DOI 10.36622/VSTU.2023.4.26.010
УДК 004.056.5

НЕЙРОСЕТЕВЫЕ ЗАДАЧИ И КОМПЕТЕНЦИИ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПО СОЗДАНИЮ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Г.А. Остапенко, А.П. Васильченко

Рассматриваются противоречия инструментальной базы проектирования атакуемых автоматизируемых информационных систем (АИС). Обосновывается объективная необходимость использования в проектной деятельности искусственных нейросетей в качестве интеллектуальной поддержки организационно- правовых и научно-технических управленческих решений по защите информации в АИС. Осуществляется целеполагание исследования в условиях неуклонно растущего многообразия компьютерных атак и революционного развития искусственного интеллекта. Формулируются задачи и ожидаемые результаты, а также - необходимые для их достижения нейросетевые компетенции, формирование и развитие которых представляется актуальным условием успеха исследований и разработок в области интеллектуализации создаваемых и эксплуатируемых АИС.

Ключевые слова: нейросети, автоматизированные информационные системы, компьютерные атаки, компетенции.

Введение

Особенностью текущего момента в процессе развития мирового и национальных киберпространств состоит в том, что они стали театром сетевых войн [1-8], где наблюдаются массированные атаки боеголовками, представляющими собой вредоносные коды [1,2,6] и деструктивные контенты [3-7], наносящие значительные информационные и другие ущербы. В этом контексте приобретают особое значение методы и средства киберзащиты [8], способные обеспечить адекватную безопасность автоматизированных информационных систем и сетей. При этом, трендом современности выступают технологии искусственного интеллекта (ИИ), эффективно автоматизирующие принятие решений в условиях обработки и слабоструктурированных данных [7]. Это имеет прямое отношение и к компьютерным атакам [8] многообразие и интенсивность которых в отношении АИС неуклонно возрастает. Поэтому настоящая работа ставит своей задачей попытку хотя бы частично отреагировать на этот вызов с использованием возможностей средств ИИ, коими зачастую выступают нейросети.

Актуальные задачи проектной деятельности по созданию защищённых автоматизированных информационных систем с помощью нейросетей

Сейчас проводится довольно активная научно-техническая работа [8] по выработке рекомендаций для построения эффективных политик, регламентов и инструкций сетевой защиты АИС. Однако проблема здесь состоит в том, что частные решения сталкиваются с многообразием деструктивов (сотни разновидностей атак и тысячи используемых ими уязвимостей), анализ которого невозможен без соответствующей автоматизации. Фактически, разработчики сталкиваются с противоречием между мультиразмерностью, стоящей перед лицом, принимающим решение, (ЛПР) задачи и отсутствием эффективного инструментария, генерирующего адекватные интеллектуальные подсказки по выбору мер организационно-правового и научно-технического противодействия вышеупомянутым вредоносам в реальном масштабе времени. Даже при наличии масштабной базы знаний о кибератаках, оперативный подбор необходимых тактик и техник борьбы с ними не представляется

возможным осуществить ЛПР вручную. И здесь уместно использовать нейросети.

В этом контексте представляется возможным осуществить следующее целеполагание проектной деятельности.

Цель: поиск эффективных организационно-правовых и научно-технических решений построения и практического использования нейросетевого инструментария для отработки и внедрения перспективных тактик и техник комплексного противодействия и распределенным сетевым атакам.

Объект: автоматизированная информационная система, подвергающаяся многосложным сетевым атакам.

Предмет: создание среды интеллектуальной поддержки управленческих решений в ходе противодействия сетевым атакам в защищаемой автоматизированной информационной системе.

Задачи:

1. На основе выработки частных регламентов обнаружения и регистрации инцидентов, реагирования на инциденты, ликвидации последствий инцидентов для многообразия сетевых атак, формирование базы знаний мер противодействия вторжениям в систему.

2. В динамике киберпротивоборства системы с нарастающим многообразием векторов сетевых атак, используемых ими уязвимостей и возникающих ущербов, обучение нейросети полученным знаниям о мерах защиты от вторжений.

3. Автоматизация формирования интеллектуальных подсказок лицу, принимающему решения в ходе сетевого противоборства, в части регламентации оперативного реагирования на выявление вторжения, а также коррекции политики и инструкций обеспечения информационной безопасности системы, исходя из накопленного опыта противодействия.

