УДК 004.056.2 Вестник УрФО № 4(50) / 2023, с. 70–76

**Частикова В.А., Козачёк К.В.**

DOI: 10.14529/secur230407

# *ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ПЛАТФОРМЕ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ КАК ЭФФЕКТИВНОЕ СРЕДСТВО УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ*[1]

*Платформы реагирования на инциденты помогают администраторам информационной безопасности управлять инцидентами. Несмотря на преимущества, которые несет автоматизация, многие компании всё ещё продолжают предоставлять IRP как платформу, основной функционал которой направлен на ведение документации и не работает без Threat Intelligence.*

*В данной статье рассмотрена типовая структура платформ реагирования на инциденты. Описаны плюсы и варианты использования машинного обучения, тонкости его применения в IRP. Предлагается вариант автоматизации реагирования посредством использования нейронных сетей. Приведены архитектура нейронной сети для определения алгоритма действий специалиста информационной безопасности L2, описаны эксперименты с архитектурами нейросетей и набором входных параметров на ограниченном датасете. Описана обучающая выборка, особенности её сбора, приведены основные категории входных параметров. Рассматриваются требования к датасетам. Приводится рекомендации по автоматизации реагирования на инциденты.*

***Ключевые слова:*** *информационная безопасность, платформа реагирования на инциденты, нейронная сеть, машинное обучение, датасет, предобработка данных.*

[1] Работа выполнена в рамках гранта ИБ МТУСИ № 04/22-д «Методология построения систем анализа инцидентов информационной безопасности для распределенных информационных систем».

# *USING NEURAL NETWORKS IN AN INCIDENT RESPONSE PLATFORM AS AN EFFECTIVE MEANS OF CYBERSECURITY MANAGEMENT*

*Incident response platforms help information security administrators manage incidents. Despite the benefits that automation brings, many companies still continue to provide IRP as a platform whose main functionality is aimed at maintaining documentation, or does not work without Threat Intelligence.*

*This article discusses the typical structure of incident response platforms. The advantages and use cases of machine learning and the subtleties of its application in IRP are described. An option is proposed to automate the response through the use of a neural network. The architecture of the neural network for determining the algorithm of actions of the L2 information security specialist is presented, experiments with the architecture of the neural network and a set of input parameters are described. Requirements for datasets are considered. The training sample, the features of its collection are described, and the main categories of input parameters are given. Recommendations for automating incident response are provided.*

***Keywords:*** *information security, incident response platform, neural network, machine learning, dataset, data preprocessing.*

**Введение**

Платформы реагирования на инциденты (Incident Response Platform, IRP) — это класс платформ, позволяющих обеспечить управление реагированием на компьютерные инциденты. IRP занимает значимое место в системе обеспечения информационной безопасности. Она позволяет упростить работу аналитиков L1 и L2. [1,2]

За обнаружение инцидента отвечает система управления информационной безопасностью и событиями безопасности (SIEM), а IRP отвечает на реагирование на инцидент: специалисту информационной безопасности (ИБ) из сием приходят уведомления об инциденте. IRP помогает в выборе алгоритма действия для устранения, определение приоритетов событий и составления документации по событиям. Ввиду увеличения числа атак на информационные инфраструктуры [1, 2], растет и число инцидентов. Часто, время на реагирование должно занимать от 15 минут до часу для критичных инцидентов [2, 5] и от 2 часов до 8 для большинства остальных [2, 5]. Таким образом даже незначительные улучшения в сторону автоматизации очень важны. Если своевременно не закрыть инцидент, может быть нанесен ущерб всей инфраструктуре предприятия [5,7]. Искусственный интеллект (ИИ) также снижает утомляемость и человеческие ошибки. Мониторинг сетей и анализ огромных объемов данных для обнаружения угроз — утомительная работа, которая может привести к ошибкам и пропущенным инцидентам.

