ИНТЕГРАЦИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗВЁРТЫВАНИИ СОВРЕМЕННОЙ ИТ-ИНФРАСТРУКТУРЫ

БУРОВЦЕВ Валерий Тимурович
студент магистратуры
НЕСТЯГИН Никита Леонидович
студент магистратуры
МИРЭА – Российский технологический университет
г. Москва, Россия

В статье рассматривается интеграция облачных технологий и искусственного интеллекта для повышения информационной безопасности современных IT-инфраструктур. Облачные платформы обеспечивают централизованное управление, масштабируемость, глобальную видимость угроз, автоматическое обновление защитных механизмов и резервное копирование. Искусственный интеллект дополняет их, предоставляя возможности анализа, обнаружения атак и автоматизации реагирования. Интеграция облачных технологий и искусственного интеллекта становится важной частью информационной безопасности. Эти инструменты совместно усиливают предотвращение, обнаружение и реагирование на угрозы, предоставляя компаниям, внедряющим их, конкурентное преимущество в защите данных и репутации в условиях меняющегося ландшафта киберугроз.

Ключевые слова: кибератаки, резервное копирование, машинное обучение, облачные технологии, киберугрозы.

Влияние современных технологий на информационную безопасность и необходимость интеграции облачных технологий и искусственного интеллекта. Современные ИТ-инфраструктуры стали невероятно сложными: они включают в себя облачные сервисы, локальные сети, устройства Интернета вещей (IoT) и множество других элементов. С развитием технологий растут и угрозы информационной безопасности: кибератаки становятся всё более изощрёнными, а злоумышленники используют всё более изощрённые методы. В таких условиях интеграция облачных технологий и искусственного интеллекта (ИИ) становится необходимым шагом для защиты данных и систем [3].

Проблемы. Ранее для защиты ИТ-инфраструктуры использовались традиционные методы, такие как антивирусы, межсетевые экраны (firewall) и системы предотвращения вторжений. Эти инструменты работают на основе заранее заданных правил и сигнатур, что делает их неэффективными против новых и быстро развивающихся угроз, таких как:

– атаки нулевого дня;

– использование скрытых методов проникновения, например, с помощью шифрования;

– массированные DDoS-атаки, направленные на перегрузку серверов.

Основная проблема традиционных подходов заключается в их реактивности: защита вступает в действие только после того, как угроза уже идентифицирована.

Как облачные технологии помогают в информационной безопасности. Облачные технологии предоставляют мощные инструменты для защиты информации благодаря своей гибкости, масштабируемости и централизованности. Вот несколько ключевых преимуществ облачных технологий в контексте безопасности:

1. **Централизованное управление**. Все данные о событиях и попытках атак собираются в единой системе, что упрощает анализ.

2. **Глобальная видимость угроз**. Облачные сервисы подключены к тысячам других систем, что позволяет быстрее распознавать новые угрозы и предупреждать клиентов.

3. **Автоматическое обновление защитных систем**. Пользователи получают актуальные версии программного обеспечения безопасности, что минимизирует риск уязвимостей.

Например, облачные платформы, такие как AWS и Microsoft Azure, уже внедряют решения

для мониторинга аномальной активности и защиты от DDoS-атак.

Роль искусственного интеллекта в информационной безопасности. ИИ меняет подход к безопасности, делая его не только реактивным, но и проактивным. Он способен обрабатывать огромные объёмы данных, выявлять скрытые угрозы и прогнозировать поведение злоумышленников.

Основные возможности ИИ в обеспечении ИБ.

1. **Анализ поведения**. ИИ изучает привычные действия пользователей и систем. Если происходит что-то необычное, например вход в систему с незнакомого устройства, это немедленно фиксируется.

2. **Обнаружение атак нулевого дня**. С помощью машинного обучения ИИ может находить паттерны, характерные для новых атак, даже если их сигнатуры ещё не известны

3. **Автоматизация реагирования**. В случае обнаружения угрозы ИИ может автоматически заблокировать доступ, изолировать систему или уведомить администратора.

Синергия облаков и искусственного интеллекта. Интеграция облаков и ИИ создаёт мощную комбинацию для защиты современных ИТ-инфраструктур. Облака предоставляют масштабируемые вычислительные мощности и централизованные данные, а ИИ обеспечивает интеллектуальный анализ и принятие решений.

Преимущества интеграции:

1. **Ускоренное обнаружение угроз**. Анализ угроз происходит в режиме реального времени благодаря облачным вычислениям и алгоритму.

2. **Снижение влияния человеческого фактора**. Автоматизированные процессы минимизируют риск ошибок, связанных с действиями человека.

3. **Прогнозирование атак**. Комбинируя данные из облачных источников и алгоритмы ИИ, можно предсказать потенциальные угрозы и подготовиться к ним заранее.

