DOI 10.36622/VSTU.2023.26.3.014
УДК 004.056

ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ: НАУЧНО-МЕТОДИЧЕСКОЕ РАЗВИТИЕ В НАПРАВЛЕНИИ ВНЕДРЕНИЯ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ОРГАНИЗАЦИОННО-ПРАВОВОЙ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ

А.Г. Остапенко, Д.В. Щербакова, А.А. Остапенко, Д.А. Нархов

Рассматривается целеполагание проектной деятельности, реализуемой на основе искусственных нейросетей. Описываются задачи и модули подобной реализации, её нормативного обеспечения. Для создания информационного обеспечения нейросети предлагаются таблицы, формирующие базу знаний по организационно-правовому обеспечению (частные политики, регламенты и инструкции безопасности) защиты корпоративных сетей. Также вниманию студентов предлагаются варианты заданий для широкого многообразия компьютерных атак, для которых требуется разрабатывать необходимые политики, регламенты и инструкции. В случае регистрации одной из них, нейросеть выдает администратору корпоративной сети интеллектуальную подсказку по эффективному противодействию вторжению. Машинное обучение нейросети будет повышать точность её решений по мере эксплуатации средств искусственного интеллекта.

Ключевые слова: искусственный интеллект, безопасность, атаки, организационно-правовая защита, проектная деятельность.

Введение

Трудно переоценить значение проектной деятельности при подготовке специалистов по защите информации. Её практическая направленность и проблемная ориентация обеспечивают значительное повышение качества подготовки таких выпускников. Поэтому разработка научно-методического обеспечения является весьма актуальной задачей специальности. Особенно насущными представляются целеполагание и структурирование проектной деятельности в сфере сетевого противоборства [1-7] в отношении борьбы с информационными эпидемиями [1,6], деструктивными контентами [3-5] и другими кибервредоносами [7]. В этом контексте уместно обратиться к самым современным средствам обеспечения информационной безопасности, коими сегодня следует считать системы искусственного интеллекта, где генеративные нейросети открывают большие перспективы эффективной технической и организационно-правовой защиты информации в сетевых структурах. Здесь проектную деятельность следует ориентировать на исследование многообразия кибератак.

Объекты исследования

На основании вышеизложенного для студентов предлагаются задания, ориентированные на нижеследующие компьютерные атаки (табл.1).

Приведенные в табл. 1 атаки лежат в основе нейросетевой реализации проектной деятельности.

Нейросетевая реализация

Представляется возможным обобщенно сформулировать целеполагание проектной деятельности в плане создания перспективной организационно-правовой защиты корпоративных сетей.

Здесь основой служит системное противоречие между наличием устойчивой тенденции неуклонного роста многообразия уязвимостей и векторов (сценариев) атак, порождающих обилие мер и частных регламентов защиты корпоративных сетей, и отсутствием автоматизированного инструментария интеллектуальной поддержки проектных решений сетевых администраторов в их информационном противоборстве со злоумышленниками.

Причем объектом исследования подвергающаяся внешним и внутренним выступает корпоративная сеть, через ее атакам.
уязвимости по различным сценариям

Таблица 1

Многообразие компьютерных атак

Наименование атаки	CAPEC- идентификатор атаки
Подмена при взаимодействии	
Подмена контрольной суммы	145
Намеренная подделка	502
Повторная привязка DNS	275
Поддельные веб-сайты	543
Подмена DNS	598
Злоупотребление функционалом	
TCP Flood	482
UDP-флуд	486
ICMP-флуд	487
HTTP-флуд	488
Перехват JSON	111
Манипулирование структурами данных	
Переполнение буфера через переменные среды	10
Сбой фильтра из-за переполнения буфера	24
Переполнение массива SOAP	256
Переполнение двоичного файла ресурсов	44
Переполнение буфера из-за расширения параметров	47
Переполнение буфера при вызове API	8
Обход относительного пути	139
Абсолютный обход пути	597
Принудительное переполнение целого числа	92
Использование кодировки UTF-8 для обхода логики проверки	80