Несмотря на преимущества, которые несет автоматизация, многие компании всё ещё продолжают предоставлять IRP как платформу (продукт) для выполнения собственных скриптов по реагированию на инциденты, а основной функционал направлен на ведение, и категорирование политик, плейбуков и прочей документации (Innostage IRP) [5], либо они не работают без ТИ (TheHive) [6,7].

Основные преимущества использования платформ реагирования на инциденты:

– увеличение точности обнаружения и мониторинга инцидентов;

– возможность автоматической координации действий;

– оптимизация времени реагирования и сокращение потенциальных ущербов;

– централизованное управление процессом реагирования;

– автоматизация задач и максимизация эффективности команды по реагированию.

В реагировании на инциденты и работе IRP выделяют следующие этапы:

1. Подготовка, создание плейбуков/сценариев реагирования.

2. Проверка, является ли событие, пришедшее из SIEM инцидентом.

3. Определение приоритета инцидента.

4. Сдерживание, локализация инцидента.

5. Устранение инцидента.

6. Восстановление системы/инфраструктуры.

7. Составление отчетов и рекомендаций, по результатам расследования.

1. На данном этапе определяются риски IT-инфраструктуры, создаются политики безопасности для пользователей, прописываются сценарии действия специалистов ИБ в случае реализации той или иной угрозы.

2. Из событий, собираемых SIEM, выбираются нежелательные и передаются IRP, однако, иногда случаются ложноположительные срабатывания, потому необходимо убедиться, что событие является инцидентом.

3. Определяется уровень значимости/приоритет инцидентов. Важный этап, из-за ошибки на котором дальнейшая работа может быть выполнена над идентифицированной угрозой неверно, что повлечет несвоевременное закрытие события.

4. Сдерживание, локализация инцидента – этап, на котором аналитик ИБ определяет, что именно произошло и какие действия необходимо выполнить. На этом этапе выполняются шаги по предотвращению дальнейшего разрастания проблемы.

5. Непосредственно устранение инцидента в соответствии со сценариями реагирования.

6. Восстановление инфраструктуры, пострадавшей от реализации угрозы.

7. Анализ действий аналитиков ИБ/группы реагирования на инциденты, составление новых плейбуков, политик безопасности и т.п.

Некоторые выделяют детектирование инцидентов как задачу IRP, хотя на практике за это отвечает SIEM, а платформа реагирования лишь проверяет корректно ли были выбраны нежелательные события или нет. [4, 7].

Хотя машинное обучение можно применять на разных этапах обнаружения и закрытия инцидентов [3, 6, 10], в данной статье рассматривается применение нейронных сетей на наиболее значимых для IRP 4 и 5 этапах – непосредственно на реагировании.

Предпосылками для использования ИИ является увеличившееся количество инцидентов, уменьшение времени реагирования на них, неочевидная, неалгоритмическая задача определения алгоритма действий в той или иной ситуации, а также огромные объемы данных о событиях, с которыми хорошо справляются нейронные сети. Однако информацию об инцидентах трудно найти в открытом доступе, т.к. её бы могли использовать злоумышленники.

По этой причине для обучения нейронной сети и тестирования был собран тестовый датасет из 23 образцов, основанный на правилах корреляции SIEM из открытых источников [9]. На рис. 1 приведен фрагмент собранного набора данных.

Так выглядят и данные, подгружаемые из SIEM в IRP. На основании их, а также плейбуков/сценариев реагирования, специалист выбирает алгоритмы действий, необходимых для закрытия инцидента.

