МРНТИ 28.23.15
УДК 004.056.5

С. Адилжанова, А. Ануарбек*
Казахский национальный университет имени аль – Фараби, 71, проспект аль-Фараби, 050040, Алматы, Казахстан
*E-mail: aidosik165@gmail.com

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ В ОБЛАЧНЫХ СРЕДАХ

Адилжанова Салтанат Альмуханбетовна, PhD, и.о. доцента кафедры «Кибербезопасность и криптология» факультета «Информационных технологий». E-mail:asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X
Ануарбек Айдос Маратұлы, магистрант 1 курса; E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440

Управление информационными рисками является ключевым элементом обеспечения безопасности современных организаций, особенно в условиях роста киберугроз и широкого внедрения облачных технологий. В настоящей работе рассматривается актуальная проблема повышения эффективности управления информационными рисками за счет интеграции организационных и технических подходов, а также автоматизации процессов их оценки и анализа. Значимость исследования обусловлена увеличением сложности и разнообразия современных киберугроз, требующих новых решений для их эффективного предотвращения. Для решения поставленной задачи использованы методологии OCTAVE и NIST SP 800-30, позволяющие комплексно подходить к управлению информационными рисками, сочетая организационные и технические аспекты. В рамках исследования проведена автоматизация процесса оценки рисков с помощью разработанных автором Python-скриптов, предназначенных для выявления сетевых уязвимостей и анализа конфигураций облачных систем. Результаты работы демонстрируют преимущества комбинированного подхода к управлению рисками и подтверждают эффективность автоматизации для повышения оперативности и точности анализа. Установлено, что модель Shared Responsibility Model требует уточнения границ ответственности сторон в облачных средах. Также подтверждается перспектива применения технологий искусственного интеллекта и машинного обучения для повышения точности прогнозирования угроз информационной безопасности. Использование этих технологий позволяет анализировать большие объемы данных и оперативно выявлять потенциальные угрозы, что значительно усиливает возможности прогнозирования и реагирования на инциденты. Полученные результаты имеют практическую значимость и могут быть использованы организациями при разработке и совершенствовании политики информационной безопасности, а также служат основой для дальнейших исследований по интеграции передовых технологий в системы управления рисками.

Ключевые слова: информационная безопасность, управление рисками, облачные технологии, политика безопасности, искусственный интеллект, машинное обучение, автоматизация аудита и оценки рисков.

С. Адилжанова, А. Ануарбек*
Әл-Фараби атындағы Қазақ ұлттық университеті, 71, әл-Фараби даңғылы, Алматы 050040, Қазақстан
*E-mail: aidosik165@gmail.com

БҰЛТТЫҚ ЖҮЙЕЛЕРДЕ АҚПАРАТТЫҚ ТӘУЕКЕЛДЕРДІ БАСҚАРУДЫ АВТОМАТТАНДЫРУ

Адилжанова Салтанат Альмуханбетовна, PhD, "Ақпараттық технологиялар" факультетінің "киберқауіпсіздік және криптология" кафедрасының доцентінің м. а. E-mail: asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X
Ануарбек Айдос Маратұлы – 1 курс магистранты. E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440

Ақпараттық тәуекелдерді басқару қазіргі заманғы ұйымдардың қауіпсіздігін қамтамасыз етудің негізгі элементі болып табылады, әсіресе киберқауіптердің өсуі және бұлтты технологияларды кеңінен енгізу жағдайында. Бұл жұмыста ұйымдастырушылық және техникалық тәсілдерді интеграциялау, сондай-ақ тәуекелдерді бағалау және талдау процестерін автоматтандыру арқылы ақпараттық тәуекелдерді басқарудың тиімділігін арттырудың өзекті мәселесі қарастырылады. Зерттеудің маңыздылығы заманауи киберқауіптердің күрделілігі мен әртүрлілігінің артуына байланысты, оларды тиімді болдырмау үшін жаңа шешімдерді қажет етеді. Мәселені шешу үшін ақпараттық тәуекелдерді басқаруға жан-жақты тәсіл ұсынатын, ұйымдастырушылық және техникалық аспектілерді біріктіретін OCTAVE және NIST SP 800-30 әдістемелері қолданылды. Зерттеу барысында желілік осалдықтарды анықтау және бұлттық жүйелер конфигурацияларын талдау үшін автор әзірлеген Python-скрипттер арқылы тәуекелдерді бағалау процесі автоматтандырылды. Жұмыс нәтижелері тәуекелдерді басқарудағы біріктірілген тәсілдің артықшылықтарын көрсетеді және талдаудың жеделдігі мен дәлдігін арттыруда автоматтандырудың тиімділігін растайды. Shared Responsibility Model моделі бұлттық ортада тараптардың жауапкершілік шекараларын нақтылауды қажет ететіндігі анықталды. Сонымен қатар, ақпараттық қауіпсіздік қатерлерін болжау дәлдігін арттыру үшін жасанды интеллект пен машиналық оқыту технологияларын қолданудың перспективасы расталды. Бұл технологияларды пайдалану үлкен көлемдегі деректерді талдауға және ықтимал қауіптерді жедел анықтауға мүмкіндік береді, бұл оқиғаларды болжау және оларға жауап беру мүмкіндіктерін айтарлықтай күшейтеді. Алынған нәтижелер практикалық мәнге ие және ұйымдар ақпараттық қауіпсіздік саясатын әзірлеу және жетілдіру кезінде қолдана алады, сондай-ақ озық технологияларды тәуекелдерді басқару жүйелеріне интеграциялау саласындағы одан әрі зерттеулерге негіз болып қызмет етеді.

