УДК 004.94

Зубченко Константин Вадимович,
магистрант,
2 курс, факультет «информационных систем и безопасности»,
ФГАОУ ВО «РГГУ – Российский государственный гуманитарный университет»

Россия, г. Москва

ПРИМЕНЕНИЕ АГЕНТНОГО ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ ПРОГНОЗИРОВАНИЯ ПОСЛЕДСТВИЙ КИБЕРАТАК НА ИНФРАСТРУКТУРУ

В статье представлены результаты эксперимента по применению агентного имитационного моделирования для прогнозирования влияния кибератак на бизнес-процессы в инфраструктуре. Были проанализированы текущие попытки прогнозирования кибератак в сфере информационной безопасности. Также была описана схема разработанного метода и описание инструментов для проведения имитации. Особое внимание уделяется результатам проведения эксперимента с представлением вывода разработанной программы, а также необходимости развития прикладного подхода для прогнозирования последствий кибератак на инфраструктуру предприятий.

Ключевые слова: *имитационное моделирование, агентное моделирование, информационная безопасность, кибератаки, прогнозирование последствий, оценка рисков.*

Zubchenko Konstantin Vadomivich,
master's candidate,
2nd year, Faculty of "Information Systems and Security",
RSUH – Russian State University for the Humanitie,

Russia, Moscow.

APPLICATION OF AGENT-BASED SIMULATION MODELLING TO PREDICT THE CONSEQUENCES OF CYBER-ATTACKS ON INFRASTRUCTURE

The article presents the results of an experiment on the use of agent-based simulation modeling to predict the impact of cyberattacks on business processes in the infrastructure. Current attempts to predict cyberattacks in the field of information security were analyzed. The scheme of the developed method and the description of the tools for conducting the simulation were also described. Particular attention is paid to the results of the experiment with the presentation of the output of the developed program, as well as the need to develop an applied approach to predicting the consequences of cyber attacks on enterprise infrastructure.

Key words: *simulation modeling, agent modeling, information security, cyber attacks, forecasting consequences, risk.*

Введение. В сфере информационной безопасности (ИБ) на данный момент существует ярко выраженный тренд на модели безопасности с нулевым доверием[1]. Во многом этот тренд состоит в оценке рисков и прогнозировании кибератак, поскольку любой компонент информационной системы считается подверженным кибератакам. Отсюда появляются более новые технические средства и инструменты для осуществления проактивной защиты: инструменты BAS, сканеры уязвимостей, средства инвентаризации активов и т.д. Стоит отметить, что происходит развитие, в том числе, и методологических, теоретических, алгоритмических аспектов информационной безопасности. Например, одним из популярных направлений можно считать использование имитационного моделирования. Достаточно большое количество компаний в сфере информационной безопасности разрабатывают и используют цифровые двойники и моделирование кибератак для проведения киберучений с целью проверки компетентности специалистов, повышения их осведомленности, а также повышения защищенности инфраструктуры[2]. Однако, в используемых

платформах достаточно редко применяется моделирование бизнес-процессов в инфраструктуре. Это связано с тем, что в научном сообществе отсутствует консенсус касаемо термина «киберполигон», а также его непосредственного прикладного значения. Кроме того, отсутствует классификация «киберполигонов». Такая ситуация возникает во многом из-за слишком разнопланового применения этой технологии[3]. Все вышесказанное приводит к тому, что в существующих на российском рынке решениях отсутствует единый подход к анализу и тестированию конкретных навыков специалистов, а также к оценке результатов киберучений. При этом особо остро стоит проблема прогнозирования последствий действий злоумышленников для инфраструктуры компании. Далее будут рассмотрены текущие достижения и примеры подходов, используемых для решения этой проблемы.

Авторы статьи [4] осуществили попытку использовать вероятностное прогнозирование, а конкретно метод интервального прогнозирования, для прогнозирования интенсивности кибератак. В результате была предложена схема проактивного противодействия кибератакам с учетом результатов интервального прогнозирования. Однако, как было верно отмечено в статье, исследований на тему прогнозирования кибератак чрезвычайно мало, в силу сложности теоретического прогнозирования такого стохастического явления, как атака на информационную систему. Кроме того, в качестве исходной подборке с данными была использована выборка за 2013 год, которая в корне не соответствует текущему ландшафту угроз. Автор статьи [5] указывает, что существующие труды либо не учитывают специфику ИБ, либо являются теоретическими выкладками, не прошедшими практическую проверку на актуальных данных. Стоит отметить, что некоторыми авторами предлагаются практико-направленные подходы к прогнозированию кибератак[6]. Таким образом, стала очевидной необходимость разработки качественного подхода для прогнозирования последствий кибератак, обязательно имеющего практическое применение, а также подтвержденного на реальных данных. В качестве основного инструмента для достижения цели было выбрано агентное имитационное моделирование.