| Incident Key | Date | Severity | Incident Name | Src IP | Src Port | Src Name | Dst IP | Dst Port | Dst Name | User ID | User Name | File Path | File Name | Command Line | Object Name | Реакция |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 17.10.2023, 10:13 | Low | Попытка перебора паролей с одного источника | 24.246.33.144 | 5256 | None | 10.10.125.135 | 22 | HOST01 | None | Alice Bob Ewa root user admin administrator | None | None | None | None | Закрытие порта |
| 2 | 17.10.2023, 10:15 | High | Успешная попытка перебора паролей на хосте | 24.246.33.144 | 5256 | None | 10.10.125.135 | 22 | HOST01 | None | administrator | None | None | None | None | Блокировка УЗ |
| 3 | 17.10.2023, 10:15 | High | Создание привилегированного аккаунта пользоват... | None | None | None | 10.10.125.7 | None | HOST-DB | 1000 | root | None | None | None | adm_db | Отправка письма пользователю |
| 4 | 17.10.2023, 10:23 | Medium | Создание локального аккаунта учетной записи н... | None | None | None | 10.10.125.64 | None | ZABBIX | 0 | ivanov_zp | None | None | None | administrator | Блокировка УЗ |
| 5 | 17.10.2023, 10:37 | High | Обнаружение модификации файлов при загрузке си... | None | None | None | 10.10.18.3 | None | HOST34 | 0 | root | /boot/ | link | None | link | Запуск АВ |

Рис. 1. Фрагмент датасета

На основании этих данных можно обучить и нейронную сеть. После обнаружения инцидента ИИ может помочь определить серьезность, масштаб, первопричину и необходимые действия гораздо быстрее, чем люди. ИИ может идентифицировать инцидент за считанные минуты, а не за часы или дни, которые могут потребоваться специалистам, чтобы обнаружить его. Благодаря ИИ, дополняющему работу аналитиков, время реагирования может быть значительно сокращено. Для каждого инцидента существует время реакции на него (время закрытия инцидента). Аналитики относительно хуже работают ночью и могут не пропускать множественные инциденты [1]. IRP может решить проблему недостаточной квалификации и способствует повышению качества реагирования и экономии денег. [1]

Набор данных был расширен до 96 элементов, путем зашумления и создания данных по образцу. В качестве входных данных выбраны дата, время, уровень приоритета, имя (краткое описание) инцидента, IP и порт источника и пункта назначения, имя пользователя и т.д. В качестве выходных данных указаны реакции: действия специалиста ИБ, которые были разделены на 3 группы: блокировка учетной записи, запуск антивирусного программного обеспечения (ПО) и в остальных случаях – отправка письма пользователю – администратору ИБ. Столь ограниченное количество реакций обусловлено небольшим набором данных, при масштабировании количество реакций может быть увеличено.

При внедрении такая система является рекомендательной: автоматически можно запустить антивирусное ПО, окончательное решение о блокировке пользователей принимает аналитик ИБ. Письмо администратору отправляется в неочевидных случаях.

Далее данные были предобработаны:

1. IP источника и назначения были разделены на частный и общий, таким образом мы сократили мерность данных критериев, увеличив их значимость.

2. User ID разделен по критерию: «является ли администратором или нет», при этом для датасета из тысяч данных было бы потеряно множество важных признаков, но на небольшом наборе это позволило сократить мерность до двух, сильно увеличив значимость.

3. Аналогично был разбит столбец «Command Line» на несколько наиболее значимых групп.

4. Уровень приоритета, порт источника были преобразованы методом get_dummies (one-hot-encoding).

5. Краткое описание инцидента было представлено в виде мешка слов (BOW), так как данных немного, разреженность такой кодировки будет незначительной, однако при масштабировании рекомендуется переходить на более гибкие методы обработки естественного языка, например, такие, как архитектура «Трансформер».

Таким образом из 15 входных параметров были получены 65.

Так как решалась задача классификации, тестовый датасет невелик, а в реагировании на инциденты важна скорость, тестировались полносвязные сети прямого распространения с добавлением слоев Dropout для уменьшения вероятности «заучивания» результатов.

