевна**, доктор биологических наук, профессор, Центральный Сибирский Ботанический сад СО РАН (*Россия*);

- **Тасболатұлы Нұрболат**, PhD, заместитель декана Высшей школы информационных технологии и инженерии, Международный университет Астана (*Казахстан*);

- **Байшоланов Сакен Советович**, кандидат географических наук, доцент, Международный университет Астана (*Казахстан*);

- **Нуркенов Серик Амангельдинович**, PhD, ассоциированный профессор, Международный университет Астана (*Казахстан*);

**EDITORIAL TEAM OF THE JOURNAL INTERNATIONAL SCIENCE REVIEWS.
NATURAL SCIENCES AND TECHNOLOGIES SERIES**

CHIEF EDITOR

Maksat Kalimoldayev, Doctor of Technical Sciences, Academician of NAS RK, Professor, SRF, CEO's counselor «The Institute of Information and Computational Technologies» CS MSHE RK (Kazakhstan)

DEPUTY CHIEF EDITOR

Anar Myrzagaliyeva, Doctor of Biological Sciences, Professor, First Vice-President, Astana International University (Kazakhstan)

EDITORS:

- **Ainur Seitkan**, Candidate of Technical Sciences, PhD, Dean of the Higher School of Natural Sciences, Astana International University (Kazakhstan);
- **Assel Mukanova**, PhD, Dean of the Higher School of Information Technology and Engineering, Astana International University (Kazakhstan);
- **Assel Abdildayeva**, PhD, Associate Professor, of the Department of Artificial Intelligence and Big Data, Al-Farabi Kazakh National University (Kazakhstan);
- **Jiri Chlachula**, PhD, Dr.Hab., Full Professor, Adam Mickiewicz University, Poznań (Poland);
- **Simon A.T. Redfern**, PhD, Professor, Nanyang Technological University (Singapore);
- **Xiaolei Feng**, PhD, Nanyang Technological University (Singapore);
- **Khan Shujaul Mulk**, PhD, Professor, Quaid-i-Azam University (Pakistan);
- **Natal'ya Bazarnova**, Doctor of Chemical Sciences, Professor, Institute of Chemistry and Chemical-Pharmaceutical Technologies (Russia);
- **Vera Cheryomushkina**, Doctor of Biological Sciences, Professor, Central Siberian Botanical Garden SB RAS (Russia);
- **Nurbolat Tasbolatuly**, PhD, Deputy Dean of the Higher School of Information Technology and Engineering, Astana International University (Kazakhstan);
- **Saken Baisholanov**, Candidate of Geographical Sciences, Associate Professor, Astana International University (Kazakhstan);
- **Serik Nurkenov**, PhD, Associate Professor, Astana International University (Kazakhstan).

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000

Tel.: (7172) 24-18-52 (ext. 316)