Защита корпоративной сети с использованием облачных технологий и искусственного интеллекта. Рассмотрим модель организации защиты информации, применяемую на практике крупным ритейлером, управляющем сетью магазинов по всему миру, которую мы, в целях соблюдения корпоративной этики, назовем XYZ. Они используют гибридную IT-инфраструктуру: часть серверов находится в локальных дата-центрах, а часть – в облаке. Это делает их цельной сетью привлекательной для кибератак, включая попытки взлома, DDoS-атаки и применения вирусов-шифровальщиков.

Шаги интеграции облачных технологий и ИИ для обеспечения безопасности:

1. Централизованный мониторинг через облако:

Компания разворачивает платформу Microsoft Azure Security Center. Эта облачная система собирает данные о событиях безопасности со всех серверов, рабочих станций и сетевых устройств. Все логи, включая подозрительные попытки доступа, загружаются в облако для анализа.

2. Использование ИИ для анализа данных:

В системе настроены алгоритмы машинного обучения, которые анализируют сетевой трафик и действия пользователей. Например, ИИ выявляет, что сотрудник, никогда не работавший ночью, пытается получить доступ к конфиденциальным данным в нерабочее время. Алгоритмы также обнаруживают новые модели атак, которые раньше не встречались [6].

3. Автоматическое реагирование на угрозы:

При обнаружении подозрительной активности ИИ автоматически блокирует доступ с подозрительного IP-адреса, уведомляет администратора и запускает сценарии расследования. Например, если подозрительная активность связана с вирусом-шифровальщиком, ИИ изолирует заражённый сегмент сети, чтобы предотвратить распространение угрозы.

4. Резервное копирование данных в облаке:

В случае атаки, например, ransomware, данные всех критически важных систем уже защищены резервными копиями в облаке (AWS Backup). Это позволяет быстро восстановить работоспособность, минимизировав простой.

Многие компании используют блокчейн-платформы, размещённые в облаке, для повышения прозрачности и безопасности данных.

Blockchain (или цепочка блоков) – это распределенная база данных, которая использует криптографию для обеспечения безопасности и целостности данных. Основ-

ной принцип работы blockchain состоит в записи данных в блоки и их последующем цепочечном соединении, что создает неизменную и непрерывную цепь блоков [4].

5. Прогнозирование и предотвращение атак:

Используя глобальную сеть облачных провайдеров, таких как AWS или Google Cloud, компания получает предупреждения о новых уязвимостях или активных угрозах. Например, система обнаруживает, что массовые атаки с использованием определённой уязвимости начались в другом регионе, и применяет обновления безопасности до того, как атака затронет компанию XYZ.

За счет использования этой стратегией компанией получены следующие результаты:

– уменьшено время обнаружения и реагирования на угрозы (с часов до минут);

– снижен риск потери данных благодаря регулярному резервному копированию;

– предотвращены попытки DDoS-атак с использованием глобальной облачной инфраструктуры;

– обеспечено соблюдение международных стандартов безопасности (GDPR, PCI DSS);

– сокращены расходы на детектирование и реагирование на инциденты при использовании технологий ИИ (рисунок 1);

– снижено время обнаружения угроз при использовании технологий ИИ (рисунок 2).

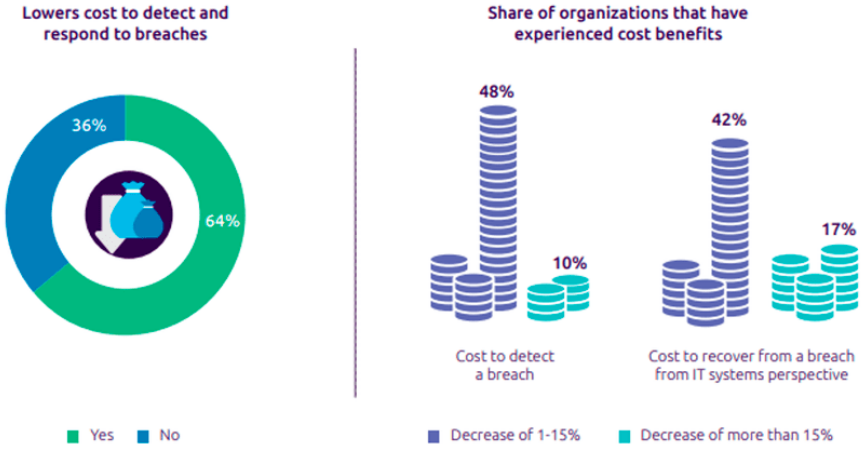

Рисунок 1. **Статистика сокращения расходов на детектирование и реагирование на инциденты при использовании технологий ИИ [4]**