Лучшие результаты показала нейронная сеть со следующей архитектурой, код построения такой НС приведен на рис. 2:

– 65 нейронов на входном слое;

– 24 нейрона на первом промежуточном слое;

– 6 нейронов на втором промежуточном слое;

– 3 выходных нейрона.

```
model01 = Sequential()
model01.add(Dense(j, input_dim=65, activation="sigmoid"))
model01.add(Dropout(0.25))
model01.add(BatchNormalization())

model01.add(Dense(6, activation="sigmoid"))
model01.add(Dropout(0.25))
model01.add(BatchNormalization())
model01.add(Dense(3, activation='sigmoid'))
```

Рис. 2. Код построения нейронной сети

При обучении использовался метод K-кратной перекрёстной проверки для «увеличения» обучающих данных. График точности обучения такой сети представлен на рис. 3.

Время обучения на 10 эпохах составляет около 2 секунд. Такое количество эпох не является необходимым, и в отдельных случаях результаты на большем или меньшем количестве были выше.

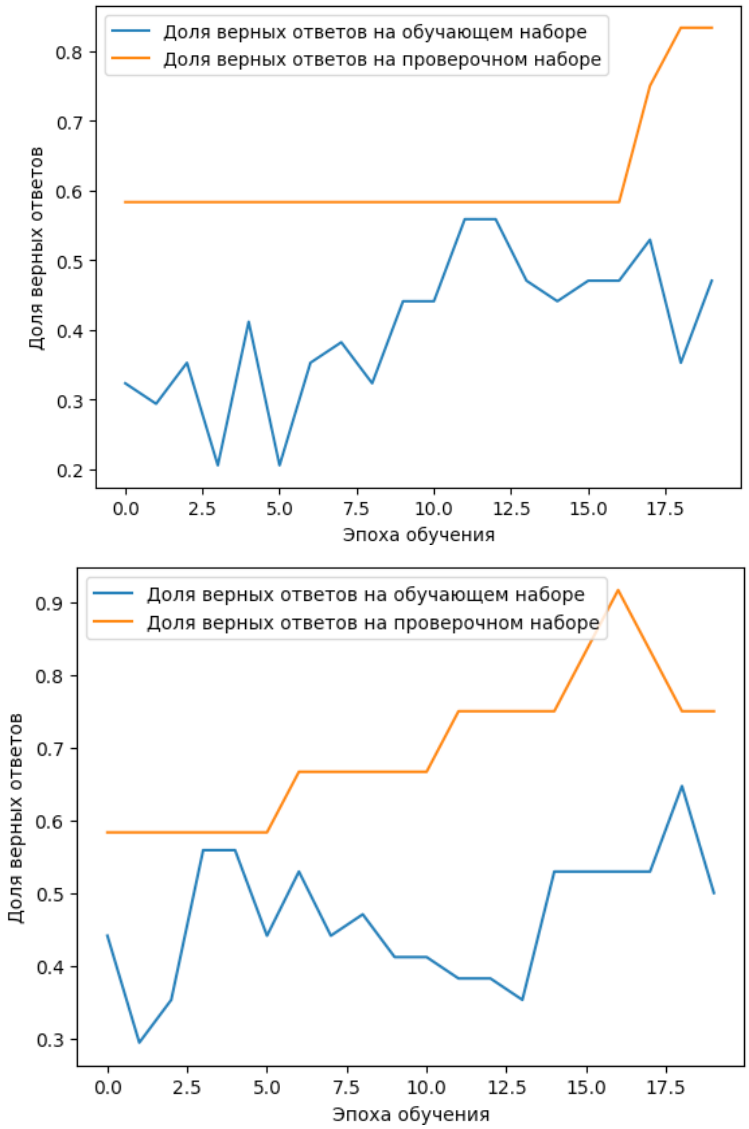


Рис. 3. График точности обучения НС в зависимости от эпохи

Так как параметры НС инициализируются случайным образом, каждая из них была запущена 50 раз для определения статистической точности. Наиболее значимые параметры обучения НС для IRP указаны в табл. 1.

