АРХИТЕКТУРА ПОСТРОЕНИЯ КОНЦЕПЦИИ НУЛЕВОГО ДОВЕРИЯ С КОМПОНЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ПОЛЫШЕВА Анастасия Кирилловна
студент
ШАФИКОВ Марат Русланович
старший преподаватель кафедры управления информационной безопасностью
Уфимский университет науки и технологий
г. Уфа, Россия

Концепция нулевого доверия – это стратегия информационной безопасности, основанная на предположении, что нельзя доверять ни одному узлу или субъекту в информационной среде. В рамках данной концепции все узлы считаются небезопасными (недоверенными). В данной статье раскрываются три фундаментальных концепции, на которой строится модель нулевого доверия, приводятся примеры продуктов и систем, используемых для реализации модели нулевого доверия. Кроме того, в статье рассматривается развитие искусственного интеллекта в модели нулевого доверия для обеспечения повышенной информационной безопасности.

Ключевые слова: нулевое доверие, безопасность, угроза, инсайдер, искусственный интеллект, механизм искусственного интеллекта.

Достижения в области сетевых технологий и облачных вычислений привели к созданию сложных корпоративных архитектур с несколькими уровнями безопасности, включая сегментацию сети, системы защиты приложений, облачных вычислений и контейнеров. Такая архитектура затрудняет работу служб безопасности и ИТ-отделов по организации безопасного доступа для сотрудников как в офисе, так и удаленно, что делает еще более важным обеспечение мгновенного и безопасного подключения как на управляемых, так и на неуправляемых устройствах [6].

В своем отчете 2010 г. Forrester Research о нулевом доверии Джон Киндерваг призвал адаптировать общепринятый подход к сетевой безопасности «доверяй, но проверяй» к стратегии «проверяй и никогда не доверяй» [6].

Почти каждое устройство безопасности, например, брандмауэр, имеет как минимум один порт, помеченный как «недоверенный», и другой, помеченный как «доверенный». Предположение о том, что специалисты по безопасности могут легко определить, каким сетевым интерфейсам можно доверять, заложено в самой конструкции устройства безопасности. Однако само по себе автоматическое предположение о том, что можно «доверять» любому человеку или любому устройству внутри сетевого периметра организации, является ошибкой.

Нулевое доверие – решение этой проблемы. Модель нулевого доверия предотвращает вторжения атакующих как внутри, так и снаружи сети, упрощает контроль и управление политиками безопасности, обеспечивает детальное сегментирование сервисов, а также обеспечивает видимость и аудит на уровне, который был невозможен при использовании традиционных средств безопасности [3].

Использование архитектуры нулевого доверия не требует комплексной замены существующих сетей или массового перехода на новые технологии – вместо этого концепция нулевого доверия должна усилить другие существующие методы и средства обеспечения безопасности.

При переходе к концепции нулевого доверия происходит отказ от идеи доверенной сети и недоверенной сети - в концепции нулевого доверия весь сетевой трафик является недоверенным [4].

Как упоминалось ранее, нулевое доверие – это новая концепция кибербезопасности, которая придерживается принципа «проверяй и никогда не доверяй», требующая постоянной идентификации и проверки прав доступа. Это основной принцип нулевого доверия,

суть которого можно сформулировать следующим образом:

1. Каждый источник данных и вычислительный сервис рассматриваются как актив организации, требующий защиты.

2. Все коммуникации считаются небезопасными, независимо от местоположения сети, указанного в запросе на доступ. Ни один объект, запрашивающий доступ, не является автоматически доверенным.

3. Доступ к ресурсам предоставляется на основе каждой сессии [2].

4. При принятии решений о доступе учитываются характеристики устройства, а также поведенческие и внешние факторы.

5. Применяется принцип наименьших привилегий.

6. Разрешение на доступ запрашивается постоянно, а не предоставляется автоматически.

Но переход на концепцию нулевого доверия для отдельных организаций может оказаться долгим и трудным. Поэтому в 2019 г. аналитической компанией Gartner был предложен универсальный фреймворк Secure Access Service Edge (SASE).