Түйін сөздер: ақпараттық қауіпсіздік, тәуекелдерді басқару, бұлттық технологиялар, қауіпсіздік саясаты, жасанды интеллект, машиналық оқыту, аудит пен тәуекелдерді бағалауды автоматтандыру.

S. Adilzhanova, A. Anuarbek*
Al-Farabi Kazakh National University, 71, Al-Farabi Avenue, Almaty 050040, Kazakhstan
*E-mail: aidosik165@gmail.com

AUTOMATION OF INFORMATION RISK MANAGEMENT IN CLOUD ENVIRONMENTS

Adilzhanova Saltanat, PhD; Acting Associate Professor of the Department of Cybersecurity and Cryptology at the Faculty of Information Technology. E-mail: asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X;
Anuarbek Aidos, 1 year master's student; E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440

Information risk management is a key element in ensuring the security of modern organizations, especially in the context of increasing cyber threats and the widespread adoption of cloud technologies. This paper addresses the urgent problem of improving the effectiveness of information risk management through the integration of organizational and technical approaches, as well as the automation of risk assessment and analysis processes. The significance of the study is due to the increasing complexity and diversity of modern cyber threats, which require new solutions for their effective prevention. To address this problem, the OCTAVE and NIST SP 800-30 methodologies were employed, allowing for a comprehensive approach to information risk management by combining organizational and technical aspects. Within the study, the risk assessment process was automated using Python scripts developed by the author, designed to identify network vulnerabilities and analyze cloud system configurations. The results demonstrate the advantages of a combined approach to risk management and confirm the effectiveness of automation in improving the efficiency and accuracy of analysis. It was established that the Shared Responsibility Model requires clarification of the parties' responsibilities in cloud environments. The study also confirms the potential of using artificial intelligence and machine learning technologies to enhance the accuracy of forecasting information security threats. These technologies enable the analysis of large volumes of data and the rapid identification of potential threats, significantly enhancing the ability to predict and respond to incidents. The obtained results have practical significance and can be utilized by organizations in the development and improvement of information security policies, as well as serving as a basis for further research on integrating advanced technologies into risk management systems.

Keywords: Information security, risk management, cloud technologies, security policy, artificial intelligence, machine learning, automation of audit and risk assessment.

ВВЕДЕНИЕ.

Современные организации сталкиваются с растущей сложностью информационной инфраструктуры и увеличением числа киберугроз, что делает управление информационными рисками важнейшим элементом обеспечения безопасности [1], [2]. Особое значение этот вопрос приобретает при внедрении облачных технологий и использовании Интернета вещей (IoT), где ресурсы распределены, а управление сторонними сервисами требует новых подходов к оценке и минимизации рисков [3], [4].

Анализ литературы показывает, что эффективное управление информационными рисками требует сочетания организационных и технических подходов. Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) акцентирует внимание на организационных приоритетах и систематической оценке уязвимостей и активов [5]. В свою очередь, модель NIST SP 800-30 ориентирована на идентификацию угроз, анализ уровня риска и рекомендации по его смягчению [6]. Совмещение этих подходов обеспечивает комплексное управление рисками, особенно в облачных средах, где важна модель разделенной ответственности (Shared Responsibility Model) [7], [8].

Для повышения эффективности процессов оценки и анализа рисков активно применяются инструменты автоматизации. Python-скрипты позволяют проводить аудит сетевых уязвимостей, анализ конфигураций облачных систем и обработку больших данных о

событиях безопасности [9], [10], [11]. Дополнительно методы искусственного интеллекта и машинного обучения обеспечивают прогнозирование потенциальных угроз и выявление аномалий, что повышает оперативность реагирования на инциденты [12], [13], [14].