E-mail: natural-sciences@aiu.kz

International Science Reviews NST - 76153

International Science Reviews

Natural Sciences and Technologies series

Owner: Astana International University

Periodicity: quarterly

Circulation: 500 copies

CONTENT

1. А.М.Касымханов, И.В.Притыкин, С.К.Китапбаев, Д.А.Костюченко, С.Е.Базаров ЕРТІС БАССЕЙНІНІҢ ХАЛЫҚАРАЛЫҚ МАҢЫЗЫ БАР БАЛЫҚ ШАРУАШЫЛЫҒЫ СУ АЙДЫҢДАРЫНДАҒЫ ТЫРАНЫҢ (ABRAMIS BRAMA LINNAEUS, 1758) БИОЛОГИЯЛЫҚ КӨРСЕТКІШТЕРІ ЖӘНЕ КӘСІПТІК МАҢЫЗЫ.....	7
2. А.Бериков, Т.Самарханов ПАТРИОТИЧЕСКОЕ ВОСПИТАНИЕ ДЕТЕЙ ШКОЛЬНОГО ВОЗРАСТА НА ПРИМЕРЕ ИСТОРИЧЕСКИХ ЛИЧНОСТЕЙ БАЯНАУЫЛА.....	17
3. Ж.Н. Елемес, Ж.М. Мукатаева ӘРТҮРЛІ ДЕНЕ БЕЛСЕНДІЛІГІМЕН АЙНАЛЫСАТЫН МЕКТЕП ОҚУШЫЛАРЫНЫҢ ФИЗИКАЛЫҚ ДАМУЫ	25
4. Т.Шалбай, Л.Кусепова СЕТЕВАЯ ВИРТУАЛИЗАЦИЯ: ТРАНСФОРМАЦИЯ СОВРЕМЕННЫХ ВОЗМОЖНОСТЕЙ ПОДКЛЮЧЕНИЯ	34
5. Ж.С.Жапарова, Л.Т.Кусепова, А.Е.Назырова ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СОВРЕМЕННОМ БИЗНЕСЕ: ПРИМЕНЕНИЕ, ТЕНДЕНЦИИ И ВЛИЯНИЕ НА ЭФФЕКТИВНОСТЬ РАБОТЫ ОРГАНИЗАЦИЙ	43
6. Е.Е.Садибек, Л.Т.Кусепова, А.Е.Назырова ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ	50
7. А.Е.Назырова, А.С.Муканова, М.Ж.Калдарова, Л.Т.Кусепова МОДЕЛЬНОЕ СТРУКТУРИРОВАНИЕ УЧЕБНОГО ПЛАНА ДЛЯ ДОСТИЖЕНИЯ ЗАРАНЕЕ ОПРЕДЕЛЁННЫХ УЧЕБНЫХ РЕЗУЛЬТАТОВ: ВИЗУАЛИЗАЦИЯ И ОПТИМИЗАЦИЯ ЧЕРЕЗ СЕТЕВУЮ ДИАГРАММУ	57
8. Б.Х.Аллажар, М.Ж.Калдарова, А.Е.Назырова РАСПОЗНАВАНИЕ ИЗОБРАЖЕНИЙ С ПОМОЩЬЮ ГЛУБОКИХ НЕЙРОННЫХ СЕТЕЙ В ПРИСУТСТВИИ ШУМА	63
9. Ермек Төле Би ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРОГНОЗИРОВАНИЯ СЕРДЕЧНО-СОСУДИСТЫХ ЗАБОЛЕВАНИЙ НА ОСНОВЕ КЛИНИКО-ДЕМОГРАФИЧЕСКИХ ДАННЫХ ПАЦИЕНТОВ	79
10. Ермек Төле Би ОПРЕДЕЛЕНИЕ СЕРДЕЧНОЙ НЕДОСТАТОЧНОСТИ ЧЕРЕЗ СОВРЕМЕННЫЕ ГАДЖЕТЫ: ПЕРСПЕКТИВЫ И ОГРАНИЧЕНИЯ	87
11. Л.М.Нұрхан, С.С.Байшоланов ГЕОГРАФИЯ ОҚУЛЫҚТАРЫНДА АУА-РАЙЫ ЖӘНЕ КЛИМАТ ТУРАЛЫ БЕРЛІГЕН МӘЛІМЕТТЕР ЖӘНЕ ОЛАРДЫ ТОЛЫҚТЫРУҒА ҰСЫНЫСТАР.....	97
12. Л.М.Нұрхан, С.С.Байшоланов ГЕОГРАФИЯ ОҚУЛЫҚТАРЫНДА КЛИМАТТЫҢ ӨЗГЕРУІ ТУРАЛЫ БЕРЛІГЕН МӘЛІМЕТТЕР ЖӘНЕ ОЛАРДЫ ТОЛЫҚТЫРУҒА ҰСЫНЫСТАР	110

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

Садибек Е.Е, Кусепова Л.Т., Назырова А.Е.

Международный университет Астана, Астана, Казахстан
elnur.sadibek55222@mail.ru

Аннотация. Облачные сервисы являются неотъемлемой частью современных информационных технологий и предоставляют широкий спектр выгод для организаций. Однако безопасность данных в облаке остается приоритетной задачей. Эта статья обсуждает важность обеспечения безопасности данных в облачных сервисах и выделяет ключевые аспекты.

Ключевые слова: Защита данных, доступность, надежность, защита от кибератак, управление рисками, политика безопасности.

ВВЕДЕНИЕ

В современной информационной эпохе облачные сервисы стали неотъемлемой составной частью как личной, так и корпоративной деятельности. Эти службы представляют собой сетевые вычислительные ресурсы и услуги, предоставляемые через Интернет, что позволяет пользователям хранить, обрабатывать и получать доступ к данным и приложениям, размещенным на удаленных серверах. Сюда включается хостинг веб-приложений, облачное хранение данных, а также облачные вычисления, чтобы назвать только несколько аспектов (рисунок 1).