Приведённые исследовательские задачи, разумеется, нуждаются в адаптации к применению технологий ИИ, где наличествует своя специфика представления и обработки больших данных, необходимых для выработки интеллектуальных подсказок ЛПР в ходе информационного противоборства.

Необходимой новизной и практической ценностью в этом случае будут обладать результаты проектной деятельности, обеспечивающие:

1. Оперативные выявления в АИС вторжений и их идентификацию по классификаторам CAPEC, MITRA, CWE, БДУ и др.

2. Создание баз знаний мер противодействия кибератакам на уровнях частных политик, регламентов и инструкций безопасности АИС.

3. Обучение нейросетей на основе вышеуказанных баз знаний и выработка практических решений по киберзащите атакуемых АИС.

Всё это представляется возможным при наличии компетенций, о которых речь пойдёт дальше.

Нейросетевые компетенции, необходимые при проектировании защищённых автоматизированных информационных систем

Для создания АИС в защищённом исполнении с помощью нейросетей уместно приобретение и использование компетенций, перечисленных в табл. 1.

Таблица 1

Компетенции, необходимые при структурировании данных для обучения искусственного интеллекта

Область применения компетенций	Структурирование данных для обучения искусственного интеллекта (ИИ):
№	Сущность необходимых компетенций
1.1	Знать средства и приложения ИИ (дипфейки, обработка текстов и речи, компьютерное зрении, клонирование голоса и др.)

Продолжение табл.1

Область применения компетенций	Структурирование данных для обучения искусственного интеллекта (ИИ):
№	Сущность необходимых компетенций
1.2	Уметь выявлять угрозы, идентифицировать атаки и уязвимости ИИ.
1.3	Уметь создавать политики безопасности, регламенты и инструкции защиты от угроз ИИ.
1.4	Знать стандарты и нормативные документы (ISO 27001, NIST, CAPEC, MITRA, CWE, БДУ и др.)
1.5	Владеть инструментами и фреймворками безопасности (TensorFlow Privacy, PySyft, PyTorch, Crypten и т. п.).

Особое значение имеет правомерность использования данных в системах ИИ. Компетенциями в этой сфере посвящены табл. 2.

Таблица 2

Компетенции по правомерности использования данных ИИ

Область применения компетенций	Правомерность использования данных ИИ:
№	Сущность необходимых компетенций
2.1	Знать о технологиях и приложениях ИИ в контексте экономических и социальных последствиях их применения.
2.2	Уметь использовать инструменты и методы ИИ, для генерации аналитической информации (прогнозы, политики, оценки безопасности и др.).
2.3	Уметь обеспечивать синергетический эффект от консолидации усилий всех сторон, заинтересованных в успехе внедрения ИИ.
2.4	Уметь управлять рисками и шансами правового регулирования ИИ.
2.5	Уметь осуществлять мониторинг и обеспечивать соответствие системам и пользователей ИИ соответствующим законам и стандартам.

Наряду с правовыми вопросами особое значение имеет формирование запросов для систем ИИ. Навыки этого перечисляются в табл. 3.

Таблица 3

Компетенции в формировании запросов для ИИ

Область применения компетенций	Безопасность применения ИИ:
№	Сущность необходимых компетенций
3.1	Иметь навыки командной работы во взаимодействии с другими генераторами запросов и прочими заинтересованными лицами
3.2	Владеть методами и средствами программирования, необходимыми для формирования ИИ-запросов.
3.3	Иметь навыки проведения АБ-тестирования и экспериментов для оценки эффективности исполнения запросов.

Не следует оставлять без внимания и аспекты безопасности применения ИИ, которым посвящена табл. 4.

