ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ НЕЙРОСЕТЕЙ

С.Р. Шишкин, *Московский технический университет связи и информатики, sergeyshishkin62@gmail.com.*

УДК 004.056.53:004.89

Аннотация. В условиях роста числа и сложности кибератак традиционные методы защиты информации становятся менее эффективными. В статье рассматривается применение имитационного моделирования, усиливаемого нейросетевыми технологиями, для решения задач кибербезопасности. Имитационное моделирование позволяет воспроизводить реалистичные сценарии атак, анализировать их воздействие на системы и разрабатывать адаптивные механизмы защиты. Рассмотрены примеры использования нейросетей, такие как генеративно-состязательные сети (*GAN*) для создания новых сценариев атак, автоэнкодеры для детекции аномалий и глубокое обучение для классификации угроз. Подчеркиваются преимущества симулятивного подхода, включая возможность тестирования новых алгоритмов, адаптации к ранее неизвестным угрозам и минимизации рисков для реальной инфраструктуры. В заключении обсуждаются проблемы, связанные с ресурсоемкостью, этическими аспектами и сложностью построения моделей, а также предлагаются направления для их преодоления.

Ключевые слова: имитационное моделирование; кибербезопасность; нейросети; генеративно-состязательные сети (*GAN*); автоэнкодеры; глубокое обучение; *DDoS*-атаки; аномалии; прогнозирование угроз; информационная безопасность.

SIMULATION MODELING IN INFORMATION SECURITY USING NEURAL NETWORKS

Sergey Shishkin, *Moscow Technical University of Communications and Informatics.*

Annotation. As the number and complexity of cyberattacks grow, traditional methods of information security are becoming less effective. This article examines the application of simulation modeling enhanced by neural network technologies to address cybersecurity challenges. Simulation modeling enables the reproduction of realistic attack scenarios, analysis of their impact on systems, and the development of adaptive defense mechanisms. Examples of neural network applications are discussed, including Generative Adversarial Networks (*GAN*) for creating new attack scenarios, autoencoders for anomaly detection, and deep learning for threat classification. The advantages of the simulation approach are highlighted, such as testing new algorithms, adapting to previously unknown threats, and minimizing risks to real infrastructure. The conclusion discusses challenges related to resource intensity, ethical concerns, and model complexity, and suggests directions for overcoming them.

Keywords: simulation modeling; cybersecurity; neural networks; Generative Adversarial Networks (*GAN*); autoencoders; deep learning; *DDoS*-attacks; anomalies; threat prediction; information security.

Введение

Современное развитие цифровых технологий сопровождается не только ростом их внедрения в различные сферы деятельности, но и значительным

увеличением числа кибератак. Усложнение атакующих методов, появление новых видов угроз и постоянное совершенствование инструментов злоумышленников ставят под угрозу безопасность информационных систем, критической инфраструктуры и личных данных [1, 2]. В условиях динамично изменяющегося ландшафта угроз традиционные методы защиты информации становятся менее эффективными, что требует применения инновационных подходов [3].

Одним из перспективных инструментов является имитационное моделирование, которое позволяет воссоздавать реальные сценарии кибератак для их анализа и выработки стратегий противодействия. Использование методов нейросетевых технологий в рамках имитационного моделирования открывает новые возможности для построения интеллектуальных и адаптивных систем безопасности. Нейросети способны анализировать сложные паттерны, прогнозировать развитие угроз и адаптировать защитные механизмы к новым вызовам.

Имитационное моделирование как инструмент в сфере защиты информации

Имитационное моделирование представляет собой процесс создания и исследования моделей, воспроизводящих динамику реальных систем в условиях, максимально приближенных к реальности. В контексте защиты информации данный метод широко применяется для воссоздания сценариев кибератак с целью анализа их воздействия на системы и выработки оптимальных мер противодействия.

Основной принцип имитационного моделирования в сфере кибербезопасности заключается в возможности воспроизведения различных видов атак, таких как распределенные атаки отказа в обслуживании (*Distributed Denial of Service – DDoS*), фишинг, попытки несанкционированного доступа и целенаправленные атаки (*Advanced Persistent Threats – APT*). Эти сценарии позволяют тестировать защитные механизмы и определять слабые стороны системы без риска для реальной инфраструктуры.