Современные международные стандарты и фреймворки, такие как ISO/IEC 27005, COBIT и NIST Cybersecurity Framework предоставляют рекомендации по управлению рисками и интеграции этих процессов в корпоративное управление и соответствие нормативным требованиям [15], [16], [17]. В сочетании с автоматизацией и AI/ML технологии, они создают возможности для более точного и быстрого анализа угроз и принятия решений [18], [19].

Таким образом, актуальность работы обусловлена необходимостью интеграции организационных и технических подходов к управлению информационными рисками, автоматизации оценки и анализа, а также использования современных технологий прогнозирования угроз.

Цель статьи – провести обзор существующих методологий и инструментов управления информационными рисками с акцентом на их автоматизацию и применение в облачных средах.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ.

Процессы оценки и управления рисками, интегрирующиеся в существующую ИТ-инфраструктуру организации, являются важным аспектом аудита информационной безопасности [3]. Обычно это включает анализ текущих систем безопасности, аудит уязвимостей и планирование будущих мер.

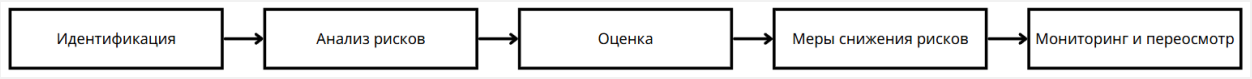

Рис. 1. Процесс управления рисками.

На рисунке 1 представлена блок-схема, иллюстрирующая процесс управления рисками в информационной безопасности. Этот процесс включает несколько ключевых шагов: идентификацию рисков, анализ угроз, разработку плана действий и мониторинг состояния безопасности.

Для крупных организаций с большим количеством информационных систем процесс оценки рисков может быть частично автоматизирован [5]. Например, с помощью скриптов на Python можно проводить аудит сетевых уязвимостей и проверку конфигураций систем.

```python
import matplotlib.pyplot as plt

scan_results = {
    '192.168.1.1': 3,
    '192.168.1.5': 1,
    '192.168.1.10': 4,
    '192.168.1.20': 0,
    '192.168.1.30': 2,
}

hosts = list(scan_results.keys())
open_ports = list(scan_results.values())

plt.figure(figsize=(10, 5))
plt.bar(hosts, open_ports, color='lightblue')
plt.xlabel('Хосты')
plt.ylabel('Количество открытых портов')
plt.title('Результаты сканирования сети (имитация)')
plt.grid(axis='y')
plt.tight_layout()
plt.show()
```

Рис. 2. Программный код сканирования уязвимости сети.

Пример скрипта на рисунке 2 демонстрирует автоматизированное сканирование сети на предмет открытых портов и потенциальных угроз.

