Моделирование и анализ данных
2024. Том 14. № 3. С. 7–21
DOI: https://doi.org/10.17759/mda.2024140301
ISSN: 2219-3758 (печатный)
ISSN: 2311-9454 (online)

Modelling and Data Analysis
2024. Vol. 14, no. 3, pp. 7–21
DOI: https://doi.org/10.17759/mda.2024140301
ISSN: 2219-3758 (print)
ISSN: 2311-9454 (online)

◇◇◇◇◇◇◇◇◇◇АНАЛИЗ ДАННЫХ◇◇◇◇◇◇◇◇◇◇

УДК 378

Анализ угроз информационной безопасности органов государственной власти с помощью нейронных сетей

Пынько Л.Е.*
Дальневосточный институт управления – филиал РАНХиГС
(ФГБОУ ВО ДВИУ-филиал РАНХиГС)
г. Хабаровск, Российская Федерация
ORCID: https://orcid.org/0000-0002-8938-130X
e-mail: lusiena_03@mail.ru

Толкачева Е.В.**
Санкт-Петербургский государственный университет (ФГБОУ ВО СПбГУ)
г. Санкт-Петербург, Российская Федерация
ORCID: https://orcid.org/0000-0003-1304-809X
e-mail: e.tolkacheva@spbu.ru

Обеспечение информационной безопасности органов государственной власти требует применение специализированных инструментов, учитывающих существование разных источников информационных угроз, их постоянное изменение, а также проблемы интеграции оценок вероятности их реализации и степени возможного ущерба. Данное исследование направлено на разработку методики анализа угроз информационной безопасности органов государственной власти с помощью нейронных сетей. В исследовании использованы методы машинного обучения, нейросетевого анализа и систематизации. Для достижения задач исследования авторами была адаптирована архитектура MLP, проведена работа по настройке гиперпараметров нейронной сети. Обучение нейронной сети было реализовано на языке программирования Python. Эффективность работы нейронной сети в решении поставленной задачи оценивалась метриками accuracy, precision, recall, f1. Результатами исследования стали: разработка способа формирования набора данных, включающего оценки угроз информационной безопасности органов государственной власти различных видов и источников происхождения, оценка эффективности работы нейронной сети по решению задач классификации органов государственной власти, интерпретация результатов нейросетевого анализа о степени устойчивости органов государственной власти угрозам информационной безопасности.

Ключевые слова: органы государственной власти, информационная безопасность, информационные угрозы, нейронная сеть, набор данных.

Для цитаты:
Пынько Л.Е., Толкачева Е.В. Анализ угроз информационной безопасности органов государственной власти с помощью нейронных сетей // Моделирование и анализ данных. 2024. Том 14. № 3. С. 7–21. DOI: https://doi.org/10.17759/mda.2024140301

***Пынько Люсьена Евгеньевна,** кандидат экономических наук, доцент кафедры экономики и цифровых технологий, Дальневосточный институт управления – филиал РАНХиГС (ФГБОУ ВО ДВИУ-филиал РАНХиГС), г. Хабаровск, Российская Федерация, ORCID: https://orcid.org/0000-0002-8938-130X, e-mail: lusiena_03@mail.ru

****Толкачева Елена Вячеславовна,** кандидат социологических наук, доцент, доцент кафедры социального анализа и математических методов в социологии, Санкт-Петербургский государственный университет (ФГБОУ ВО СПбГУ), г. Санкт-Петербург, Российская Федерация, ORCID: https://orcid.org/0000-0003-1304-809X, e-mail: e.tolkacheva@spbu.ru

1. ВВЕДЕНИЕ

Цифровизация общества повысила значимость информационной безопасности данных, безопасность информационных сетей и систем, используемых органами государственной власти для осуществления своих полномочий. Современная цифровизация обозначила новые формы социокультурной и социо-экономической трансформации, представляющие собой не только переход к комфортному развитию и жизнедеятельности общества, но и к увеличению количества угроз, связанных с этим переходом [10].

Актуальность исследования обусловлена наблюдаемым в сфере государственного управления ростом разных видов информационных угроз. Следует отметить, что на текущий момент в России зарегистрировано свыше 200 различных угроз информационной безопасности[1]. К ним можно отнести такие как распространение состояния «отказ в обслуживании» в облачной инфраструктуре, утечка информации с неподключенных к сети Интернет компьютеров, захват информации в процессе ее передачи и др. [5; 12].

В этих условиях, анализ совокупности угроз информационной безопасности, а также классификация и ранжирование органов государственной власти по степени устойчивости к информационным угрозам для принятия дальнейших управленческих решений, становится трудоемкой задачей, решение которой видится нами в применении нейронных сетей.