Одной из ключевых задач в сфере защиты информации является не только выявление текущих уязвимостей, но и способность систем адаптироваться к новым угрозам. Имитационное моделирование предоставляет возможность тестирования механизмов защиты в безопасной среде, приближенной к реальным условиям. Этот подход позволяет анализировать последствия атак, разрабатывать стратегии противодействия и минимизировать возможный ущерб.

Имитационные модели позволяют воспроизводить сценарии различных кибератак с высокой степенью детализации. Например, в случае *DDoS*-атаки можно оценить, как система распределяет нагрузку и насколько эффективно работают фильтрующие механизмы. Это дает возможность протестировать системы обнаружения вторжений (*Intrusion Detection System – IDS*) и автоматизированные средства блокировки атак.

На приведенном ниже графике (рис. 1) демонстрируется изменение пропускной способности сети под воздействием *DDoS*-атаки [4]. Красная вертикальная линия обозначает момент начала атаки, после чего наблюдается резкое снижение доступных ресурсов.

График на рис. 1 демонстрирует, как пропускная способность сети уменьшается под воздействием высокоинтенсивного вредоносного трафика. Начало атаки (обозначено красной вертикальной линией) приводит к резкому падению доступных ресурсов, что вызывает деградацию или полный отказ в обслуживании.

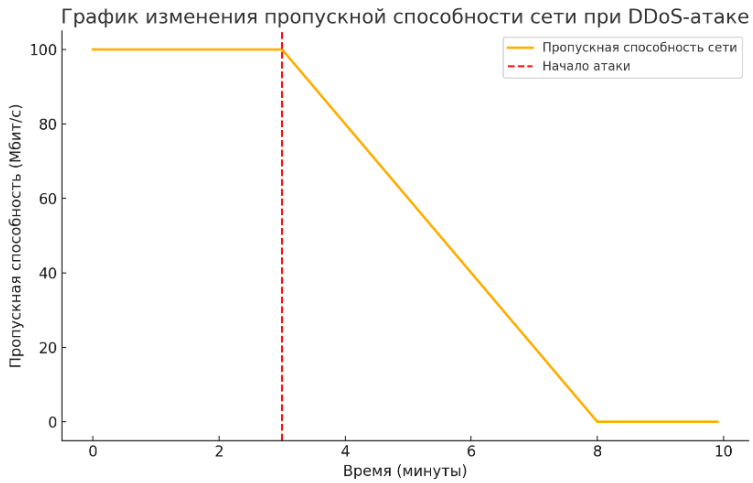

Рисунок 1

Имитационные эксперименты требуют значительно меньших затрат, чем тестирование в реальной инфраструктуре. Например, моделирование атаки на сложные системы, такие как инфраструктуры облачных вычислений (*Cloud Computing*) или интернет вещей (*Internet of Things – IoT*), может проводиться виртуально. Это снижает затраты на настройку и обслуживание оборудования, а также позволяет избежать простоев систем.

Более того, моделирование позволяет воспроизводить редкие и опасные сценарии атак без риска для реальной инфраструктуры. Например, тестирование атак методом перебора паролей (*Brute Force*) или анализа уязвимостей аутентификации можно проводить в изолированной среде, где злоумышленник «воссоздается» алгоритмически.

В табл. 1 представлены ключевые различия между физическим тестированием и имитационным моделированием.

Таблица 1.

Критерий	**Физическое тестирование**	**Имитационное моделирование**
Затраты на оборудование	Высокие	Минимальные
Риск для инфраструктуры	Присутствует	Отсутствует
Масштабируемость	Ограничена	Высокая
Точность сценариев атак	Часто упрощенные	Высокодетализированные

Имитационное моделирование не только воспроизводит текущие атаки, но и позволяет анализировать и прогнозировать действия злоумышленников. Это особенно важно для защиты от целенаправленных атак, которые могут развиваться поэтапно, включая разведку, проникновение и эскалацию.

С помощью методов машинного обучения и нейросетей возможно создание интеллектуальных моделей, способных не только воспроизводить известные атаки, но и «предсказывать» новые подходы злоумышленников. Например, алгоритмы могут обучаться на реальных данных о кибератаках, чтобы выявлять потенциальные уязвимости, еще не задействованные злоумышленниками.