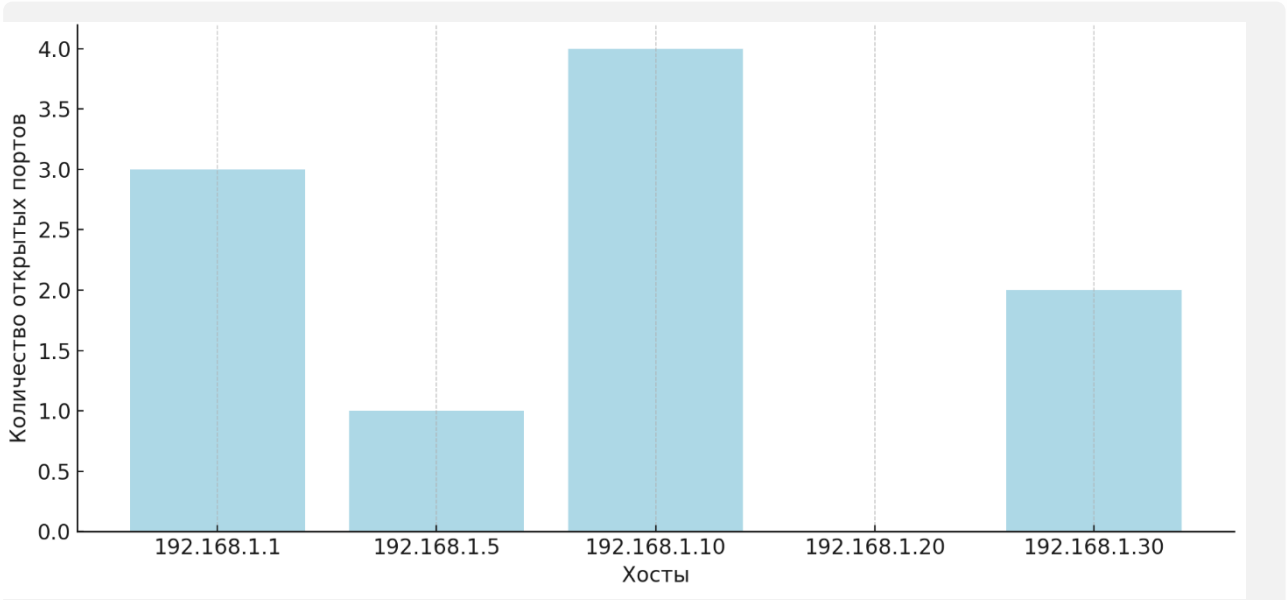

Рис. 3. Открытые порты по хостам.

На рисунке 3 представлена диаграмма, показывающая количество открытых портов на каждом обнаруженном хосте в локальной сети с использованием библиотеки nmap. Такой анализ позволяет определить наиболее уязвимые узлы сети и приоритеты для дальнейшего управления рисками [6].

Для успешного управления рисками необходимо не только выбрать правильные методы и модели, но и интегрировать их в повседневную деятельность организации [7]. Современные системы GRC (Governance, Risk, and Compliance) позволяют централизованно управлять всеми аспектами безопасности, обеспечивая соответствие корпоративным и нормативным требованиям.

С переходом многих организаций на облачные технологии возникают новые вызовы в информационной безопасности [8]. Облачные системы требуют особого подхода к оценке рисков, так как предполагают совместное использование ресурсов, управление сторонними провайдерами и глобальный доступ. Ключевым принципом является модель разделенной ответственности (Shared Responsibility Model), где провайдер облака отвечает за безопасность инфраструктуры, а клиент — за безопасность своих данных и приложений [1][8].

Примеры практической автоматизации включают:

Анализ конфигураций облака с AWS Config:

aws configservice put-config-rule --config-rule file://config-rule.json

Данный скрипт создаёт правило для проверки политик IAM в AWS, помогая минимизировать риски.

Включение шифрования на уровне базы данных AWS RDS:

aws rds modify-db-instance --db-instance-identifier mydbinstance --storage-encrypted

Это повышает уровень безопасности данных и снижает риск утечек.

Современные технологии, такие как искусственный интеллект и машинное обучение, позволяют анализировать большие объёмы данных о событиях безопасности и прогнозировать потенциальные угрозы [10][11]. Эти методы помогают организациям предсказывать возможные атаки на основе исторических данных, автоматизировать процессы анализа рисков и своевременно адаптировать системы защиты к новым видам угроз [10][11].

Модели и методы оценки рисков должны адаптироваться к новым реалиям, так как технологии и угрозы развиваются стремительно [9]. В ближайшем будущем ожидается

усиленное применение искусственного интеллекта и машинного обучения для автоматизации процессов анализа рисков и предсказания возможных атак [10][11].

Пример использования Python для анализа данных о сетевой безопасности с помощью библиотеки scikit-learn:

```python
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score

# Загрузка данных о сетевых событиях
data = load_security_data()  # Функция для загрузки данных
X = data[['feature1', 'feature2', 'feature3']]  # Факторы угроз
y = data['is_attack']  # Метка атаки

# Разделение данных на обучающую и тестовую выборки
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3)

# Обучение модели RandomForest
model = RandomForestClassifier()
model.fit(X_train, y_train)

# Оценка точности модели
y_pred = model.predict(X_test)
print(f"Точность модели: {accuracy_score(y_test, y_pred)}")
```

Рис. 4. Программный код анализа данных о сетевой безопасности.

Данный скрипт демонстрирует, как с помощью методов машинного обучения можно анализировать данные о событиях безопасности и классифицировать их как атаки или обычные действия.

Для эффективного управления рисками информационной безопасности организации используют различные международные стандарты и модели, которые предоставляют рекомендации по оценке и управлению рисками [12].

ISO/IEC 27005 — международный стандарт, посвящённый управлению рисками в области информационной безопасности. Он содержит чёткие рекомендации по проведению процесса оценки рисков, начиная от идентификации угроз и уязвимостей до разработки плана реагирования на инциденты [13].