Анализ литературных источников показал недостаточность исследований, касающихся аналитико-управленческих аспектов оценки подверженности органов государственной власти информационным угрозам, в том числе, с помощью нейронных

[1] По данным официального интернет-портала «Банк данных угроз безопасности информации» ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: https://bdu.fstec.ru/threat

сетей. Кроме того, в органах государственной власти существует необходимость постоянного мониторинга событий информационной безопасности, позволяющего оперативно противодействовать внешним нарушителям, повышать уровень защищенности сетей за счет интеллектуализации методов борьбы с угрозами информационной безопасности [7; 8]. Соответственно существует необходимость в создании методики, позволяющей анализировать актуальность различных информационных угроз, классифицировать и ранжировать с помощью нейронных сетей органы государственной власти по степени их устойчивости угрозам информационной безопасности.

Данное исследование нацелено на разработку методики анализа угроз информационной безопасности с помощью нейронных сетей на основе концепта устойчивости органов государственной власти угрозам информационной безопасности.

Основные задачи исследования:

- охарактеризовать угрозы информационной безопасности органов государственной власти и правовые последствия от их реализации;
- сформулировать правила формирования набора данных, для классификации органов государственной власти по степени устойчивости угрозам информационной безопасности с помощью нейронных сетей;
- описать этапы обучения нейронной сети для решения задач классификации органов государственной власти по степени их устойчивости угрозам информационной безопасности;
- дать оценку качества нейронной сети, а также интерпретацию полученным в ходе обучения результатам.

Новизна исследования заключается в разработке правил формирования набора данных об угрозах информационной безопасности для нейросетевого анализа устойчивости органов государственной власти информационным угрозам. В предложенный набор данных можно включать разнообразный перечень угроз, оценка каждой из которых должна быть дана по дихотомической шкале.

Методологию исследования составляет системный подход, который позволяет придерживаться идеи формирования набора данных для нейросетевого анализа, включающего различные угрозы информационной безопасности данным и каналам связи органов государственной власти. Использованная в исследовании архитектура MLP адаптирована под задачу исследования. Модуль нейронной сети был реализован на языке программирования Python. Вычисления проводились с помощью библиотек TensorFlow, Keras, Pandas, Scikit-learn, Matplotlib. Разработка велась в специализированной среде Jupyter Notebook.

Разработанная методика позволяет решать задачи классификации органов государственной власти по интегральной оценке, характеризующей степень их устойчивости ко всей совокупности анализируемых угроз информационной безопасности.

2. СОВРЕМЕННЫЕ ПОДХОДЫ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Угрозы информационной безопасности в деятельности органов государственной власти тесно коррелируют с уже существующими системами по противодействию преступности, которые используют правоохранительные органы. Зарубежный опыт применения информационных систем для анализа и прогнозирования преступлений в сфере информационной безопасности и определения мер их предупреждения активно используется на протяжении последних десятилетий. При этом, опыт использования информационных систем в деятельности правоохранительных органов для осуществления анализа киберпреступлений, прогнозирования (преступлений, личностей правонарушителей, жертв преступлений), определения мероприятий по предупреждению преступности, в том числе с привязкой к их географическому положению, оперативный анализ данных из сети Интернет, а также на основе данных из социальных сетей с дачей оценки последствий их проведения, на протяжении последних десятилетий активно используется в зарубежных странах [3].

Угрозы информационной безопасности органов государственной власти могут содержать противоправные и насильственные действия отдельных групп людей, направленные на дискредитацию социально-политической и правовой системы российского общества, т.е. преступления террористической и экстремистской направленности.

Также, сегодня необходимы исследования системы факторов, определяющих угрозы информационной безопасности, которые могут, в определенных условиях, преобразоваться в реальные угрозы жизни, здоровью, свободе передвижения государственных служащих и их семей. Эта тема нуждается не только в широком экспертном разностороннем обсуждении (с позиции знаний политологии, социологии, информационных угроз, инженерии информационных систем, правового регулирования и т.п.); но, и, в междисциплинарном исследовании с разработкой единообразных подходов защиты органов государственной власти в информационном поле и социально-экономическом пространстве. Необходимы разработки конкретных методик, позволяющих выявлять подверженность информационным угрозам и своевременно разрабатывать меры по противодействию им.

Проведение анализа угроз информационной безопасности органов государственной власти, в первую очередь, предполагает их идентификацию. При идентификации, выявляются не только угрозы информационной безопасности в деятельности органов государственной власти, но и источники их возникновения. При этом мы предлагаем использовать системный подход, включающий в себя научно-технический, социальный, экономический и политический аспекты возникновения угроз информационной безопасности в деятельности органов государственной власти. Еще раз подчеркнем о необходимости классификации и градации самих информационных угроз.