Одной из наиболее актуальных угроз для современных систем остаются *DDoS*-атаки [5, 6], целью которых является перегрузка серверов или сетевой

инфраструктуры огромным количеством трафика. В результате сервисы становятся недоступными для легитимных пользователей, что приводит к значительным финансовым потерям и репутационным рискам. Имитационное моделирование позволяет воссоздавать подобные сценарии с высокой степенью детализации, анализируя поведение системы при изменении нагрузки и тестируя различные защитные стратегии. В ходе моделирования, например, можно сравнивать традиционные методы фильтрации трафика с адаптивными нейросетевыми алгоритмами, обученными на реальных данных об аномалиях. Такие эксперименты позволяют оценить эффективность динамического выявления вредоносного трафика и уменьшить вероятность ложных срабатываний.

Наряду с *DDoS*-атаками значительную угрозу представляют попытки несанкционированного доступа. Атаки методом перебора паролей продолжают использоваться для взлома систем аутентификации, особенно тех, где отсутствуют дополнительные меры безопасности. Имитация подобных атак помогает оценить надежность защитных механизмов, таких как двухфакторная аутентификация (*Two-Factor Authentication – 2FA*), которая добавляет второй уровень проверки через одноразовые коды или биометрические данные. Также можно анализировать, насколько эффективно система распознает подозрительную активность и блокирует учетные записи при многократных неудачных попытках входа. Моделирование позволяет выявить уязвимости и доработать существующие алгоритмы аутентификации.

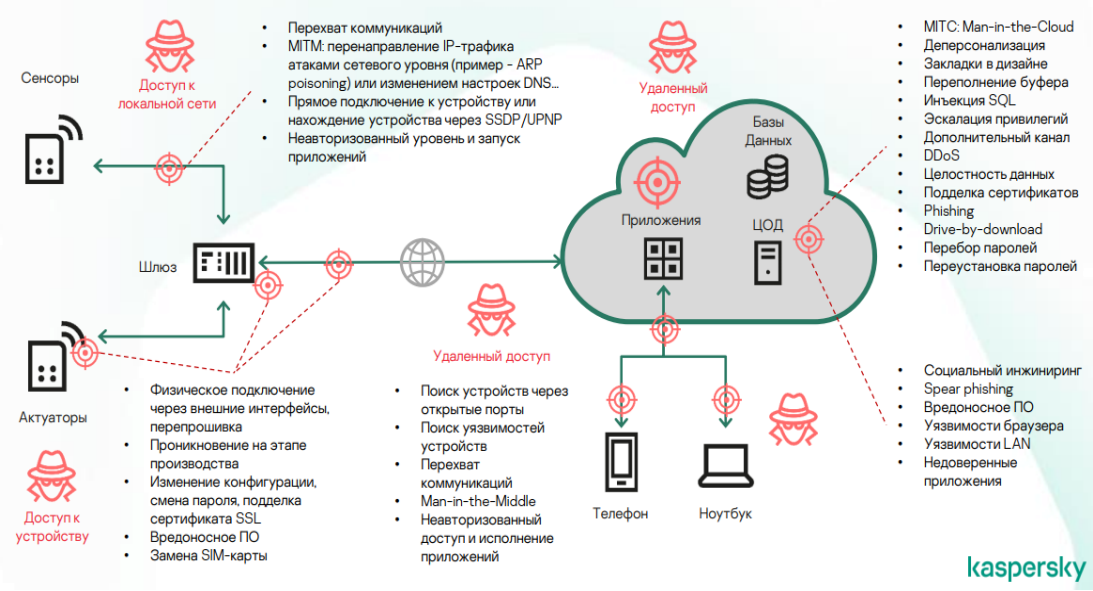

Рисунок 2

Особое внимание заслуживают атаки на инфраструктуру интернета вещей (рис. 2) [7]. Большое количество подключенных устройств с низким уровнем защиты создает уязвимые точки в корпоративных и домашних сетях. Имитационные эксперименты позволяют исследовать сценарии захвата устройств интернета вещей для формирования ботнетов или проникновения в защищенные сети. Захваченные устройства могут использоваться для распространения вредоносного программного обеспечения (ПО), сбора конфиденциальных данных или участия в *DDoS*-атаках. Результаты моделирования помогают тестировать защитные решения на уровне устройств, шлюзов и управляющих систем, включая методы шифрования и аутентификации устройств.