Таким образом, на небольшом объеме данных приоритетное значение имеют правильно выбранные параметры обучения, а не архитектура сети, а избыточно выбранные параметры, наоборот, ухудшают точность (в некоторых случаях это можно отнести за счёт погрешности). При увеличении числа записей точность нейросетей, работающих на основе текста, немного повышается, тогда как эффективность прочих параметров растет значительно.

На итоговом датасете из 96 элементов тестировались сети с 65 параметрами на входе НС. Так как решалась задача множественной классификации, то 90 и даже 80% верных срабатываний являются значимыми и позволяют упростить работу аналитика ИБ L1/L2. Очевидно, что ввиду ограниченного набора данных результаты работы НС невысоки, таким

*Таблица 1*

**Статистика по результатам работы нейронных сетей**

| Архитектура нейронной сети, № | Количество записей | Количество параметров обучения | Средняя точность, % |
|---|---|---|---|
| 1 | 23 | 34 | 36 |
| 2 | 23 | 34 | 39,3 |
| 1 | 23 | 44 | 44 |
| 2 | 23 | 44 | 44,7 |
| 2 | 23 | 65 | 44,1 |
| 1 | 46 | 34 | 42 |
| 2 | 46 | 34 | 42,4 |
| 1 | 46 | 44 | 50,1 |
| 2 | 46 | 44 | 50,8 |
| 2 | 46 | 65 | 69.6 |
| 1 | 96 | 65 | 76,3 |
| 2 | 96 | 65 | 82,1 |
| 3 | 96 | 65 | 89,8 |

образом, основное решение проблемы заключается в расширении датасета, что в компаниях со средствами мониторинга решается автоматически: можно собирать датасет действий, выполняемых специалистом ИБ.

**Заключение**

В результате проведенного исследования были выделены особенности и функции платформ реагирования на инциденты, указаны рекомендации по сбору датасетов и автоматизации IRP. Были построены нейросети, позволяющие определить действия в зависимости от характеристик инцидента. Даже несмотря на небольшие наборы данных, тестируемые нейросетевые архитектуры показали высокую среднюю точность около 90%. Кроме того, были указаны возможности и перспективы масштабирования подобных систем.

**Литература**


1. Containing the Uncontainable: Using AI for Incident Response, URL доступа: https://www.linkedin.com/pulse/containing-uncontainable-using-ai-incident-response-bise- (дата обращения: 15.10.2023)

2. Sarker I. H. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, №10(3), 2022. pages 1–26.

3. Очередько А.Р. Исследование irp-систем на основе анализа механизмов реагирования на инциденты информационной безопасности / А. Р. Очередько, Д. А. Бачманов, М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 1(53). – С. 74-82. – DOI 10.21672/2074-1707.2021.53.1.074-082. – EDN LVMANX.

4. Махнев А. О. Исследование платформ реагирования на инциденты информационной безопасности / А. О. Махнев, Н. П. Деканова // Молодая наука Сибири. – 2023. – № 1(19). – С. 147-157. – EDN UDRWEZ.

5. Computer Security Incident Handling Guide NIST, URL доступа: https://csrc.nist.gov/pubs/sp/800/61/r2/final (дата обращения: 15.10.2023)

6. Частикова В. А. Нейросетевая технология обнаружения аномального сетевого трафика / В. А. Частикова, С. А. Жерлицын, Я. И. Воля, В. В. Сотников // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 1(49). – С. 20-32. – DOI 10.21672/2074-1707.2020.49.4.020-032. – EDN WUCDII.

7. Обзор Innostage IRP, автоматизированной системы управления ИБ, URL доступа: https://www.anti-malware.ru/reviews/Innostage-IRP#part22 (дата обращения: 15.10.2023).