С точки зрения типов угроз информационной безопасности, в частности, МВД России ведет статистику числа киберпреступлений в соответствии с нормами УК РФ

(ст.ст.159.3, 272, 273, 274 и т. п.). Например, если в первый год действия норм гл. 28 УК РФ было зарегистрировано 2698 преступлений, то в 2017 г. таких преступлений стало почти вдвое меньше – 1883 (рис. 1).

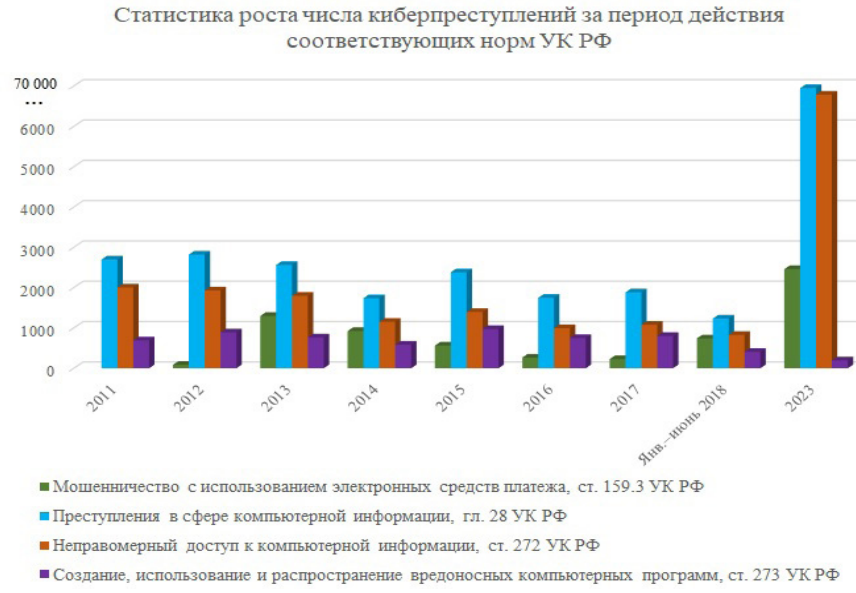

Рис. 1. Статистика роста числа киберпреступлений в России за 2011–2023 гг.[2]

Примечательно, что ст. 274 УК РФ о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации совсем не пользуется популярностью: всего 2 преступления зафиксировано в 2017 г. и ни одного – за первое полугодие 2018-го. В тоже время число преступлений, предусмотренных ст. 273 УК РФ, о создании, использовании и распространении вредоносных программ, напротив, возросло до 802 в 2017 г. по сравнению с 693 случаями в 2011 г. Всплеск преступлений, предусмотренных ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа», наблюдался в 2013 г. – втором году действия нормы –1297 случаев. Почти аналогичная цифра формируется и в текущем году – 741 преступление за первое полугодие. Увеличилось число хакерских атак на бюджетников и госслужащих. На их страницах появляются обращения к подписчикам с просьбой совершить определенные противоправные действия или распространить запрещенные ссылки. Министерство внутренних дел РФ за 2023 год зарегистрировало 677 тыс. IT – преступлений в стране, что стало рекордным уровнем за все время. В 2022 году МВД зафиксировало 522,1 тыс. таких преступлений – на треть меньше, чем в 2023 году.

[2] Составлено по данным официального интернет-портала МВД Российской Федерации. – URL: https://мвд.рф/reports, портала правовой статистики Генеральной прокуратуры России. – URL: http://crimestat.ru/analytics

Удельный вес дел по таким правонарушениям увеличился с 26,5% до 34,8%. Свыше половины зарегистрированных преступлений, совершенных с использованием информационных технологий, относится к категориям тяжких и особо тяжких. Число преступлений с применением Интернет выросло с 381 тыс. до 526,7 тыс.

Следом идут преступления, совершенные с использованием средств мобильной связи и пластиковых карт.

В контексте изучаемой нами проблемы следует отметить, что угрозы информационной безопасности в деятельности органов государственной власти связаны с ростом напряженности в обществе, что повышает риск нарушений в обращении с персональными данными в деятельности органов государственной власти, что также является отдельным видом угроз. Задача оценки и предотвращения подобных угроз заключается в уменьшении социальной напряженности российского общества, страдающего от негативных последствий этих угроз в будущем.

3. ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Рассматриваемая в данной статье методика анализа угроз информационной безопасности органов государственной власти предполагает решение задачи классификации с помощью нейронных сетей. Задача классификации может быть поставлена в случаях, когда требуется определить, какие органы государственной власти могут быть отнесены к группам с удовлетворительной и низкой степенью устойчивости к угрозам информационной безопасности.

Предлагаемая нами методика анализа включает в себя несколько этапов.