Облачные сервисы разделяются на несколько основных моделей:

IaaS (Infrastructure as a Service): Предоставление вычислительных ресурсов, сетевой инфраструктуры и хранилища данных в виде виртуальных машин, серверов и хранилища. Примерами являются Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform (GCP).

PaaS (Platform as a Service): Предоставление платформы для разработки, тестирования и развертывания приложений, освобождая от необходимости управления инфраструктурой. Примерами являются Heroku, Google App Engine и Microsoft Azure App Service.

SaaS (Software as a Service): Предоставление готовых приложений и сервисов через Интернет, с возможностью использования без необходимости установки и обслуживания. Примерами могут служить Gmail, Microsoft Office 365 и Salesforce.

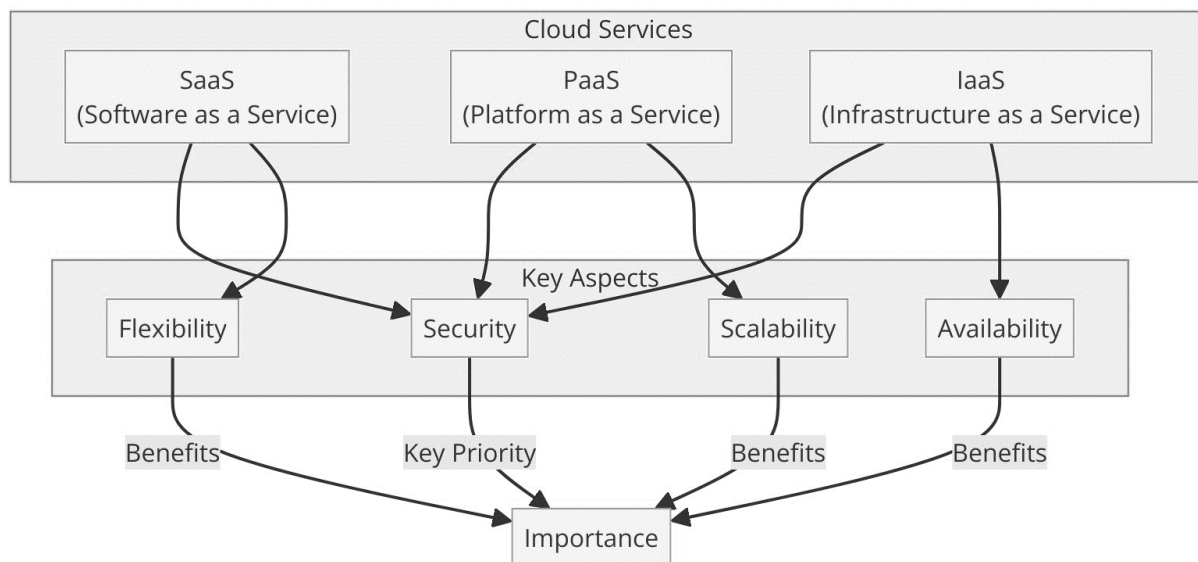


Рисунок 1 - Взаимосвязь облачных сервисов и ключевых аспектов безопасности

Актуальность облачных сервисов в наше время трудно переоценить. Они обеспечивают гибкость, масштабируемость и доступность данных и приложений в мировом масштабе. Это означает, что как организации, так и частные лица могут легко обмениваться информацией и работать с данными практически в любой точке мира, при наличии доступа в Интернете.

Рассмотрение важных аспектов безопасности в контексте облачных сервисов является неотъемлемой составляющей современной информационной инфраструктуры (рисунок 2).



Рисунок 2 - Ключевые элементы безопасности в облачных сервисах

Защита данных, соблюдение законодательства, обеспечение доступности и надежности сервисов, защита от кибератак и внутренних угроз, соблюдение политик безопасности, управление рисками, защита интеллектуальной собственности и обеспечение долгосрочной устойчивости - ключевые аспекты, которые обеспечивают сохранность и эффективное использование облачных ресурсов. Эффективная безопасность в облачных сервисах не только защищает данные и операции, но и способствует укреплению доверия пользователей и поддержанию преимуществ, которые предоставляют эти сервисы в современной цифровой экосистеме.