Таблица 4

Компетенции по безопасности применения ИИ

Область применения компетенций	Безопасность применения ИИ:
№	Сущность необходимых компетенций
4.1	Знать федеральные законы и нормы о защите персональных данных и конфиденциальности потребителей.
4.2	Уметь оценивать защищённость данных (DPIA - Data Protection Impact Assessment), выявлять информационные риски и владеть мерами по урегулированию этих рисков в связи с использованием персональных данных и другой конфиденциальной информации в системах ИИ.
4.3	Уметь применять и анализировать законодательные нормы и требования в области ИИ на соответствие целям, политикам и мерам защиты корпораций.
4.4	Уметь проводить мониторинг и аудит производительности и эффективности систем ИИ в соответствии с принципами и стандартами обеспечения безопасности.
4.5	Уметь взаимодействовать и сотрудничать с заинтересованными лицами (специалисты по работе с данными, специалисты по надзору, клиенты и т. п.).

Отсюда вытекает необходимость эффективного правового регулирования процесса внедрения систем ИИ. Этому аспекту посвящены компетенции, перечисленные в табл. 5.

Таблица 5

Компетенции правового регулирования применения ИИ

Область применения компетенций	Безопасность применения ИИ:
№	Сущность необходимых компетенций
5.1	Владеть правовой и технической базой использования ИИ, включая инструментальные средства и практики применения данного инструментария.
5.2	Знать теорию и принципы разработки и использования ИИ с точки зрения этики и права.
5.3	Владеть навыками аналитического мышления для оценки и проработки решений по сложным социальным и этическим вопросам.
5.4	Владеть навыками коммуникации, уметь объяснять, и обосновывать ИИ-решения при взаимодействии с разными аудиториями.
5.5	Владеть навыками математической количественной оценки уровня необъективности и адекватности результатов работы ИИ.

В обществе активно обсуждаются этические проблемы внедрения ИИ. Компетенции, перечисленные в табл. 6, ориентированы именно на эту проблематику.

Таблица 6

Компетенции в области этики использования ИИ

Область применения компетенций	Безопасность применения ИИ:
№	Сущность необходимых компетенций
6.1	Владеть технологическим обеспечением использования ИИ и представлять его влияние на социум и личность.
6.2	Знать основы информационного права в области социальной инженерии этики использования ИИ, о правоприменительной практике в этом вопросе.
6.3	Владеть опытом применения ИИ с учётом специфики бизнеса и отраслей, социальных групп.

Продолжение табл. 6

Область применения компетенций	Безопасность применения ИИ:
№	Сущность необходимых компетенций
6.4	Владеть навыками коммуникации и уметь работать с разными организациями и социальными группами.
6.5	Уметь представлять и прогнозировать социальные последствия и возможности внедрения инноваций в области ИИ.

Революционное шествие ИИ-технологий остановить уже не представляется возможным. В этом контексте представляют теоретический и практический интерес компетенции, способствующие расширению внедрения ИИ. Они перечислены в табл. 7.

Таблица 7

Компетенции расширения использования ИИ

Область применения компетенций	Безопасность применения ИИ:
№	Сущность необходимых компетенций
7.1	Владеть опытом в области исследований пользовательского поведения и тестирования, построения обратной связи от пользователей с целью выявления их потребностей, предпочтений и опасений, в т.ч в области ИИ.
7.2	Уметь создавать типажи пользователей, макеты и прототипы для проектирования и реализации плана действий, в результате которого будет улучшен опыт взаимодействия с ИИ.
7.3	Знать принципы, владеть методами и инструментами проектной деятельности для создания комфортных, интуитивно понятных, доступных и удобных пользовательских интерфейсов ИИ.
7.4	Владеть инструментами дизайна, необходимыми для создания удобного внешнего вида продуктов ИИ.
7.5	Владеть языками программирования (HTML, CSS и JavaScript) для реализации надёжного продукта и совместной работы с разработчиками ИИ.

Продолжение табл. 7

Область применения компетенций	Безопасность применения ИИ:
№	Сущность необходимых компетенций
7.6	Знать концепции и инструменты ИИ для интеграции их функций и возможностей в интеллектуальный продукт.
7.7	Знать этические принципы применения инфотехнологий для реализации ответственного и справедливого использования ИИ в социуме.

Представленное в табл. 1-7 множество нейросетевых компетенций, разумеется, не претендует на абсолютную полноту и при необходимости может быть расширено. Однако ориентация на этот перечень (табл. 1-7) может быть весьма полезна в плане развития эффективности проектной деятельности в области создания защищённых АИС.