Первый этап предполагает выбор органов государственной власти для последующего анализа. Мы не дифференцируем органы государственной власти на исполнительные, законодательные и судебные, делая акцент на универсальности методики. При ее внедрении в практическую деятельность органов государственной власти, необходимо осуществлять выбор объектов анализа, исходя из ключевых положений Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. N 646, в которой обозначены основные участники системы обеспечения информационной безопасности.

Второй этап предполагает составление реестра угроз информационной безопасности, подлежащих анализу. В контексте данного этапа необходимо отметить, что при составлении реестра следует учитывать методический документ «Методика оценки угроз безопасности информации», утвержденный Федеральной службой по техническому и экспертному контролю 5 февраля 2021 года (далее Методический документ). Для составления реестра угроз информационной безопасности с целью последующего анализа, также, необходимо опираться на общий перечень угроз безопасности

информации, а также существование шести типов нарушителей и их потенциал[3]. При этом следует учитывать отсутствие метода, позволяющего выявить прямые зависимости между конкретным видом угроз и типом нарушителя. В связи с этим, реестр угроз информационной безопасности может быть построен путем перебора всех возможных нарушителей относительно отдельно взятой угрозы [1].

На третьем этапе осуществляется оценка и градация каждой угрозы по двум признакам: «вероятность реализации угрозы» и «значимость ущерба, причиненного в случае реализации угрозы». Указанные признаки связаны с основными задачами, решаемыми в ходе оценки и обозначенными в Методическом документе. При оценке значимости ущерба, причиненного в случае реализации угрозы, в первую очередь рассматриваются такие последствия как нарушение конфиденциальности, целостности и доступности информации. В свою очередь, Федеральная служба по техническому и экспертному контролю предлагает рассматривать 52 негативных последствия[4]. Однако не все из них возникают в случаях, когда речь идет об органах государственной власти.

Четвертый этап предполагает экспертную оценку и присвоение каждому из анализируемых органов государственной власти класса от 0 до 2 с учетом значимости ущерба и вероятности реализации угроз информационной безопасности. Набор данных, формируемый для последующего нейросетевого анализа, будет содержать оценки угроз информационной безопасности по дихотомической шкале: актуальные (1) или неактуальные (0), составленные на основании правил, предложенных Ершовым В.Н. и Смирновой П.Л. [1]. Оценка угроз информационной безопасности производится экспертами или сотрудниками, ответственными за обеспечение информационной безопасности в органах государственной власти. При этом следует отметить важность оценки размера потенциального ущерба (градация угроз по величине потенциального ущерба или масштабу негативных последствий). В вопросах информационной безопасности ключевым значением является неприемлемость ущерба, возникшего вследствие нарушения информационной защищенности органов государственной власти.

При составлении набора данных существует риск получения несбалансированных данных, когда один или два класса являются преобладающими, а третий находится в меньшинстве. Одно из возможных решений предложено Azad S., Naqvi S.S., Sabrina F., Sohail S., Thakur S., которые отмечали, что в случае возникновения проблемы обучения нейронной сети на основе несбалансированных данных можно использовать бинарный классификатор для каждой категории угроз информационной безопасности, где объекты рассматриваемого класса угроз могут быть помечены как класс 1, а остальные объекты – как класс 0 [9].

На пятом этапе подготовленный набор данных используется для обучения нейронной сети. Данные, нормализуются с помощью формулы Z-преобразования для

[3] По данным официального интернет-портала «Банк данных угроз безопасности информации» ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: https://bdu.fstec.ru/threat

[4] По данным официального интернет-портала «Банк данных угроз безопасности информации» ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: https://bdu.fstec.ru/threat

каждого признака, далее они делятся на обучающий и тестовый набор, включающие в себя: обучающий набор признаков, тестовый набор признаков, обучающий набор целевых переменных, тестовый набор целевых переменных; размер тестового набора. После этого осуществляется обучение нейронной сети, которая представляет собой многослойный перцептрон (MLP). В данном случае MLP имеет два скрытых слоя. Входной слой имеет столько нейронов, сколько признаков в данных. Выходной слой имеет столько нейронов, сколько классов в задаче классификации. В предлагаемой нами модели это 3 класса. MLP обучается с использованием алгоритма обратного распространения. Он минимизирует функцию потерь, которая измеряет ошибку модели на обучающем наборе. В данном случае используется функция потерь кросс-энтропии для многоклассовой кластеризации. При классификации угроз информационной безопасности может возникнуть необходимость решения проблемы несбалансированности данных [9].

После создания нейронной сети необходимо провести оценку качества. Оценка качества нейронной сети выполняется с помощью формулы для вычисления точности [4]:

$$accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)},$$

где: TP – количество истинных положительных результатов; TN – количество истинных отрицательных результатов; FP – количество ложных положительных результатов; FN – количество ложных отрицательных результатов.