Такой новый пакет технологий, как SASE, позволяет выявлять конфиденциальные данные и вредоносные программы, а также расшифровывать трафик с помощью непрерывного мониторинга подключений пользователей и устройств к облачным сервисам. Основой фреймворка как раз и является модель нулевого доверия.

Как показало исследование Gartner, 63% компаний во всем мире полностью либо частично внедрили стратегию нулевого доверия, причем для 78% из них эти инвестиции составили менее 25% их общего бюджета на кибербезопасность [5].

Опрос Gartner, проведённый в четвёртом квартале 2023 г. среди 303 руководителей служб безопасности, чьи организации уже внедрили полностью или частично или планируют внедрить стратегию нулевого доверия, показал, что 56% организаций в первую очередь внедряют стратегию нулевого доверия, потому что это считается передовой отраслевой практикой [5].

На рисунке 1 представлена процентная доля среды, охватываемой нулевым доверием.

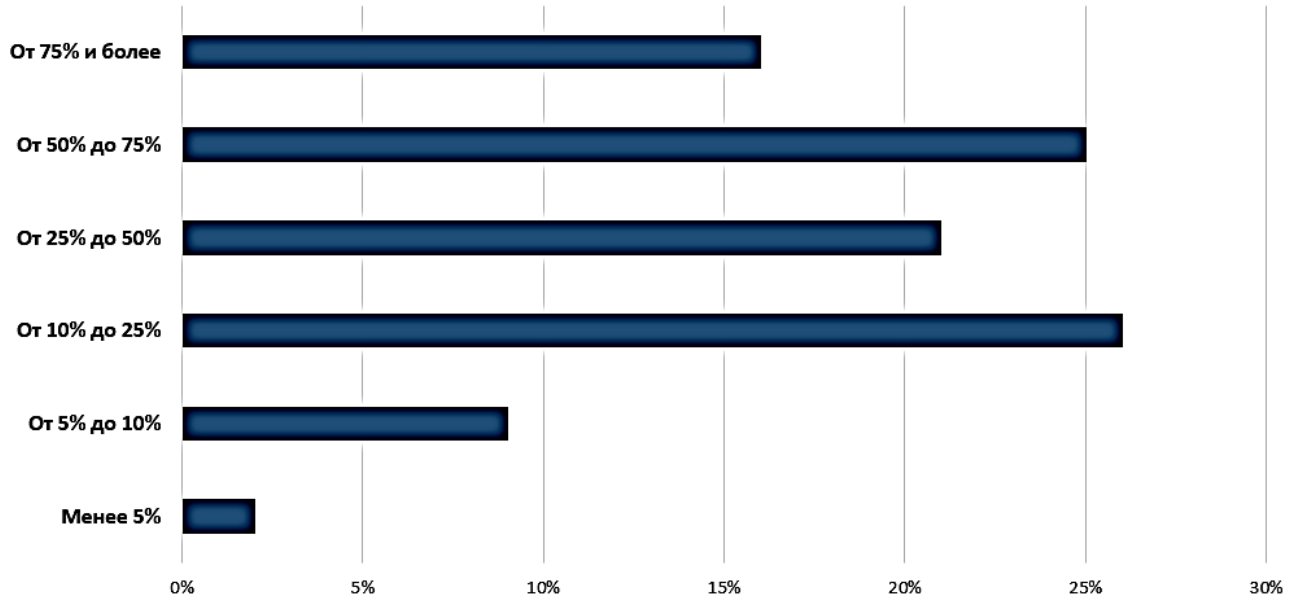

Рисунок 1. **Процент охвата корпоративной среды стратегией нулевого доверия**

В 2021 г. была представлена интеллектуальная архитектура нулевого доверия i-ZTA (Intelligent Zero Trust Architecture) [1]. Ключевыми элементами данной разработанной модели, в основе которых лежит искусственный интеллект, являются такие механизмы, как IPE, INSSA и IGP.

На рисунке 2 представлены основные компоненты и механизмы искусственного интеллекта архитектуры i-ZTA.