Риски безопасности в облачных сервисах

Диаграмма "Риски безопасности в облачных сервисах" представляет собой ментальную карту, разбитую на три основные категории: "Утрата данных", "Последствия потери данных" и "Меры предосторожности", каждая из которых детализирует ключевые аспекты и стратегии управления рисками безопасности данных в облачных сервисах.

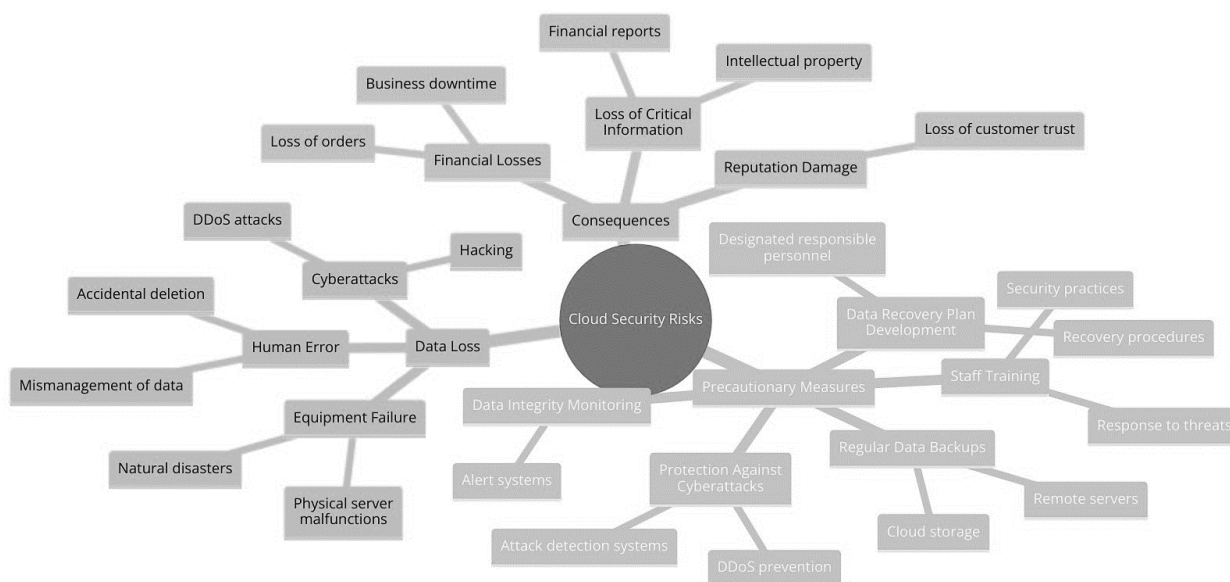


Рисунок 3 - Риски безопасности в облачных сервисах

В разделе "Утрата данных" выделены три основные причины потери данных: неисправности оборудования, включая сбои физических серверов и последствия природных катастроф; человеческие ошибки, такие как неправильное удаление файлов и некорректное управление данными; а также кибератаки, включая DDoS атаки и хакерские взломы.

"Последствия потери данных" охватывают финансовые потери из-за простоев в работе, потери заказов и клиентов; ущерб репутации, влекущий за собой потерю доверия со стороны клиентов и общественности; а также потерю критически важной информации, такой как финансовые отчеты и интеллектуальная собственность.

В секции "Меры предосторожности" представлены рекомендации по минимизации рисков потери данных: регулярное создание резервных копий данных на удаленные серверы или в облачное хранилище; мониторинг целостности данных для оперативного выявления и реагирования на проблемы; разработка и проверка плана восстановления данных, включая процедуры восстановления и назначение ответственных лиц; защита от кибератак через применение механизмов обнаружения и сдерживания атак; а также обучение персонала основам безопасности данных и методам предотвращения угроз.

The mind map is centered on 'Data Confidentiality Breaches'. It branches into three main categories: Causes, Consequences, and Preventive Measures.