Агентное имитационное моделирование. Суть агентного моделирования заключается в независимой природе поведения агентов[7]. Для реализации этого типа моделирования на практике был использован фреймворк с открытым исходным кодом Ghosts[8]. Его принцип работы заключается в использовании заранее заданных сценариев поведения, которые через сервер-оркестратор передаются на клиентские устройства. В силу особенностей реализации, данный инструмент позволяет имитировать практически любую активность сотрудников в инфраструктуре: от обычного открытия ссылки в браузере, до использования узкоспециализированного ПО. Кроме того, оркестратор позволяет собирать всю информацию о состоянии агентов, а также о статусе выполнения ими своих задач. Все действия выполняются агентами недетерминированно, т.е. в заданный промежуток, но не в фиксированный момент времени. Все агенты заранее были размещены на устройства в виртуальной инфраструктуре, после чего произведен запуск эксперимента.

Проведение тестовых кибератак. Данная часть эксперимента была реализована с использованием фреймворка Mitre Caldera[9]. Он позволяет проводить кибератаки на заданную инфраструктуру. Основная идея заключается в бесконечном проведении одних и тех же кибератак, которые генерируются из доступных техник и тактик, по принципу «все со всеми». Детали реализации и его конкретное применение не будут рассматриваться в рамках данной статьи, поскольку являются лишь маркером для проявления основного рассматриваемого явления. Стоит отметить, что кибератаки выбирались целенаправленно с неизбежным влиянием на инфраструктуру и бизнес-процессы в ней, чтобы однозначно определить способность агентного имитационного моделирования установить последствия их проведения.

Прогнозирование последствий кибератак. Таким образом, схема прогнозирования кибератак может быть представлена следующим образом:

1. Производится установка агентов на конечные устройства в инфраструктуре, заранее задается перечень действий для агентов с последующим запуском эксперимента.
2. На эту же инфраструктуру проводится набор кибератак. Предполагается, что для повышения эффективности прогноза конкретные цепочки кибератак должны генерироваться случайным образом. Так будет соблюдена недетерминированность всего эксперимента. Однако, варианты реализации могут быть изменены в угоду целям и задачам испытания.
3. В случае реального влияния кибератаки на бизнес-процессы рассматриваемой инфраструктуры, агент не сможет выполнить хотя бы одну из своих задач, что является теоретическим последствием конкретной кибератаки или их совокупности. Эта информация поступает из оркестратора при соответствующем запросе (Рисунок 1). На представленном скриншоте видно, что одно из действий не было выполнено.


```
{
  "trackableId": "track-98765",
  "agentId": "agent-001",
  "machineName": "WORKSTATION-01",
  "currentStatus": "active",
  "timeline": [
    {
      "activityId": "act-123",
      "activityType": "fileDownload",
      "fileName": "report.pdf",
      "fileSize": "2.4 MB",
      "status": "completed",
      "utctimeon": "2025-05-20T14:30:45Z",
      "utctimeoff": "2025-05-20T14:31:10Z",
      "durationSeconds": 25,
      "details": {
        "sourceUrl": "http://intranet/files/report.pdf",
        "destinationPath": "C:\\Downloads\\report.pdf",
        "integrityCheck": "sha256:abc123..."
      }
    },
    {
      "activityId": "act-124",
      "activityType": "processExecution",
      "processName": "powershell.exe",
      "status": "failed",
      "utctimeon": "2025-05-20T14:32:00Z",
      "utctimeoff": "2025-05-20T14:32:05Z",
      "durationSeconds": 5,
      "details": {
        "commandLine": "-ExecutionPolicy Bypass -File script.ps1",
        "exitCode": 1,
        "error": "Access denied"
      }
    }
  ],
  "metadata": {
    "created": "2025-05-20T12:00:00Z",
    "lastUpdated": "2025-05-20T14:32:05Z",
    "trackableType": "fileOperation",
    "priority": "high",
    "tags": ["financial", "sensitive"]
  },
  "statusHistory": [
    {
      "status": "pending",
      "timestamp": "2025-05-20T12:00:00Z"
    },
    {
      "status": "inProgress",
      "timestamp": "2025-05-20T14:30:45Z"
    },
    {
      "status": "active",
      "timestamp": "2025-05-20T14:31:10Z"
```


Рисунок 1 – Результат выполнения действий агентом

Критически важно учитывать реальную причину невыполнения агентом своей задачи, поскольку ошибки могут возникать и по независящим от тестовых кибератак причинам. Чтобы избежать такого сценария, было заранее проведено тестирование поведения агентов без проведения атак на инфраструктуру. В ходе этого эксперимента все агенты выполняли свои задачи без ошибок. Этот факт позволяет с высокой долей уверенности заключить, что обнаруженные ошибки в течение реального эксперимента вызваны именно влиянием проведенных кибератак, а значит являются искомыми последствиями. Весь цикл эксперимента заключается в последовательном псевдо-случайном проведении кибератак бесконечное количество раз, до того момента, пока он не будет остановлен вручную. Поскольку прогноз является вероятностной величиной, в разработанной системе происходит подсчет количества зафиксированных последствий и делится на общее количество идентичных запущенных цепочек атак. Результатом проведения полных 5 циклов кибератак (т.е. все доступные цепочки запустились строго по 5 раз) стал следующий вывод разработанной программы (Рисунок 2)

```
Возможная цепочка:
T1018 -> T1018 -> T1135 -> T1021.002 -> T1047
Вероятность успешной атаки: 5/5
Вероятность влияния атаки: 0/5
Влияние:
Отсутствует


Возможная цепочка:
T1074.001 -> T1005 -> T1074.001 -> T1560.001 -> T1041
Вероятность успешной атаки: 4/5
Вероятность влияния атаки: 1/5
Влияние:
WORKSTATION06: [{"action":"act-128"}]
```