Интеллектуальный механизм определения политики IPE (Intelligent Policy Engine) использует алгоритм доверия искусственного интеллекта для авторизации запросов на доступ на основе привилегий и состояния безопасности субъекта, правил политики безопасности, состояния сети и оценки, отражающей уровень доверия к доступу. IPE использует нейронную сеть с долговременной и кратковременной памятью для оценки риска предоставления доступа субъекту на основе всех предыдущих действий субъекта и сети.

Политика IPE разрабатывается с помощью алгоритма обучения с подкреплением (Reinforcement learning, RL) с целью минимизации вероятности ложноположительных и ложноотрицательных результатов. После принятия решения, в результате которого предоставляется доступ или отказывается в доступе, IPE отслеживает состояние безопасности сеанса – насколько строго субъект соблюдает правила политики безопасности. Интеллектуальный анализ состояния безопасности сети INSSA (Intelligent Network Security State Analysis) может использовать графовые нейронные сети (GNN), в частности рекуррентную GNN, для определения состояния безопасности сети и моделирования моделей связи в сети – целью является присвоение узлам оценок риска таким образом, чтобы общая оценка безопасности при предоставлении доступа была максимальной [1].

Такой механизм выполняет оценку риска при доступе к заданному ресурсу в сети.

Кроме того, еще одной важной задачей интеллектуального анализа состояния безопасности сети является обнаружение аномалий. Цель этой задачи – обнаружить и предотвратить потенциальные атаки, например, такие как DoS- и DDoS-атаки.

Пользовательский ИИ-механизм IGP (Intelligent aGent/Portal) предназначен для моделирования состояния безопасности объекта. IGP анализирует состояние безопасности сетевого трафика субъекта и обеспечивает его осведомленность о состоянии сети. Целью обучения IGP является поддержание высокого уровня безопасности субъекта при доступе к сетевым ресурсам [1].

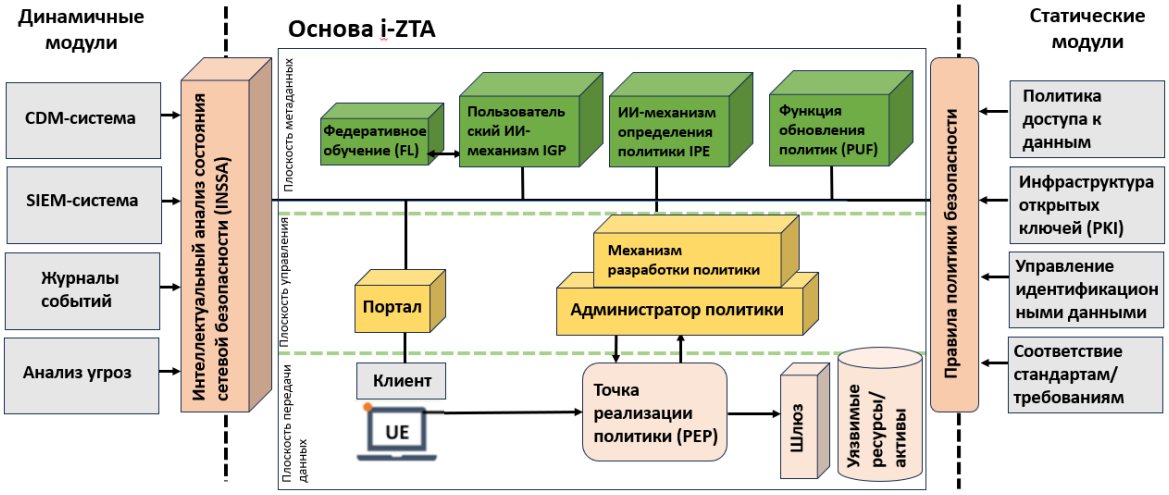

Рисунок 2. **Логические компоненты предлагаемого i-ZTA, показывающие правила политики безопасности и механизмы искусственного интеллекта для осуществления интеллектуального мониторинга, оценки и принятия решений**

Все компоненты и механизмы ИИ, представленные в данной архитектуре i-ZTA, работают в единой структуре для удовлетворения повышенных потребностей в информационной безопасности [1].