- Causes:**
 - Unauthorized Access
 - Security breaches
 - Loss of customer trust and business volume
 - Fines for data protection violations
 - At rest and in transit
 - Data Leaks
 - Human errors
 - Inadequate security measures
 - Social Engineering
 - Deceiving employees or users
 - Stolen credentials
 - Cyberattacks
 - Legal Consequences
 - Lawsuits from clients or regulators
 - Disclosure of Sensitive Information
 - Medical records
 - Personal and financial client data
 - Commercial information
 - Long-term customer and partner relationships impact
 - Reputation Damage
 - Financial Losses
- Consequences:**
 - Unauthorized Access
 - Stolen credentials
 - Cyberattacks
 - Legal Consequences
 - Disclosure of Sensitive Information
 - Reputation Damage
 - Financial Losses
- Preventive Measures:**
 - Employee Training
 - Data security rules and responsibilities
 - Attack simulations and security practices against social engineering
 - Who can access what data and permitted actions
 - Strict Access Policies
 - Security Monitoring and Audits
 - Network activity and event logs analysis
 - 2FA
 - Password and one-time code
 - Regular Security Checks
 - Identifying vulnerabilities and assessing security measures effectiveness
 - Compliance
 - Adhering to data protection regulations like GDPR, HIPAA
 - Data Encryption
 - Insufficient Encryption
 - Third-party access
 - Data Interception

Рисунок 4 - Нарушение конфиденциальности данных в облачных сервисах

Источники рисков конфиденциальности включают неавторизованный доступ через украденные учетные данные или нарушения уровня безопасности, утечки данных, обусловленные человеческими ошибками, недостаточными мерами безопасности или кибератаками, недостаточное шифрование, подразумевающее риск перехвата и чтения данных третьими сторонами, а также социальную инженерию, направленную на обман сотрудников или пользователей для доступа к конфиденциальной информации.

Последствия нарушения конфиденциальности охватывают раскрытие чувствительной информации, включая личные и финансовые данные клиентов, медицинские записи и коммерческую информацию, что может привести к финансовым убыткам, ущербу репутации организации и юридическим последствиям, в том числе судебным искам и штрафам за нарушение законодательства о защите данных.

Меры предосторожности, направленные на предотвращение нарушения конфиденциальности данных, включают шифрование данных в состоянии покоя и при передаче, внедрение двухфакторной аутентификации для добавления дополнительного уровня безопасности при входе в систему, разработку строгих правил доступа, регулярный мониторинг и аудит безопасности для выявления подозрительной активности, обучение сотрудников правилам безопасности данных, проведение регулярных проверок безопасности для идентификации уязвимостей и оценки эффективности мер безопасности, а также соблюдение

нормативных требований и законодательства о защите данных, таких как GDPR и HIPAA.

Киберугрозы для облачных сервисов

Диаграмма "Киберугрозы для облачных сервисов" представляет собой структурированное визуальное изображение, категоризирующее различные типы кибератак, их потенциальные последствия для облачных сервисов, а также рекомендуемые меры предосторожности для предотвращения и смягчения угроз (рисунок 5). Основные категории включают атаки на доступность, такие как DDoS, направленные на перегрузку серверов и нарушение работы сервисов; перехват данных, целью которого является кража чувствительной информации; взлом учетных записей для несанкционированного доступа к данным и ресурсам; вредоносное программное обеспечение для повреждения данных и инфраструктуры; и фишинговые атаки для обмана сотрудников и получения конфиденциальных данных.