На шестом этапе предполагается применение обученной нейронной сети на новых данных, что позволяет осуществлять классификацию органов государственной власти по степени устойчивости к угрозам информационной безопасности. С помощью обученной нейронной сети предсказываются классы. На этом этапе используются тестовый набор данных с аналогичными параметрами. Нейронная сеть вычисляет вероятность того, что точка данных принадлежит каждому классу, а затем предсказывает класс с наивысшей вероятностью.

На седьмом этапе осуществляется разработка мер по обеспечению большей защищенности от угроз информационной безопасности органов государственной власти, отнесенных к классам с удовлетворительной и низкой устойчивостью. Для успешного обучения нейронной сети необходима разметка данных, при которой органы государственной власти классифицируются по степени устойчивости к угрозам информационной безопасности с учетом того, что вероятность реализации хотя бы одной из анализируемых угроз имеется:

- хорошая устойчивость угрозам информационной безопасности (2);
- удовлетворительная устойчивость угрозам информационной безопасности (1);
- низкая устойчивость угрозам информационной безопасности (0).

Предлагаемая нами методика позволяет анализировать различные модели угроз, включающие в себя как угрозы данным, так и информационным системам или сетям,

используемых органами государственной власти; учитывает критерий «достаточности защиты», при этом выстроена не вокруг оценки уровня защищенности органов государственной власти, а сконцентрирована на выявлении степени их устойчивости угрозам информационной безопасности.

4. РЕЗУЛЬТАТЫ ПОСТРОЕНИЯ НЕЙРОННОЙ СЕТИ

Модуль нейронной сети реализован нами на языке программирования Python с использованием смоделированного набора данных. Обучающий набор включал 1000 записей, тестовый – 200 записей. Эти данные послужили основой для разработки и обучения нейронной сети, которая представляет собой многослойный перцептрон (MLP) и используется для обеспечения высокой точности в задачах классификации. Разработка нейронной сети велась в специализированной среде jupyter notebook. Вычисления проводились с помощью библиотек TensorFlow, Keras, Pandas, Scikit-learn, Matplotlib.

Ключевые особенности архитектуры нейронной сети:

- Входной слой: принимает данные с размерностью, равной количеству признаков. В нашем случае признаков 20, что соответствует количеству анализируемых угроз информационной безопасности, каждая из которых была оценена по признакам вероятности реализации и вероятности значимости ущерба на основе правил, сформулированных Ершовым В.Н. и Смирновой П.Л. [1].
- Скрытые слои: два скрытых слоя с 68 нейронами в каждом, функцией активации ReLU и L2 регуляризацией для предотвращения переобучения. В данном случае был учтен опыт первоначального построения нейронной сети с двумя скрытыми слоями и без регуляризации, что приводило к ее переобучению.
- Dropout слои: с вероятностью отключения нейронов 0,5 после каждого скрытого слоя для уменьшения переобучения.
- Выходной слой: предполагающий наличие трех классов.
- Оптимизатор: метод адаптивного момента (Adam) с функцией потерь перекрестной энтропии для многоклассовой классификации [6].

Для корректного обучения нейронной сети было задано 200 эпох, тем не менее, высокая точность достигалась раньше. Нами были получены следующие результаты, указывающие на качество машинного обучения: пройдено 128 эпох из 200, точность на обучающем наборе данных составляет 96,25%, а на валидационном – 96,5%. Это очень близко к итоговой точности на тестовом наборе данных, которая равна 97% (рис. 2).

Потери на тестовом наборе данных низкие и составляют 0,2276. Это свидетельствует о том, что модель хорошо обучилась и обладает хорошей обобщающей способностью, поскольку показатели на валидационном и тестовом наборах данных схожи с результатами на обучающем наборе. Соответственно, риск переобучения минимален (рис. 3).

Для оценки качества модели использовались следующие метрики: accuracy (точность), precision (точность) для каждого класса, recall (полнота), f1-score (среднее гармоническое precision и recall) [4].