Роль нейросетей в имитационном моделировании

Современные нейросетевые технологии представляют собой мощный инструмент для имитационного моделирования в сфере защиты информации. Их основное преимущество заключается в способности обучаться на больших объемах данных, выявлять сложные паттерны и адаптироваться к новым угрозам. Инновационность нейросетей позволяет значительно повысить реалистичность моделирования атак и эффективность разрабатываемых систем защиты.

Ключевым направлением применения нейросетей является прогнозирование поведения атакующих и анализ сложных паттернов атак. В отличие от традиционных алгоритмов, которые часто используют жестко заданные правила, нейросети способны выявлять скрытые закономерности в данных и адаптироваться к ранее неизвестным угрозам.

Особого внимания заслуживают генеративно-состязательные сети (*Generative Adversarial Networks – GAN*). Эти нейросети состоят из двух компонентов – генератора и дискриминатора, которые соревнуются друг с другом: генератор создает синтетические данные, а дискриминатор пытается отличить их от реальных. В контексте имитационного моделирования *GAN* используются для создания реалистичных симуляций атакующих, что позволяет:

- тестировать системы безопасности на новых, ранее не встречавшихся сценариях атак;
- генерировать аномальные данные для обучения моделей обнаружения вторжений.

Используя данные реальных *DDoS*-атак, генеративно-состязательные сети могут создавать новый трафик, имитирующий атаки с различной степенью интенсивности и структурой пакетов. Такой подход позволяет тестировать системы защиты в условиях, максимально приближенных к реальным, а также выявлять их слабые места.

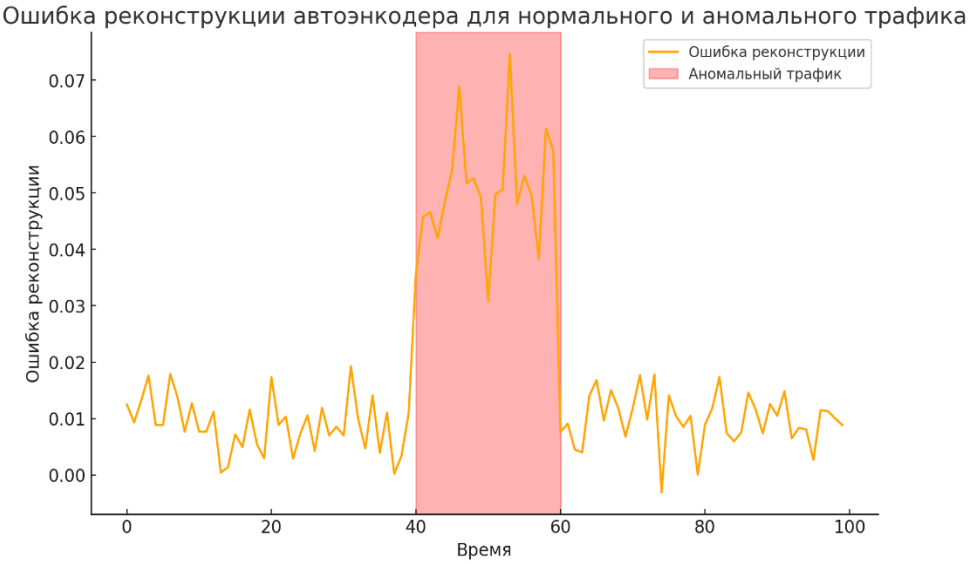

Рисунок 3

Примерами нейросетевых решений является детекция аномалий в трафике с использованием автоэнкодеров. Автоэнкодеры представляют собой нейросетевые модели, которые обучаются на нормальных данных с целью их реконструкции. Поскольку модель формирует представление о типичном поведении системы, любое отклонение от нормы приводит к значительному увеличению ошибки

реконструкции. В контексте сетевой безопасности это означает, что при появлении аномального трафика (например, при *DDoS*-атаке или попытке вторжения) автоэнкодер фиксирует высокие ошибки реконструкции. Это позволяет оперативно детектировать подозрительные события и передавать сигнал системам реагирования.

На рис. 3 представлен график изменения ошибки реконструкции автоэнкодера для нормального и аномального трафика. Временной промежуток аномалий выделен красной областью, где отчетливо видно значительное отклонение ошибок по сравнению с фоновыми значениями.