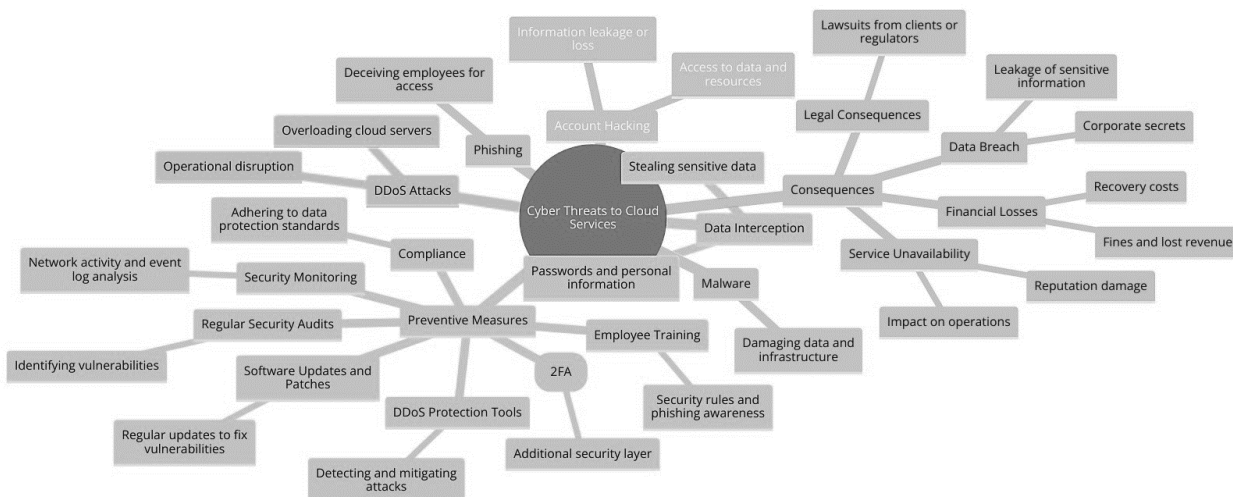


Рисунок 5 - Киберугрозы для облачных сервисов

Последствия этих угроз могут включать недоступность сервисов, утечку данных, финансовые убытки, а также юридические последствия в случае нарушения законодательства о защите данных. Для защиты облачных сервисов рекомендуется использовать инструменты защиты от DDoS-атак, двухфакторную аутентификацию, регулярные обновления и патчи программного обеспечения, обучение персонала по безопасности, мониторинг безопасности и проведение регулярных аудитов безопасности, а также соблюдение стандартов и нормативов по защите данных.

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности в рамках облачных сервисов представляет собой сложную и критически значимую задачу в современной эпохе, когда множество

компаний воспользуется облачным хранилищем и обработкой данных. Эта проблема охватывает как аспекты защиты данных, так и широкие меры информационной безопасности. В данной статье мы тщательно исследовали ключевые аспекты обеспечения безопасности в сфере облачных сервисов и представили советы о наилучших методах для достижения данной цели.

Мы выявили, что угрозы безопасности в сфере облачных сервисов включают в себя опасность потери данных, утечку конфиденциальной информации и возможные кибератаки. Потеря данных может возникнуть по различным причинам, таким как технические сбои, программные ошибки и человеческие недоразумения, поэтому регулярное создание резервных копий данных становится обязательной мерой безопасности. Утечка конфиденциальной информации может быть следствием несанкционированного доступа к данным, но использование шифрования и строгого контроля доступа способствует предотвращению таких инцидентов. Кибератаки могут иметь серьезные последствия, и меры мониторинга безопасности, регулярное обновление программного обеспечения и использование безопасных систем помогают уменьшить этот риск.

Средства обеспечения безопасности включают разработку политики безопасности, шифрование данных, процедуры идентификации и аутентификации пользователей, регулярное обновление и контроль состояния систем, создание резервных копий данных, обеспечение физической безопасности, контроль и управление угрозами, а также соблюдение требований и нормативов, таких как GDPR и HIPAA. Соблюдение законодательных и нормативных требований помогает не только защитить данные, но и предотвратить возможные юридические последствия.

Внедрение наилучших практик в сфере обеспечения безопасности облачных сервисов включает разработку политики безопасности, использование шифрования данных, проверку личности и аутентификацию пользователей, регулярное обновление и наблюдение за системами, создание резервных копий данных, обеспечение физической безопасности, контроль и управление угрозами, а также соблюдение требований и нормативов. Постоянное усовершенствование стратегии безопасности также играет ключевую роль. Гарантирование безопасности облачных сервисов требует всестороннего и системного подхода. Организации должны вкладывать ресурсы в область безопасности, обучать свой персонал и регулярно обновлять свои меры безопасности, чтобы адаптироваться к новым угрозам и обеспечивать надежность и конфиденциальность данных в сфере облачных сервисов.

СПИСКИ ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Haider Al-Khateeb. "A Survey of Cloud Computing Security Management"

2. Jinshu Su, Jinshu Su, and Han Zhao. "Security and Privacy Issues in Cloud Computing: A Survey"
3. Prashant K. Jadhav, Poonam S. Patil, and Sunil B. Manke."Data Security in Cloud Computing: A Comprehensive Survey"
4. Arati Baliga, K. R. Anjali "Security Issues in Cloud Environments: A Survey"
5. Krishna Kant "Cloud Computing Security Challenges and Solutions: A Survey"