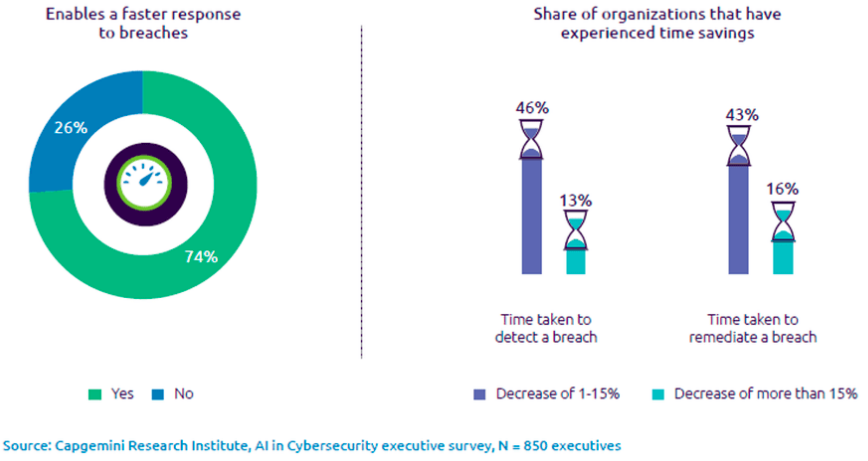

Рисунок 2. **Статистика сокращения времени обнаружения угроз при использовании технологий ИИ [4]**

Этот пример показывает, как синергия облаков и ИИ защищает даже сложные IT-инфраструктуры от современных киберугроз [1].

Уже 95% российских финтех компаний уже внедрили технологии ИИ в основные процессы – такую статистику привела Ассоциация ФинТех (предоставление финансовых услуг и сервисов с использованием инновационных технологий, таких как Big Data, искусственный интеллект, машинное обучение, роботизация, блокчейн, облачные технологии, биометрия и другие, объединяется под термином «финтех» или финансовые технологии) в исследовании «Применение технологий искусственного интеллекта на финансовом рынке» [2].

А.А.Рыбалка и Ю.З. Насиров выделяют следующие качества облачных технологий, которые отличают их от других информационных технологий: «быстрая и максимально комфортная масштабируемость системы; управляемое автоматизированное самообслуживание» [5].

Заключение. Интеграция облачных технологий и искусственного интеллекта становится неотъемлемой частью информационной безопасности. Вместе эти инструменты предоставляют широкие возможности для предотвращения, обнаружения и реагирования на угрозы. Компании, которые своевременно внедряют такие решения, получают конкурентное преимущество, защищая свои данные и репутацию в условиях постоянно меняющихся киберугроз.

В результате проведённого исследования рекомендуется расширять использование возможностей искусственного интеллекта и облачных технологий для повышения уровня защиты информационных систем. Интеграция этих технологий позволит улучшить мониторинг, обнаружение угроз и автоматизацию реакции на инциденты безопасности, что в свою очередь повысит устойчивость ИТ-инфраструктур к современным киберугрозам.

ЛИТЕРАТУРА

1. *Гладилин И.А.* Оценка рисков информационной безопасности организации // Лучшая научная работа 2022: сборник статей III Международного научно-исследовательского конкурса, Пенза, 15 января 2022 г. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 26-31.
2. *Клементьев И.П., Устинов В.А.* Введение в облачные вычисления. Учебное пособие. – М.: Издательство ИНТУИТ, 2016. – 310 с.
3. Искусственный интеллект в финтехе и банкинге // ГРАНТ.РУ: [сайт]. – URL:https://www.garant.ru/article/1649470/ (дата обращения: 29.02.2024).
4. *Нестягин Н.Л.* Вызовы глобализации и развитие цифрового общества в условиях новой реальности (Москва, 22 мая 2023 года).
5. *Рыбалка А.А., Насиров Ю.З.* Облачные технологии как часть инновационного прогресса в области экономики // Академическая публицистика. – 2021. – № 1. – С. 122-125
6. *Широкова Е.А.* Облачные технологии // Современные тенденции технических наук: материалы междунар. науч. конф. (г. Уфа, октябрь 2011 г.). – Уфа: Лето, 2011. – С. 30-33.
7. Why AI Is The Future Of Cybersecurity // Forbes от 14 июля 2019 г.

INTEGRATION OF CLOUD TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE FOR ENSURING INFORMATION SECURITY DURING THE DEPLOYMENT OF MODERN IT INFRASTRUCTURE

NESTYAGIN Nikita Leonidovich
Undergraduate Student
BUROVTSEV Valeriy Timurovich
Undergraduate Student
MIREA – Russian Technological University
Moscow, Russia

The article explores the integration of cloud technologies and artificial intelligence to enhance the information security of modern IT infrastructures. Cloud platforms provide centralized management, scalability, global threat visibility, automated updates of protective mechanisms, and backup solutions. Artificial intelligence complements these capabilities by enabling analysis, attack detection, and response automation. The integration of cloud technologies and artificial intelligence is becoming a crucial component of information security. Together, these tools enhance threat prevention, detection, and response, giving companies that adopt them a competitive advantage in protecting their data and reputation amidst an ever-evolving cyber threat landscape.
Keywords: cyberattacks, backup, machine learning, cloud technologies, cyber threats.