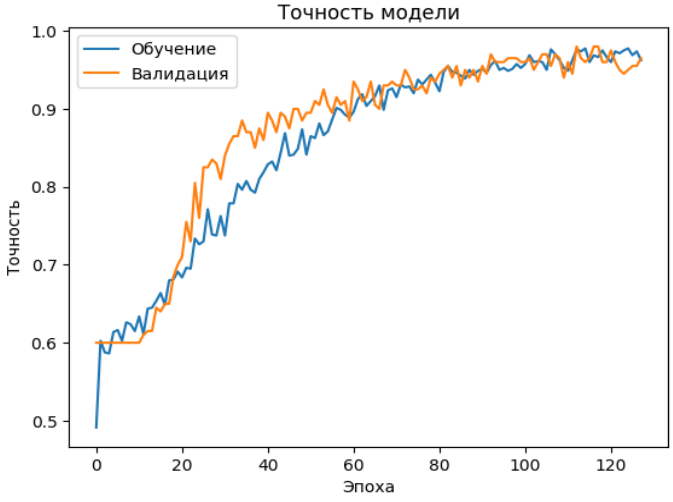

Рис. 2. Отчет о качестве работы нейронной сети, указывающие на ее точность

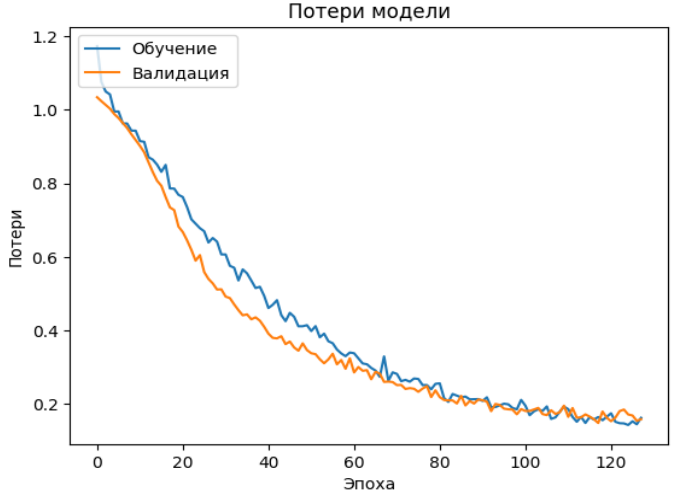

Рис. 3. Отчет о качестве работы нейронной сети, демонстрирующие потери

Применение обученной модели на новых данных показало, что модель демонстрирует высокую точность в 95% случаев на тестовом наборе данных. При этом класс 0 имеет показатели precision и recall равные 1, что означает, что нейронная сеть отлично классифицирует этот класс. Класс 1 также показывает хорошие результаты, так как показатель precision равен 0,94, а показатель recall равен 0,99, что указывает на высокую точность и полноту. Класс 2 имеет хороший показатель precision

равный 0,97, но при этом показатель recall равен 0,8, что указывает на то, что модель может упускать некоторые положительные случаи этого класса.

Полученные нами результаты демонстрируют, что в анализе угроз информационной безопасности возможно применение системного подхода, позволяющего включать в набор данных оценки информационных угроз разных видов, при условии оценки вероятности возникновения и вероятности нанесения значимого ущерба по дихотомической шкале. Обученная нейронная сеть может быть использована при анализе систем информационной безопасности органов государственной власти. Востребованность в этом отмечалась, например, Resch C. [11].

Проведенное исследование показало, что применение нейронных сетей позволяет давать точные результаты классификации органов государственной власти при работе с набором данных, содержащим оценки разных угроз информационной безопасности. Применение разработанной авторами методики анализа угроз информационной безопасности возможно в различных органах государственной власти.

5. ЗАКЛЮЧЕНИЕ

Полученные в ходе исследования результаты позволяют сделать вывод, что предложенные нами правила формирования набора данных угроз информационной безопасности для классификации органов государственной власти по степени устойчивости угрозам информационной безопасности с помощью нейронных сетей, позволяют получать результаты высокой точности.

Ограничением предлагаемой методики является необходимость решения вопроса об используемых для обучения нейронной сети объемах данных, которое определяется рядом факторов. К ним относятся сложность задачи, неизвестная целевая функция, которая оптимально описывает связь между входными и выходными переменными, а также сложность выбранного алгоритма обучения. Также следует учитывать существование риска переобучения модели нейронной сети. В связи с чем, необходимо обращать внимание на такие ее параметры как: погрешность ошибок или число итераций. В решаемой задаче метод классификации был определен нами заранее. Сложность задачи потребовала применение функции потерь, что на начальном этапе разработки нейронной сети нами не предполагалось.

Использование системного подхода представлено в формировании набора данных, включающих различные виды информационных угроз, имеющих разные источники возникновения. В данном случае мы придерживались точки зрения, что выполнение анализа информационных угроз изолированно друг от друга нецелесообразно, так как нарушается целостность научного изучения «информационной безопасности».

Применение данной методики может представлять интерес при анализе систем информационной безопасности органов государственной власти и возможно в ходе аудита. Результатом применения методики на практике является получение интегрированной оценки степени устойчивости органов государственной власти актуальным угрозам информационной безопасности. По результатам нейросетевого анализа

могут приниматься управленческие решения, связанные с противодействием информационным угрозам, в том числе разрабатываться инструкции для государственных служащих, детальные планы мероприятий с четким описанием последовательности действий по предотвращению информационных угроз.