На сегодняшний день происходит активное слияние искусственного интеллекта и модели нулевого доверия в области обеспечения информационной безопасности в недоверенных сетях.

По данным исследования MarketsandMarkets, прогнозируется, что спрос на искусственный интеллект в сфере кибербезопасности к 2026 г. вырастет до 38,2 млрд долла-

ров при среднегодовом темпе роста 23,3%. В представленном исследовании также делается акцент на растущую востребованность в искусственном интеллекте в сфере кибербезопасности в связи с участившимися случаями киберугроз и дефицитом квалифицированных кадров в области кибербезопасности.

Использование традиционных средств обеспечения безопасности не гарантируют полную защиту сети – большинство таких средств не предназначены для облачных сред, проверки политик безопасности и создания прозрачной инфраструктуры безопасности. Кроме того, они используют базы данных с информацией об известных угрозах, чего сейчас уже недостаточно. Для обеспечения эффективной защиты специалисты по безопасности должны моментально принимать решения о том, кому и к каким ресурсам предоставлять доступ, и учитывать степень конфиденциальности соответствующих данных.

Поэтому для защиты корпоративных ресурсов все чаще переходят на адаптивные, непрерывные и интеллектуальные технологии кибербезопасности, в основе которых лежат алгоритмы искусственного интеллекта и машинного обучения.

Новые решения в области кибербезопасности, использующие искусственный интеллект и машинное обучение, для обнаружения угроз используют такие источники информации для управления системами, как журнальные файлы, бизнес-транзакции, конфигурации приложений, назначения ролей и прав и другие источники, неизвестные традиционным средствам обеспечения безопасности [7].

Одним из таких решений является платформа Oracle Management Cloud, которая представляет собой интегрированный набор служб мониторинга, управления и анализа, использующий технологии машинного обучения и больших данных для работы с самыми разными наборами операционных данных [7]. Такая платформа строится на модели нулевого и использует предварительно запрограммированные модели искусственного интеллекта, объединяющий отдельные возможности модулей в единой системе безопасности.

У Oracle есть набор облачных сервисов, который обеспечивает большую прозрачность, эффективный анализ и автоматизацию информационной безопасности - все эти сервисы работают на платформе Oracle Management Cloud (OMC). Например, сервис Oracle Security Monitoring and Analytics (SMA) Cloud Service позволяет быстро обнаруживать, расследовать и устранять угрозы безопасности, и сопоставлять результаты с привилегиями, назначенными на платформе управления идентификацией и доступом (Identity and Access Management, IAM) или Active Directory.

К тому же современная система безопасности может адаптироваться к меняющимся условиям благодаря технологии машинного обучения, которая автоматически выявляет и устраняет проблемы без участия человека. Это так называемое адаптивное реагирование.

Сервисы брокера безопасного доступа CASB (Cloud Access Security Broker) используют анализ поведения пользователей и иных субъектов (User Entity Behavior Analytics, UEBA) для определения индивидуальных и ключевых критериев поведения для каждого из них [7]. Такие сервисы направлены на непрерывное сравнение необычных действий с предполагаемыми для выявления аномального, подозрительного или потенциально небезопасного поведения. Обнаружив наличие аномалии, брокер безопасного доступа запускает интеллектуальную реакцию и взаимодействует с системой регистрации инцидентов и управления ими для сравнения случившегося с аналогичными случаями и предложения необходимого решения с участием сотрудника.

К подозрительным и аномальным действиям может привести и кража учетных данных доверенного пользователя, что позволит санкционированно проникнуть в сеть организации. В таком случае CASB подает сигнал тревоги и использует более строгие ограничения безопасности – например, требует двухфакторную аутентификацию для доступа к определенному ресурсу.

Централизованная система идентификации позволяет сотрудникам службы безопасности проверять, какие пользователи и в какое время получают доступ к тем или иным ресурсам.

Oracle также использует технологию ма-

шинного обучения для группировки пользователей на основе общих поведенческих характеристик – откуда они приходят, к каким внутренним ресурсам и облачным сервисам обращаются и получают доступ и в какое время суток работают. Такая группировка позволяет легко идентифицировать аномальное поведение. Например, если специалист отдела кадров вдруг начинает вести себя как финансовый директор, это может быть индикатором украденной учетной записи или инсайдерской угрозы.