Процесс оценки рисков по ISO/IEC 27005 включает следующие этапы:

1. Идентификация активов: определение всех информационных активов, которые необходимо защитить;
2. Определение угроз: выявление возможных угроз для каждого актива;
3. Анализ уязвимостей: исследование слабых мест систем и процессов, которые могут быть использованы злоумышленниками;
4. Оценка последствий: оценка влияния инцидента на организацию (например, финансовые потери, утрата репутации);
5. Оценка вероятности реализации угрозы: определение вероятности того, что угроза будет реализована;
6. Оценка уровня риска: определение уровня риска на основе вероятности и потенциальных последствий;
7. Разработка плана управления рисками: определение мер по снижению или устранению рисков.

COBIT (Control Objectives for Information and Related Technologies) — это фреймворк, созданный ISACA для управления ИТ и защиты данных. Он помогает организациям контролировать риски и обеспечивать соблюдение требований безопасности [14].

Применение COBIT для управления рисками может включать:

Связь с бизнес-целями: COBIT позволяет согласовать управление ИТ с стратегическими задачами организации;

Анализ текущей ситуации: оценка существующих мер безопасности и сравнение их с установленными стандартами;

План улучшений: рекомендации по улучшению контроля и безопасности, включая создание политик, обучение персонала и внедрение технологий.

Фреймворк NIST (National Institute of Standards and Technology Cybersecurity Framework) предназначен для гибкого управления киберрисками и состоит из пяти ключевых этапов [15]:

Идентификация: выявление активов, угроз и уязвимостей;

Защита: внедрение защитных мер;

Обнаружение: мониторинг и своевременное выявление инцидентов;

Ответ: реагирование на события безопасности;

Восстановление: меры по минимизации последствий и восстановлению работы.

Этот подход широко применяется в государственных и частных организациях, обеспечивая системное управление киберрисками.

Пример автоматизации реакции на инциденты с помощью NIST:

if security_incident_detected:

alert ("Обнаружен инцидент безопасности, выполняется план реагирования")

Политики безопасности являются важным инструментом управления рисками, так как задают правила работы с данными и системами, снижая вероятность угроз.

Пример политики по защите конфиденциальной информации:

Цель: предотвратить утечки и несанкционированный доступ;

Правила: Все конфиденциальные данные должны быть зашифрованы; Доступ разрешен только уполномоченным сотрудникам; Устройства с конфиденциальной информацией должны быть защищены паролями; В случае инцидента немедленно уведомлять службу ИБ.

Пример настройки межсетевого экрана для защиты от утечек:

iptables -A OUTPUT -p tcp --dport 443 -d malicious.example.com -j DROP

Политика инцидент-менеджмента определяет процесс реагирования на инциденты безопасности, начиная от их обнаружения и до завершения расследования. Она включает такие шаги, как:

- Идентификация инцидента;
- Оповещение заинтересованных сторон;
- Реагирование на инцидент (например, отключение от сети или блокировка доступа);
- Анализ причин инцидента;
- Восстановление системы;
- Разработка рекомендаций для предотвращения аналогичных инцидентов в будущем.

Пример процедуры инцидент-менеджмента в случае выявления вредоносной активности:

```
# Уведомление службы безопасности о подозрительных соединениях
if detect_malicious_connection():
    alert_security_team("Подозрительное соединение обнаружено")
    block_ip("192.168.1.200")
```

Рис. 5. Программный код уведомляющий службы безопасности.

С развитием технологий, таких как искусственный интеллект, машинное обучение, Интернет вещей (IoT) возникает необходимость адаптации подходов к управлению рисками **[12].** Интернет вещей включает множество подключенных устройств, которые часто работают на уязвимых платформах. Риски IoT включают:

- Возможность удаленного управления устройствами;
- Уязвимости в прошивке и программном обеспечении;
- Недостаток обновлений безопасности;
- Потенциальные атаки через IoT-устройства на другие системы.

Пример кода настройки доступа к IoT-устройствам через VPN:

iptables -A INPUT -p tcp --dropt 22 -s vpn_gateaway_ip -j ACCEPT.

Системы на основе искусственного интеллекта и машинного бучения становятся важной частью ИТ-инфраструктуры. Однако они также несут новые риски, такие как:

- Манипуляция данными для обучения модели (data poisoning);
- Уязвимости, связанные с неточными прогнозами;
- Непреднамеренные предвзятости в алгоритмах.

Пример использования ИИ для автоматизации анализа безопасности:

```
# Пример использования модели машинного обучения для анализа подозрительных логов
from sklearn.svm import SVC

# Загрузка данных
logs = load_security_logs()

# Обучение модели
model = SVC(kernel='linear')
model.fit(logs['features'], logs['labels'])

# Предсказание инцидентов
predictions = model.predict(new_logs['features'])
```

Рис. 6. Программный код для обучения анализа подозрительных логов.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ И ИХ ОБСУЖДЕНИЕ.