Рисунок 2 – Результат выполнения разработанной экспериментальной программы

Стоит пояснить результаты эксперимента. Происходит вывод случайно сгенерированной цепочки атак по идентификаторам ее техник в той

последовательности, в которой эти этапы проводились. Затем выводится вероятность успешной атаки (M), которая вычисляется по формуле:

$$M = \frac{S}{P}$$

Где P – частота появления конкретно этой цепочки за все циклы, S – частота успешного прохождения конкретно этой цепочки за все циклы

Вероятность влияния атаки (F) вычисляется по следующей формуле:

$$F = \frac{A}{N}$$

Где A – количество циклов, в которых хотя бы одно из действий агента в ходе имитационного моделирования было не выполнено, N – общее количество циклов.

Затем выводится список идентификаторов действий агента, которые были затронуты.

Заключение. В ходе проведения эксперимента была реализована программа, которая использует результаты агентного имитационного моделирования и фреймворк Mitre Caldera для определения последствий кибератак на инфраструктуру. У предложенной реализации есть множество недочетов, которые заключаются в упрощенной валидации последствий, слишком трудоемком составлении действий агентов, а также в достаточно долгом достижении сколько-нибудь эффективных данных. Тем не менее, по мнению автора, результаты эксперимента подтверждают гипотезу о том, что имитационное агентное моделирование может быть использовано для прогнозирования последствий кибератак на инфраструктуру, а также для оценки рисков. Более того, реализованная программа показывает, что простейшим прикладным подходом можно добиться реальных результатов и обеспечить общее представление о защищенности инфраструктуры и ее бизнес-процессов.

Однако, данный метод должен быть исследован и значительно усложнен дополнительными валидациями и теоретической базой для реального применения в компаниях.

Использованные источники:

1. Соломинский Алексей Владимирович, Железин Виталий Александрович, Миргородский Артём Дмитриевич, Краснобаев Сергей Валерьевич, Колотилина Наталья Михайловна АКТУАЛЬНЫЕ ТЕНДЕНЦИИ НА РЫНКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ // Вестник науки и образования. 2023. №8 (139). URL: https://cyberleninka.ru/article/n/aktualnye-tendentsii-na-rynke-informatsionnoy-bezopasnosti (дата обращения: 05.07.2025).

2. Солар: 85% российских компаний планируют киберучения для защиты инфраструктуры в 2025 году // Digital Russia URL: https://d-russia.ru/solar-85-rossijskih-kompanij-planirujut-kiberuchenija-dlja-zashhity-infrastruktury-v-2025-godu.html (дата обращения: 05.07.2025)

3. Прохоров, А. И. Киберполигон как современный инструмент обеспечения информационной безопасности / А. И. Прохоров // Информатизация в цифровой экономике. – 2023. – Т. 4, № 4. – С. 363-378. – DOI 10.18334/ide.4.4.119301 (дата обращения: 05.07.2025)

4. Краковский Юрий Мечеславович, Курчинский Борис Валентинович, Лузгин Александр Николаевич Интервальное прогнозирование интенсивности кибератак на объекты критической информационной инфраструктуры // Доклады ТУСУР. 2018. №1. URL: https://cyberleninka.ru/article/n/intervalnoe-prognozirovanie-intensivnosti-kiberatak-na-obekty-kriticheskoy-informatsionnoy-infrastruktury (дата обращения: 05.07.2025).

5. Можно ли предсказать кибератаки? // Бизнес без опасности URL: https://lukatsky.ru/threats/mozhno-li-predskazyvat-kiberataki.html (дата обращения: 06.07.2025)

6. Зубченко К.В. Обзор возможности применения многоподходного имитационного моделирования в области информационной безопасности // Наукосфера. 2025. №5 (2). С. 7-12 (дата обращения: 06.07.2025)

7. Лебедюк Эдуард Андреевич Агентное моделирование: состояние и перспективы // Вестник РЭА им. Г. В. Плеханова. 2017. №6 (96). URL: https://cyberleninka.ru/article/n/agentnoe-modelirovanie-sostoyanie-i-perspektivy (дата обращения: 06.07.2025).

8. Модуль имитации активности пользователей // Ghosts Framework URL: https://cmu-sei.github.io/GHOSTS/ (дата обращения: 06.07.2025).

9. Фреймворк для проведения кибератак // Mitre Caldera URL: https://caldera.mitre.org/ (дата обращения: 06.07.2025)

Информация о себе: Зубченко К.В., zkonst12@gmail.com