Литература

1. *Ершов В.Н., Смирнова П.Л.* Информационная защита персональных данных: доминирующий источник угрозы // Бизнес-информатика. 2012. № 2(20).
2. *Клименко Л.В.* Концептуальные основания исследования социетальной сферы поликультурных регионов // Материалы международной научно-практической конференции «Этносоциальные процессы на Юге России: способы регулирования» (г. Майкоп, 21–22 ноября 2017 г.). Майкоп: ООО «Электронные издательские технологии», 2017. С. 48–50.
3. *Лаптев А.С.* Цифровой портал «Криминологическое планирование» – основной помощник в принятии управленческих решений в сфере предупреждения преступлений // Юридические исследования. 2023. № 8. С. 84–95. doi:10.25136/2409-7136.2023.8.43734
4. *Мамиев О.А., Финогенов Н.А., Сологуб Г.Б.* Использование методов машинного обучения для решения задач прогнозирования суммы и вероятности покупки на основе данных электронной коммерции // Моделирование и анализ данных. 2020. Т. 10. № 4. С. 31–40. doi:10.17759/mda.2020100403
5. *Михайлова Л.С.* О некоторых проблемах обеспечения информационной безопасности органов исполнительной власти // Вестник Воронежского института МВД России. 2022. № 2. С. 276–282.
6. Сравнение методов обучения нейронных сетей в задаче классификации / Перков А.С. [и др.] // Известия СПбГЭТУ ЛЭТИ. 2019. № 6. С. 53–61.
7. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / Пучков А.Ю. [и др.] // Прикладная информатика. 2023. Т. 18. № 2(104). С. 85–102. doi:10.37791/2687-0649-2023-18-2-85-102
8. *Сиденко А.И.* О подготовке стратегии информационной безопасности исполнительных органов государственной власти Санкт-Петербурга // Сборник трудов Санкт-Петербургской международной конференции «Региональная информатика и информационная безопасность» (г. Санкт-Петербург, 25–27 октября 2023 г.). Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 8–18.
9. *Azad S. et al.* IoT Cybersecurity: On the Use of Machine Learning Approaches for Unbalanced Datasets // *2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Brisbane, Australia. 2021. P. 1–6. doi:10.1109/CSDE53843.2021.9718426
10. *Bohme G.* Am Ende des Beconschen Zeitalters, Wissenschaft und Gesellschaft. Science and. Society. N. 3. 129 p.
11. *Resch C.* Designing an information security system // 5th Annual IEEE Information Assurance Workshop. 2004. P. 449–450. doi:10.1109/IAW.2004.1437857
12. *Stephen D.G.* IT Audit Drivers // The Basics of IT Audit. 2014. P. 129–148. doi:10.1016/B978-0-12-417159-6.00007-9

Analysis of Threats to Information Security of Public Authorities Using Neural Networks

Luyciyena E. Puinko*
Far Eastern Institute of Management – branch of RANEPA
Khabarovsk, Russian Federation
ORCID: https://orcid.org/0000-0002-8938-130X
lusiena_03@mail.ru

Elena V. Tolkacheva**
St. Petersburg State University, St. Petersburg, Russian Federation
ORCID: https://orcid.org/0000-0003-1304-809X
e-mail: e.tolkacheva@spbu.ru

Ensuring the information security of public authorities requires the use of specialized tools that take into account various sources of information threats and their constant changes. This study aims to develop a methodology for analyzing these threats using neural networks. The research uses methods such as machine learning and neural network analysis to systematize the data. The authors adapted the Multi-Layer Perceptron (MLP) architecture and configured the hyperparameters of the neural network to achieve their objectives. The neural network was trained using the Python programming language, and its effectiveness was evaluated using metrics such as accuracy, precision, recall, and F1 score. The results of the study included the development of a method for creating a data set that encompasses assessments of threats to the information security of various public authorities and their sources. Additionally, the study evaluated the effectiveness of neural networks in solving classification problems for public authorities. Finally, the study interpreted the results of neural network analysis to determine the resistance of public authorities against information security threats.

Keywords: public authorities, information security, information threats, neural network, data set.

For citation:
Puinko L.E., Tolkacheva E.V. Analysis of Threats to Information Security of Public Authorities Using Neural Networks. *Modelirovanie i analiz dannykh = Modelling and Data Analysis,* 2024. Vol. 14, no. 3, pp. 7–21. DOI: https://doi.org/10.17759/mda.2024140301 (In Russ., abstr. in Engl.).