Другим примером использования нейросетей является классификация угроз с применением глубокого обучения. Глубокие нейросети, такие как сверточные нейронные сети (*Convolutional Neural Networks – CNN*) и рекуррентные нейронные сети (*Recurrent Neural Networks – RNN*), успешно применяются для анализа сетевого трафика и классификации угроз. *CNN* используются для обработки структурированных данных и выявления закономерностей в пакетах трафика, тогда как *RNN* эффективны для анализа временных последовательностей, позволяя детектировать аномальные изменения в поведении системы.

Преимущества симулятивного подхода для кибербезопасности

Симуляционное моделирование занимает ключевое место в процессе апробации и совершенствования систем защиты информации. Его использование дает возможность разворачивать механизмы обороны в условиях, максимально близких к реальным сценариям кибератак. При этом важную роль играет не только повышение точности функционирования защитных алгоритмов, но и их способность корректно реагировать на неизвестные ранее угрозы.

Одним из наиболее существенных достоинств подобного метода является обучение моделей глубокого обучения на данных, имитирующих настоящие кибератаки. Если традиционные способы анализа ограничиваются статическими наборами, то симуляции помогают генерировать динамические и более сложные сценарии, где могут присутствовать нетипичные аномалии и нестандартные паттерны, типичные для современных кибератак.

В качестве иллюстрации можно привести нейросетевые модели, предназначенные для распознавания аномалий в сетевом трафике. При обучении на данных, полученных в ходе моделирования *DDoS*-атак или попыток взлома, такие модели демонстрируют высокую точность при определении подозрительной активности. Более того, они способны выявлять опасные действия даже в том случае, если злоумышленники меняют свой подход или пробуют новые способы обхода защиты.

Таблица 2.

Критерий	**Статические данные**	**Симулятивные данные**
Адаптивность к новым угрозам	Ограничена	Высокая
Уровень реалистичности	Средний	Максимальный
Гибкость и масштабируемость	Низкая	Высокая
Затраты на сбор и обновление данных	Высокие	Относительно низкие

Результаты, отраженные в табл. 2, указывают на то, что симулятивные данные формируют у нейросетевых моделей большую адаптивность и

реалистичность. Это значит, что подобные алгоритмы лучше распознают сложные векторы атак, в том числе ранее не встречавшиеся.

Симулятивный подход дает возможность апробировать новые средства и методы киберзащиты в специально созданной тестовой среде, не подвергая действующую инфраструктуру рискам. Так, имитация дает детальное понимание того, как система реагирует на различные атаки и насколько эффективно работают уже внедренные средства защиты.

К примеру, при моделировании фишинговых кампаний можно проверить, насколько качественно алгоритмы фильтрации почты определяют потенциально опасные письма. В ходе эксперимента формируется множество вариантов фишинговых сообщений, что позволяет протестировать систему в условиях, приближенных к реальным. Аналогичным образом симуляции применяются при проверке решений для интернета вещей, когда злоумышленники стремятся взять под контроль «умные» устройства или изменить их данные. Здесь можно выявить слабые места как в самих гаджетах, так и в облачной инфраструктуре, которая отвечает за их работу.

По мере усложнения самих кибератак и появления новых уязвимостей системы защиты должны постоянно приспосабливаться к изменчивому ландшафту угроз. Благодаря симуляциям можно смоделировать сценарии, о которых пока нет статистических данных, и заранее выработать механизмы противодействия. Использование генеративно-состязательных сетей (*GAN*) позволяет создавать такие сценарии, практически неизвестные на момент моделирования. Алгоритмы глубокого обучения, прошедшие подготовку на подобных кейсах, имеют все шансы оперативно обнаружить и остановить новую угрозу, предложив оптимальный план нейтрализации.

На рис. 4 представлен график количества обнаруженных аномалий нейросетевой моделью при обучении на симулированных данных. Красные точки представляют новые, ранее неизвестные паттерны атак, выявленные в процессе тестирования.