Заключение

В работе предпринята попытка формализации задач и компетенций нейросетевого проектирования защищённых АИС. По мнению авторов, это удалось осуществить в контексте целеполагания проектной деятельности по созданию организационно-правового и научно-технического обеспечения информационной безопасности АИС с использованием нейросетей, включая задачи, предмет и объект исследования. Наряду с этим формализованы компетенции, необходимые для успешного решения поставленных задач и получения ожидаемых результатов, обладающих необходимой новизной и практической ценностью, в контексте нейросетевой реализации проектирования. Перспектива развития результатов работы прежде всего видится в уточнении и освоении обозначенных компетенций проектировщиками защищённых АИС.

Список литературы

1. Эпидемии в телекоммуникационных сетях : монография / А.Г. Остапенко, Н.М. Радько, А.О. Калашников, О.А. Остапенко, З.К. Бабаджанов ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 1. М. : Горячая линия-Телеком, 2017. 282 с.

2. Атакуемые взвешенные сети : монография / А.Г. Остапенко, Д.Г. Плотников, А.О. Калашников, В.Б. Щербаков, Г.А. Остапенко ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 2. М. : Горячая линия-Телеком, 2017. 248 с.

3. Социальные сети и деструктивный контент : монография / А.Г. Остапенко, А.В. Паринов, А.О. Калашников, В.Б. Щербаков, А.А. Остапенко ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 3. М. : Горячая линия-Телеком, 2017. 274 с.

4. Социальные сети и риск-мониторинг : монография / А.Г. Остапенко, Е.Ю. Чапурин, А.О. Калашников, О.А. Остапенко, Г.А. Остапенко ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 4. М. : Горячая линия-Телеком, 2020. 266 с.

5. Социальные сети и психологическая безопасность : учеб. пособие для вузов / А.Г. Остапенко, Е.Б. Белов, А.О. Калашников, В.П. Лось, О.А. Остапенко ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 5. М. : Горячая линия-Телеком, 2021. 266 с.

6. Сетео-информационная эпидемиология : учеб. пособие для вузов / А.Г. Остапенко Е.Б. Белов, А.О. Калашников, В.П. Лось, А.А. Остапенко ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 6. М. : Горячая линия-Телеком, 2021. 216 с.

7. Картография защищаемого киберпространства / А.Г. Остапенко, А.Л.

Сердечный, А.О. Калашников ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 7. М. : Горячая линия-Телеком, 2023. 372 с.

8. Организационно-правовая защита сетей : монография /Г.А. Остапенко, Д.В. Щерабакова, А.О. Калашников и др.; под ред. акад. РАН Д.А. Новикова; серия «Теория сетевых войн»; вып. 8. М : Горячая линия – Телеком, 2023. 226 с.

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Поступила в редакцию 07.11.2023

Информация об авторах

Остапенко Григорий Александрович – д-р. техн. наук, профессор, проректор по цифровизации Финансового университета при Правительстве Российской Федерации, e-mail: ostg@mail.ru.

Васильченко Алексей Петрович – аспирант, Финансовый университет при Правительстве Российской Федерации, e-mail: rainichek@yandex.ru.

NEURAL NETWORK TASKS AND COMPETENCIES OF PROJECT ACTIVITY FOR CREATION OF SECURE AUTOMATED INFORMATION SYSTEMS

G.A. Ostapenko, A.P. Vasilchenko

The contradictions of the instrumental base of designing the attacked automated information systems (AIS) are considered. The objective necessity of using artificial neural networks in project activities as intellectual support for organizational, legal, scientific and technical management decisions on information security in AIS is substantiated. The goal-setting of the research is carried out in the conditions of a steadily growing variety of computer attacks and the revolutionary development of artificial intelligence. The tasks and expected results are formulated, as well as the neural network competencies necessary for their achievement, the formation and development of which seems to be an urgent condition for the success of research and development in the field of intellectualization of created and operated AIS.

Keywords: neural networks, automated information systems, computer attacks, competencies.

Submitted 07.11.2023

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Professor, Vice-Rector for digitalization of the Financial University under the Government of the Russian Federation, e-mail: ostg@mail.ru.

Aleksey P. Vasilchenko – graduate student, Financial University under the Government of the Russian Federation, e-mail: rainichek@yandex.ru.