Для организаций с развитой цифровой инфраструктурой эффективный анализ данных, связанных с безопасностью, имеет огромное значение. Процессы, выполняемые вручную сотрудниками, и технологии, основанные на соблюдении определенных правил, уже не могут справиться с современными киберугрозами. Для эффективной защиты необходимы автоматизированные технологии искусственного интеллекта и машинного обучения с учетом контекста, позволяющие обнаруживать и отражать известные и неизвестные угрозы.

Концепция нулевого доверия вместе с искусственным интеллектом и машинным обучением обеспечивают безопасную основу. Если вы сможете проверять и регистрировать каждого пользователя, каждое устройство и каждую точку доступа, вы сможете создать более детальные и информативные политики и средства контроля, которые обнаружат и смягчат действия злоумышленников и неправомерное использование технологий [7].

СПИСОК ЛИТЕРАТУРЫ

1. Адаптивный анализ на основе машинного обучения: будущее кибербезопасности // Oracle | Cloud Applications and Cloud Platform: [сайт]. – URL:https://www.oracle.com/a/ocom/docs/ai-security_whitepaper.pdf (дата обращения: 02.11.2024).

2. Внедрение модели нулевого доверия в информационной безопасности (No More Chewy Centers: Introducing The Zero Trust Model Of Information Security) // Palo Alto Networks: [сайт]. – URL:https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf (дата обращения: 06.10.2024).

3. *Дипа Аджиш* Значение искусственного интеллекта в технологиях с нулевым доверием: развернутый обзор (The significance of artificial intelligence in zero trust technologies: a comprehensive review) // SpringerOpen: [сайт]. – URL:https://jesit.springeropen.com/articles/10.1186/s43067-024-00155-z (дата обращения: 06.10.2024).

4. *Кейван Рамезампур, Джитхин Джаганнат* Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning / Кейван Рамезампур, Джитхин Джаганнат // ResearchGate: [сайт]. – URL:https://www.researchgate.net/ publication/351342318_Intelligent_Zero_Trust_Architecture_for_5G6G_Tactical_Networks_Principles_Challenges_and_the_Role_of_Machine_Learning#pf5 (дата обращения: 06.10.2024).

5. Создание безопасности в структуре вашей сети: Архитектура сети с нулевым доверием (Build Security Into Your Network’s DNA: The Zero Trust Network Architecture) // Palo Alto Networks: [сайт]. – URL:https://www.itbriefcase.net/downloads/Forrester_zero_trust_DNA.pdf (дата обращения: 06.10.2024).

6. Что такое нулевое доверие? Архитектура, принципы и технология (What Is Zero Trust? Architecture, Principles, and Technology) // TIGERA: Security and observability for containers and Kubernetes: [сайт]. – URL:https://www.tigera.io/learn/guides/zero-trust/ (дата обращения: 06.10.2024).

7. Что такое нулевое доверие? (What is zero trust?) // Red Hat: [сайт]. – URL:https://www.redhat.com/en/topics/security/what-is-zero-trust (дата обращения: 06.10.2024).

ARCHITECTURE FOR BUILDING A ZERO-TRUST CONCEPT WITH COMPONENTS OF ARTIFICIAL INTELLIGENCE

POLYSHEVA Anastasia Kirillovna
Student
SHAFIKOV Marat Ruslanovich
Senior Lecturer of the Department of Information Security Management
Ufa University of Science and Technology
Ufa, Russia

The concept of zero trust is an information security strategy based on the assumption that no node or entity in the information environment can be trusted. Under this concept, all nodes are considered insecure (untrusted). This article discusses the three fundamental concepts on which the zero-trust model is based, giving examples of products and systems used to implement the zero-trust model. In addition, the article discusses the development of artificial intelligence in a zero-trust model to provide enhanced information security.
Keywords: zero trust, security, threat, insider, artificial intelligence, artificial intelligence engine.