В ходе проведённого исследования был осуществлён комплексный анализ подходов к управлению информационными рисками с использованием методологий OCTAVE и NIST SP 800-30. На основе этих моделей были идентифицированы и проанализированы риски для ИТ-инфраструктуры, определены уровни угроз и предложены рекомендации по их минимизации.

Автоматизация процесса оценки рисков с помощью скриптов Python показала свою эффективность, обеспечив оперативность и точность сбора информации о состоянии портов и конфигураций облачных сервисов. Дополнительно была подтверждена целесообразность применения модели разделённой ответственности (Shared Responsibility Model) в облачных средах, которая чётко разграничивает зоны ответственности между провайдером и клиентом [12]. Полученные результаты согласуются с данными других исследователей, подчёркивающих значимость интеграции организационных и технических аспектов управления рисками. В частности, методология OCTAVE, ориентированная на организационные приоритеты, успешно дополняется технической направленностью модели NIST SP 800-30, что обеспечивает комплексный подход к безопасности. Автоматизация оценки рисков с помощью Python продемонстрировала очевидные преимущества: Снижение трудоёмкости процессов; Ускорение получения результатов; Повышение достоверности данных.

Однако данный подход требует высокой квалификации персонала и регулярного обновления знаний о новых угрозах [13]. Использование модели разделённой ответственности показало свою практическую значимость, но выявило трудности, связанные с недостаточной прозрачностью со стороны провайдеров и сложностью управления рисками со стороны клиента.

Применение технологий искусственного интеллекта и машинного обучения для прогнозирования угроз подтвердило их высокую эффективность при работе с большими объёмами данных. Вместе с тем остаются нерешёнными вопросы, связанные с предвзятостью данных и потенциальными ошибками алгоритмов [14][15].

Таким образом, проведённое исследование обладает практической ценностью, так как предлагает организациям конкретные инструменты для эффективного управления информационными рисками. В то же время результаты требуют дальнейшей адаптации под индивидуальные условия компаний и расширения исследований в области применения ИИ и облачных технологий.

ЗАКЛЮЧЕНИЕ.

В работе предложено решение научной задачи повышения эффективности управления информационными рисками за счёт интеграции организационных и технических подходов, а также автоматизации процессов их оценки и анализа. На основе проведённых исследований и анализа полученных данных сформулированы следующие выводы:

1. Для комплексного управления информационными рисками целесообразно сочетать организационные методы (OCTAVE) с техническими инструментами (NIST SP 800-30), что обеспечивает систематический и детализированный подход к выявлению и минимизации угроз.
2. Проведённые эксперименты по автоматизации оценки рисков подтвердили эффективность применения скриптов Python для быстрого и точного анализа сетевых уязвимостей и конфигураций облачных систем. Оптимальными условиями для реализации данного подхода являются регулярное обновление баз угроз, высокая квалификация специалистов и интеграция автоматизированных инструментов в существующие системы мониторинга.
3. Использование модели разделённой ответственности (Shared Responsibility Model) в облачных средах требует уточнения границ ответственности и повышения прозрачности взаимодействия между провайдерами и клиентами, что является важным условием эффективного управления рисками.
4. Подтверждена перспективность применения технологий искусственного интеллекта и машинного обучения для прогнозирования угроз информационной безопасности. Вместе с тем остаётся необходимость дальнейшего исследования проблем предвзятости данных и разработки мер по снижению ошибок прогнозирования.

Полученные результаты обладают практической значимостью: они могут быть использованы для совершенствования политики информационной безопасности организаций, а также создают основу для дальнейших исследований в области управления информационными рисками и внедрения инновационных технологий защиты данных.

ЛИТЕРАТУРА

1. Adilzhanova Saltanat, Kunelbayev Murat, Amirkhanova Gulshat, Zhussupov Yesset, Tortay Alikhan (2025) Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise//International Journal of Innovative Research and Scientific Studies, 8(2), pp. 176-196. DOI: https://doi.org/10.53894/ijirss.v8i2.5136 (in English)

2. Akhmetov, B., Lakhno, V., Chubaievskyi, V., Adilzhanova, S., Ydyryshbayeva, M. (2022) Automation of Information Security Risk Assessment International Journal of Electronics and Telecommunications, 68(3), pp. 549–555 (in English)

3. Amirkhanov B.S., Bauyrzhan S.,G.A., Amirkhanova Gulshat A.,M.M., Kunelbayev, Murat Merkebekovich, S., Adilzhanova, Saltanat, M., Tokhtassyn, Miras (2025) Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration, International Journal of Innovative Research and Scientific Studies (in English)