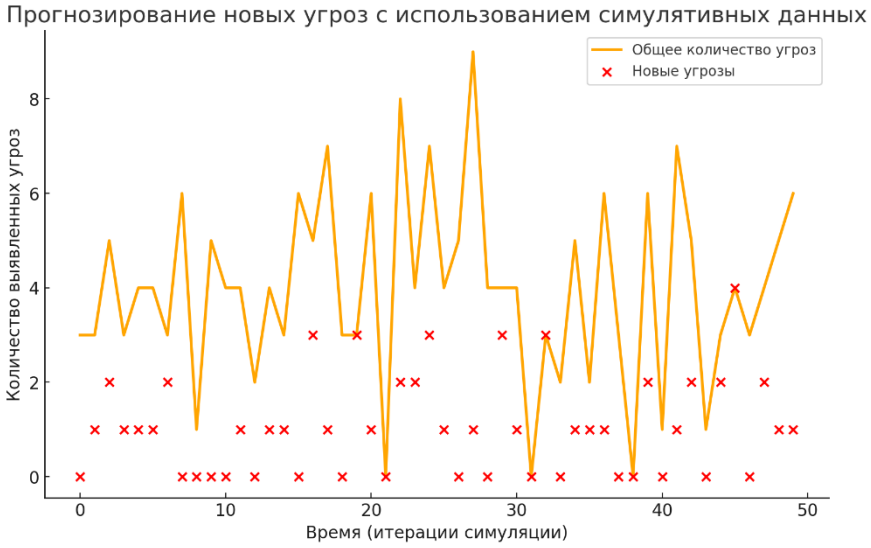

Рисунок 4

График на рис. 4 демонстрирует, как в процессе симуляции системы защиты фиксируют ранее неизвестные угрозы (обозначены красными точками). Это позволяет адаптировать алгоритмы к новым сценариям атак и повышать их эффективность.

Проблемы и вызовы симулятивного подхода в кибербезопасности

Одной из основных проблем симулятивного подхода в кибербезопасности является сложность построения моделей, что напрямую связано с необходимостью высококачественных данных. Нейросетевые алгоритмы требуют большого количества репрезентативной и чистой информации для обучения, однако данные о кибератаках часто оказываются неполными, зашумленными или неструктурированными. Особенно это касается новых и малоизученных угроз, таких как целевые атаки, для которых не существует исторических записей. В таких случаях возникают трудности в создании реалистичных симуляций, что снижает эффективность моделируемых сценариев для тестирования систем защиты.

Этическая сторона применения нейросетевых моделей также вызывает серьезные опасения. Генеративно-состязательные сети, которые успешно используются для создания реалистичных симуляций атак, имеют двойственную природу. Если эти технологии попадут в руки злоумышленников, они могут быть использованы для создания высокоточных атакующих инструментов. Например, *GAN* способны генерировать новые виды фишинговых писем, имитировать нормальный сетевой трафик или разрабатывать сложные методы обхода защитных систем. Это создает дополнительную угрозу и требует жесткого контроля над распространением таких технологий.

Помимо этого, симулятивное моделирование, особенно с использованием нейросетей, требует значительных вычислительных ресурсов. Высокая сложность расчетов и необходимость обработки больших объемов данных делают подобные решения крайне ресурсоемкими. Обучение моделей глубокого обучения, работающих с сетевыми данными или сложными паттернами атак, требует длительного времени и мощных вычислительных систем на базе графических процессоров (*Graphics Processing Unit – GPU*). При этом моделирование в реальном времени, которое необходимо для детекции и противодействия атакам, становится еще более трудозатратным, что усложняет его применение в масштабных инфраструктурах.

Дополнительные трудности возникают при создании реалистичных симуляций атак, особенно для новых и малоизвестных угроз. Стандартные методы моделирования часто ограничиваются упрощенными сценариями, которые не отражают всей сложности поведения атакующих. Современные подходы, такие как использование нейросетей для генерации аномального трафика или динамических сценариев атак, помогают решить эту проблему частично, но требуют тонкой настройки и значительных экспериментов. Например, гибридное моделирование, сочетающее статистические методы и нейросетевые модели, позволяет улучшить качество симуляций, однако такие эксперименты остаются сложными в реализации и масштабировании.

На фоне развития нейросетевых технологий наблюдается рост их применения как в системах защиты, так и в инструментах атак. По мере совершенствования нейросетевых методов эта тенденция будет только усиливаться, что видно из анализа данных за последние годы. Однако такая динамика требует разработки стратегий по минимизации рисков нецелевого использования технологий и повышению устойчивости систем защиты к новым методам атак.

График на рис. 5 демонстрирует рост внедрения нейросетевых технологий как в системах защиты, так и в инструментах злоумышленников. Параллельное развитие обоих направлений требует повышения мер контроля и этического использования подобных технологий.