8. The Hive и Security Vision, URL доступа: https://habr.com/ru/articles/571604/ (дата обращения: 15.10.2023).

9. Detection–Rule-Dump набор правил обнаружения, URL доступа https://github.com/archanchoudhury/Detection-Rule-Dump (дата обращения: 15.10.2023).

10. Chastikova V.A. Method of analyzing computer traffic based on recurrent neural networks / V.A.

Chastikova, V.V. Sotnikov // Journal of Physics: Conference Series. International Conference "High-Tech and Innovations in Research and Manufacturing," 2019. C. 012133.

## References

1. Containing the Uncontainable: Using AI for Incident Response, URL dostupa: https://www.linkedin.com/pulse/containing-uncontainable-using-ai-incident-response-bise- (data obrashcheniya: 15.10.2023).

2. Sarker I. H. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, №10(3), 2022. pages 1–26.

3. Ochered'ko A.R. Issledovaniye irp-sistem na osnove analiza mekhanizmov reagirovaniya na intsidenty informatsionnoy bezopasnosti / A. R. Ochered'ko, D. A. Bachmanov, M. M. Putyato, A. S. Makaryan // Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. – 2021. – № 1(53). – S. 74-82. – DOI 10.21672/2074-1707.2021.53.1.074-082. – EDN LVMANX.

4. Makhnev A. O. Issledovaniye platform reagirovaniya na intsidenty informatsionnoy bezopasnosti / A. O. Makhnev, N. P. Dekanova // Molodaya nauka Sibiri. – 2023. – № 1(19). – S. 147-157. – EDN UDRWEZ.

5. Computer Security Incident Handling Guide NIST, URL dostupa: https://csrc.nist.gov/pubs/sp/800/61/r2/final (data obrashcheniya: 15.10.2023).

6. Chastikova V. A. Neyrosetevaya tekhnologiya obnaruzheniya anomal'nogo setevogo trafika / V. A. Chastikova, S. A. Zherlitsyn, YA. I. Volya, V. V. Sotnikov // Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. – 2020. – № 1(49). – S. 20-32. – DOI 10.21672/2074-1707.2020.49.4.020-032. – EDN WUCDII.

7. Obzor Innostage IRP, avtomatizirovannoy sistemy upravleniya IB, URL dostupa: https://www.anti-malware.ru/reviews/Innostage-IRP#part22 (data obrashcheniya: 15.10.2023).

8. The Hive i Security Vision, URL dostupa: https://habr.com/ru/articles/571604/ (data obrashcheniya: 15.10.2023).

9. Detection–Rule-Dump nabor pravil obnaruzheniya, URL dostupa https://github.com/archanchoudhury/Detection-Rule-Dump (data obrashcheniya: 15.10.2023).

10. Chastikova V.A. Method of analyzing computer traffic based on recurrent neural networks / V.A. Chastikova, V.V. Sotnikov // Journal of Physics: Conference Series. International Conference "High-Tech and Innovations in Research and Manufacturing," 2019. S. 012133.

---

**ЧАСТИКОВА Вера Аркадьевна**, кандидат технических наук, доцент, доцент кафедры «Кибербезопасность и защита информации» федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: chastikova_va@mail.ru

**КОЗАЧЁК Константин Валериевич,** аспирант кафедры «Кибербезопасность и защита информации» федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: Koza4ek.Konstantin@yandex.ru

**CHASTIKOVA Vera Arkadyevna,** candidate of Technical Sciences, associate professor, associate professor of the department «Cybersecurity and information protection» of the federal state budget educational institution of higher education «Kuban State Technological University». 350072, Krasnodar, Moskovskaya st., 2. E-mail: chastikova_va@mail.ru

**KOZACHOK Konstantin Valerievich,** post-graduate student of the department «Cybersecurity and information protection» of the federal state budget educational institution of higher education «Kuban State Technological University». 350072, Krasnodar, Moskovskaya st., 2. E-mail: Koza4ek.Konstantin@yandex.ru