4. S. Adilzhanova, M. Kunelbayev, G. Amirkanova, G. Tyulepberdinova, and D. Sybanova, “Analysis of the dynamics of cyberattacks and fraud methods using machine learning algorithms for IIoT: Information security of digital twins in Industry 4.0,” Int. J. Innov. Res. Sci. Stud., vol. 8, no. 2, pp. 4012–4026, 2025. https://doi.org/10.53894/ijirss.v8i2.6201

5. Черикбаева Л.Ш., Мукажанов Н.К., Адилжанова С.А, Тюлепбердинова Г.А, Сакыпбекова М.Ж. регулизация мен коассоциациялық матрицаны пайдалана отырып нашар бақыланатын регрессия есебін шешу// қазақстан-британ техникалық университетінің хабаршысы. № 2 (69), pp. 83-94 (in Kazakh)

6. Ezeugwa, C. (2024) Cybersecurity threats and vulnerabilities in industrial internet of things (IIOT) environment: A conceptual review. *Journal of Advanced Research and Reports* 18(2), 1–23. DOI: https://doi.org/10.9734/ajarr/2024/v18i2601 (in English)

7. Ferencz, K., Kovacs, D. (2024) Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations. *Acta Polytechnica Hungarica* 21(4), 7–31 (in English)

8. Guo, Z., Liu, Y., Lu, F. (2022) Embedded remote monitoring system based on NBIOT. *Journal of Physics: Conference Series* 2384(1), 012038, 1–8. DOI: https://doi.org/10.1088/1742-6596/2384/1/012038 (in English)

9. Ibrahim, A. N., Lim, S. C. J. (2024) Real-Time Machining Power Prediction using Adaptive Neuro-Fuzzy Inference System for Sustainable Manufacturing. *Journal of Science and Technology* 16(1), 33–44 (in English)

10. Karnati, M.Z. (2023) Portable Air Quality Detection Device. In: *International Conference on Intelligent Computing and Systems (ICICS-2023)*, pp. 953–958. Springer, Singapore (in English)

11. Kim, Y., Choi, D., Park, J. (2022) Hybrid CNN-LSTM architecture for IoT anomaly detection. *IEEE Internet of Things Journal* 9(10), 7431–7442 (in English)

12. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskyi, V., Desiatko, A. (2023) Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 69(1), pp. 75–82 (in English)

13. Lyu, Y., Yin, P. (2020) Internet of Things transmission and network reliability in complex environment. *Computer Communications* 150, 757–763 (in English)

14. Mahmood, M. R., Matin, M. A., Sarigiannidis, P., Goudos, S. K. (2022) A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. *IEEE Access* 10, 87535–87562 (in English)

15. Naik, U. U., Salgaokar, S. R., Jambhale, S. (2023) IoT based air pollution monitoring system. *International Journal of Scientific Research & Engineering Trends (IJSRET)* 9(3), 835–838 (in English)

16. Ramadan, M. N. A., Ali, M. A. H., Khoo, S. Y., Alherbawi, M., Alkhedher, M. (2024) Real-time air quality monitoring system based on IoT: A case study in Malaysia. *Ecotoxicology and Environmental Safety* 283, 116856. DOI: https://doi.org/10.1016/j.ecoenv.2024.116856 (in English)

17. Ragnoli, M., Pavone, M., Epicoco, N., Pola, G., De Santis, E., Barile, G., Stornelli, V. (2023) A condition and fault prevention monitoring system for industrial computer numerical control machinery. *IEEE Access* 11, 60633–60652. DOI: https://doi.org/10.1109/ACCESS.2017. (in English)

18. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. (2023) Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 118(2), pp. 83–94 (in English)

19. Uzair, M., Salah Yacoub, A.-K., Karam Manaf, A.-J., Ibrahim Abdulrahman, A.B. (2022) A Low-Cost IoT Based Buildings Management System (BMS) Using Arduino Mega 2560 and Raspberry Pi 4 for Smart Monitoring and Automation. *International Journal of Electrical and Computer Engineering Systems* 13(3), 219–236 (in English)

REFERENCES

1. Adilzhanova Saltanat, Kunelbayev Murat, Amirkhanova Gulshat, Zhussupov Yesset, Tortay Alikhan (2025) Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise//International Journal of Innovative Research and Scientific Studies, 8(2), pp. 176-196. DOI: https://doi.org/10.53894/ijirss.v8i2.5136 (in English)