Luyciyena E. Puinko, PhD (Economics), Associate Professor, Department of Economics and Digital Technologies, Far Eastern Institute of Management the Russian Presidential Academy of National Economy and Public Administration, Russia, ORCID: https://orcid.org/0000-0002-8938-130X, e-mail: lusiena_03@mail.ru

****Elena V. Tolkacheva,*** PhD (Social), Associate Professor, Department of Social Analysis and Mathematical Methods in Sociology, St. Petersburg State University, Russia, ORCID: https://orcid.org/0000-0003-1304-809X, e-mail: e-v-tolkacheva@ya.ru

References

1. Ershov V.N., Smirnova P.L. Informatsionnaya zashchita personal'nykh dannykh: dominiruyushchii istochnik ugrozy [Information protection of personal data: the dominant source of threat]. *Biznes-informatika = Business Informatics*. 2012. no. 2 (20).
2. Klimenko L.V. Kontseptual'nye osnovaniya issledovaniya sotsietal'noi sfery polikul'turnykh regionov [Conceptual foundations for the study of the societal sphere of multicultural regions]. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii "*Etnosotsial'nye protsessy na Yuge Rossii: sposoby regulirovaniya*" (g. Maikop, 21–22 noyabrya 2017 g.) [Proceedings of the International Scientific and Practical Conference "*Ethnosocial processes in the South of Russia: methods of regulation*"]. Maykop: Publ. Electronic Publishing Technologies LLC, 2017. pp. 48–50.
3. Laptev A.S. Tsifrovoi portal "Kriminologicheskoe planirovanie" – osnovnoi pomoshchnik v prinyatii upravlencheskikh reshenii v sfere preduprezhdeniya prestuplenii [Digital portal "Criminological planning" – the main assistant in making managerial decisions in the field of crime prevention]. *Yuridicheskie issledovaniya = Legal research*. 2023. no. 8. pp. 84–95. doi:10.25136/2409-7136.2023.8.43734
4. Mamiev O.A., Finogenov N.A., Sologub G.B. Ispol'zovanie metodov mashinnogo obucheniya dlya resheniya zadach prognozirovaniya summy i veroyatnosti pokupki na osnove dannykh elektronnoi kommertsii [Using machine learning methods to solve problems of predicting the amount and probability of purchase based on e-commerce data]. *Modelirovanie i analiz dannykh = Modeling and data analysis*. 2020. T. 10. no. 4. pp. 31–40. doi:10.17759/mda.2020100403
5. Mikhailova L.S. O nekotorykh problemakh obespecheniya informatsionnoi bezopasnosti organov ispolnitel'noi vlasti [About some problems of ensuring information security of executive authorities]. *Vestnik Voronezhskogo instituta MVD Rossii = Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2022. no. 2. pp. 276–282.
6. Perkov A.S. [i dr.] Sravnenie metodov obucheniya neironnykh setei v zadache klassifikatsii [Comparison of neural network training methods in the classification problem] *Izvestiya SPbGETU LETI = Izvestiya SPbGETU LETI*. 2019. no. 6. pp. 53–61.
7. Puchkov A.Yu. [i dr.] Algoritm vyyavleniya ugroz informatsionnoi bezopasnosti v raspredelennykh mul'tiservisnykh setyakh organov gosudarstvennogo upravleniya [Algorithm for identifying information security threats in distributed multiservice networks of government agencies] *Prikladnaya informatika = Applied Informatics*. 2023. T. 18. no. 2 (104). pp. 85–102. doi:10.37791/2687-0649-2023-18-2-85-102
8. Sidenko A.I. O podgotovke strategii informatsionnoi bezopasnosti ispolnitel'nykh organov gosudarstvennoi vlasti Sankt-Peterburga [On the preparation of the information security strategy of the executive bodies of state power of St. Petersburg]. Sbornik trudov Sankt-Peterburgskoi mezhdunarodnoi konferentsii "*Regional'naya informatika i informatsionnaya bezopasnost'*" (g. Sankt-Peterburg, 25–27 oktyabrya 2023 g.) [Proceedings of the St. Petersburg International Conference *"Regional Informatics and Information Security"*]. St. Petersburg: Publ. St. Petersburg Society of Informatics, Computer Technology, Communication and Management Systems, 2023. pp. 8–18.
9. Azad S. et al. IoT Cybersecurity: On the Use of Machine Learning Approaches for Unbalanced Datasets *2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Brisbane, Australia. 2021. pp. 1–6. doi:10.1109/CSDE53843.2021.9718426
10. Bohme G. Am Ende des Beconschen Zeitalters, Wissenschaft und Gesellschaft. *Science and Society*. no. 3. 129 p.

11. Resch C. Designing an information security system *5th Annual IEEE Information Assurance Workshop*. 2004. pp. 449–450. doi:10.1109/IAW.2004.1437857
12. Stephen D.G. IT Audit Drivers *The Basics of IT Audit*. 2014. pp. 129–148. doi:10.1016/B978-0-12-417159-6.00007-9

Получена 19.07.2024 Received 19.07.2024
Принята в печать 18.08.2024 Accepted 18.08.2024