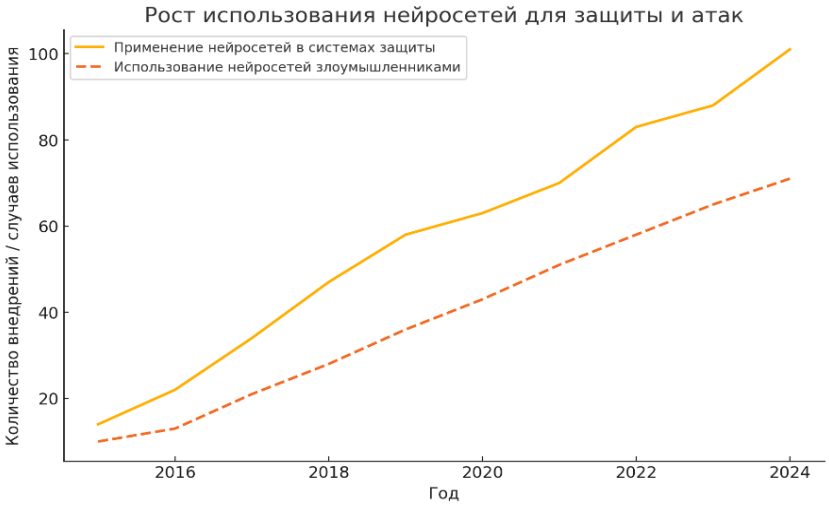

Рисунок 5

Заключение

Имитационное моделирование в сочетании с нейросетевыми технологиями является мощным инструментом для решения задач защиты информации в условиях постоянно усложняющегося ландшафта киберугроз. Благодаря своей способности воссоздавать сценарии атак и анализировать их последствия, этот подход позволяет не только тестировать существующие системы безопасности, но и разрабатывать новые, адаптивные механизмы защиты. Нейросети, применяемые в рамках имитационного моделирования, обеспечивают высокий уровень реалистичности симуляций, что особенно важно для прогнозирования новых угроз и тестирования систем в условиях ранее неизвестных атак.

Несмотря на очевидные преимущества, симулятивный подход сталкивается с рядом вызовов, таких как высокая ресурсоемкость, сложность создания реалистичных сценариев и этические аспекты использования технологий. Для преодоления этих проблем необходимы совместные усилия разработчиков, исследователей и специалистов по кибербезопасности. Особое внимание следует уделить развитию гибридных методов, которые объединяют статистические подходы и нейросетевые модели, а также созданию стандартов контроля за использованием технологий, таких как генеративно-состязательные сети (*GAN*).

С развитием технологий киберугроз и защитных решений неизбежно усиливается противостояние между злоумышленниками и разработчиками систем безопасности. В этих условиях успех будет зависеть от способности быстро адаптироваться к новым вызовам и внедрять инновационные решения. Имитационное моделирование с применением нейросетей остается одним из ключевых направлений для достижения этой цели, открывая возможности для создания интеллектуальных и устойчивых систем защиты.

Литература

1. Шаньгин В.Ф. «Информационная безопасность компьютерных систем и сетей». Учеб. пособие для сред. проф. образования. – М.: Форум, 2008. – 416 с.
2. Милославская Н.Г. «Управление рисками информационной безопасности». Учеб. пособие. – М.: Горячая линия – Телеком, 2012. – 130 с.
3. Мансуров Г.З. «Право цифровой безопасности». Учебник. – Москва: Директ-Медиа, 2022. – 148 с.
4. Лобова А. И., Вершинин Е.В., Федоров В.О. Обзор DDoS-атак на IoT устройства // Нацбезопасность, 2022. – № 1 (3).

5. Баженов А.С. Обзор DDoS атак на IoT устройства // Наука настоящего и будущего, 2019. – Т. 1. – С. 122-125.
6. Горев А.В. Интеллектуальный анализ DDoS-атак ботнета на IoT устройства при помощи Sap Analytics Cloud // Безопасность информационного пространства. Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2021. – С. 10-14.
7. Обзор Kaspersky IoT Secure Gateway, шлюза для построения безопасных систем интернета вещей Источник: https://www.anti-malware.ru/reviews/Kaspersky-IoT-Secure-Gateway // anti-malware.ru URL: anti-malware.ru/reviews/Kaspersky-IoT-Secure-Gateway (дата обращения: 10.12.2024).