2. Akhmetov, B., Lakhno, V., Chubaievskyi, V., Adilzhanova, S., Ydyryshbayeva, M. (2022) Automation of Information Security Risk Assessment International Journal of Electronics and Telecommunications, 68(3), pp. 549–555 (in English)

3. Amirkhanov B.S., Bauyrzhan S.,G.A., Amirkhanova Gulshat A.,M.M., Kunelbayev, Murat Merkebekovich, S., Adilzhanova, Saltanat, M., Tokhtassyn, Miras (2025) Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration, International Journal of Innovative Research and Scientific Studies (in English)

4. S. Adilzhanova, M. Kunelbayev, G. Amirkanova, G. Tyulepberdinova, and D. Sybanova, “Analysis of the dynamics of cyberattacks and fraud methods using machine learning algorithms for IIoT: Information security of digital twins in Industry 4.0,” Int. J. Innov. Res. Sci. Stud., vol. 8, no. 2, pp. 4012–4026, 2025. https://doi.org/10.53894/ijirss.v8i2.6201

5. Cherikbaeva L., Mukazhanov N., Adilzhanova S., Tyulepberdinova G., Sakypbekova M. (2024)Solution of the problem of poorly controlled regression using regularization and COASSOCIATION Matrix// Bulletin of the Kazakh-British Technical University. № 2 (69), pp. 83-94 (in Kazakh)

6. Ezeugwa, C. (2024) Cybersecurity threats and vulnerabilities in industrial internet of things (IIOT) environment: A conceptual review. *Journal of Advanced Research and Reports* 18(2), 1–23. DOI: https://doi.org/10.9734/ajarr/2024/v18i2601 (in English)

7. Ferencz, K., Kovacs, D. (2024) Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations. *Acta Polytechnica Hungarica* 21(4), 7–31 (in English)

8. Guo, Z., Liu, Y., Lu, F. (2022) Embedded remote monitoring system based on NBIOT. *Journal of Physics: Conference Series* 2384(1), 012038, 1–8. DOI: https://doi.org/10.1088/1742-6596/2384/1/012038 (in English)

9. Ibrahim, A. N., Lim, S. C. J. (2024) Real-Time Machining Power Prediction using Adaptive Neuro-Fuzzy Inference System for Sustainable Manufacturing. *Journal of Science and Technology* 16(1), 33–44 (in English)

10. Karnati, M.Z. (2023) Portable Air Quality Detection Device. In: *International Conference on Intelligent Computing and Systems (ICICS-2023)*, pp. 953–958. Springer, Singapore (in English)

11. Kim, Y., Choi, D., Park, J. (2022) Hybrid CNN-LSTM architecture for IoT anomaly detection. *IEEE Internet of Things Journal* 9(10), 7431–7442 (in English)

12. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskyi, V., Desiatko, A. (2023) Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 69(1), pp. 75–82 (in English)

13. Lyu, Y., Yin, P. (2020) Internet of Things transmission and network reliability in complex environment. *Computer Communications* 150, 757–763 (in English)

14. Mahmood, M. R., Matin, M. A., Sarigiannidis, P., Goudos, S. K. (2022) A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. *IEEE Access* 10, 87535–87562 (in English)

15. Naik, U. U., Salgaokar, S. R., Jambhale, S. (2023) IoT based air pollution monitoring system. *International Journal of Scientific Research & Engineering Trends (IJSRET)* 9(3), 835–838 (in English)

16. Ramadan, M. N. A., Ali, M. A. H., Khoo, S. Y., Alherbawi, M., Alkhedher, M. (2024) Real-time air quality monitoring system based on IoT: A case study in Malaysia. *Ecotoxicology and Environmental Safety* 283, 116856. DOI: https://doi.org/10.1016/j.ecoenv.2024.116856 (in English)

17. Ragnoli, M., Pavone, M., Epicoco, N., Pola, G., De Santis, E., Barile, G., Stornelli, V. (2023) A condition and fault prevention monitoring system for industrial computer numerical control machinery. *IEEE Access* 11, 60633–60652. DOI: https://doi.org/10.1109/ACCESS.2017. (in English)

18. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. (2023) Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 118(2), pp. 83–94 (in English)

Uzair, M., Salah Yacoub, A.-K., Karam Manaf, A.-J., Ibrahim Abdulrahman, A.B. (2022) A Low-Cost IoT Based Buildings Management System (BMS) Using Arduino Mega 2560 and Raspberry Pi 4 for Smart Monitoring and Automation. *International Journal of Electrical and Computer Engineering Systems* 13(3), 219–236 (in English)