Продолжение табл. 1

Наименование атаки	CAPEC-идентификатор атаки
Манипулирование ресурсами	
Загрузка вредоносного программного обеспечения	185
Вредоносное автоматическое обновление программного обеспечения с помощью перенаправления	187
Вредоносное обновление программного обеспечения вручную	533
Вредоносное автоматическое обновление программного обеспечения с помощью подмены	657
Изменение обновления программного обеспечения	669
Противоречивые направления в схемах маршрутизации трафика	481
Инъекции	
Использование метасимволов в заголовках электронных писем для внедрения вредоносных полезных данных	41
Загрязнение параметров HTTP	460
Внедрение локального файла PHP	252
Внедрение команд IMAP / SMTP	183
Выполнение командной строки с помощью SQL-инъекции	108
Расширение контроля над операционной системой из базы данных	470
Анализ целевого объекта	
Обнаружение неопубликованных веб-страниц	143
Сбор данных из буфера обмена	637
Прослушивание сетевого трафика	158
Проверка эхо-запроса ICMP	285
Нарушение авторизации или аутентификации	
Фальсификация учетных данных сеанса посредством манипуляций	226
Межсайтовая идентификация	467
Принудительное использование поврежденных файлов	263

Отсюда предметом исследования является регламентация деятельности корпоративной сети на стадиях обнаружения инцидента и идентификации разновидности вторжения, реагирования на инцидент нарушения безопасности и ликвидации его последствий путем автоматизированной интеллектуальной поддержки управленческих решений администратора в ходе сетевого противоборства со злоумышленниками.

Тогда цель исследования состоит в создании информационного, методического и программного обеспечения для инструментария интеллектуальной поддержки программно-технической и организационно-правовой защиты корпоративных сетей. Для достижения поставленной цели необходимо решать следующие задачи:

1. Для существующих разновидностей сетевых атак формирование риск-ландшафтов, где третьим измерением выступает риск их успешности в привязке к плоскости пар «вектор атаки – используемая им уязвимость» с ранжированием элементов поверхности ландшафта по вышеуказанному риску.

2. Выработка методических рекомендаций противодействия в виде мер и регламентов: обнаружения и регистрации инцидентов; реагирования на инциденты; ликвидации их последствий для всевозможных пар «вектор – уязвимость» существующих разновидностей сетевых атак, включая формирование из них баз знаний в качестве информационного обеспечения создаваемого инструментария.

3. Автоматизация процесса регистрации инцидента и идентификации «пар», лежащих в его основе, на базе машинного обучения и сформированных баз знаний.

4. С использованием нейроподобных сетей и накопленных в ходе машинного их обучения знаний о программно-технической и организационно-правовой защите корпоративных сетей, автоматизация интеллектуальной поддержки для лиц, принимающих решения в ходе сетевого противоборства.

5. Удобная (возможно, картографическая) визуализация проектной ситуации (в реальном масштабе времени), включая дообучение нейросети по результатам внедрения принятых регламентных мер защиты корпоративной сети.

6. Отладка разработанного программно-технического комплекса на реальных задачах сетевого противоборства, включая оценку эффективности созданного инструментария.

7. Публичная презентация инструментария и подготовка заявок на конкурсы и патенты, проектов публикаций, отражающих новизну и практическую ценность реализованного инструментария в области обеспечения информационной безопасности корпоративных сетей.

Вышеизложенное иллюстрирует рис. 1, где выделены следующие модули.

1. Модуль обнаружения сетевых вторжений, включая идентификацию векторов атаки, используемых уязвимостей.

2. Модуль риск-анализа, включая измерения вероятности успеха вторжения и ожидаемого ущерба на основе текущих статистических данных из соответствующих информационных источников.

3. Модуль формирования мер противодействия сетевым вторжениям на уровне частных регламентов обнаружения и регистрации инцидентов, реагирования на них, ликвидации последствий.

4. Модуль машинного обучения нейросети мерам противодействия сетевым вторжениям.

5. Модуль генерации регламентирования мер противодействия сетевым вторжениям.

6. Модуль выработки рекомендаций для корректировки частной политики и инструкций обеспечения сетевой безопасности.

7. Модуль интегрирования и визуализации результатов работы вышеуказанных программно-технических решений.

При этом нормативной основой проектирования должны быть источники:

1. Сценарии реализации атак целесообразно описывать в тактиках и техниках из MITRE ATT&CK и из Перечня основных тактик и соответствующих им типовых техник ФСТЭК России.

2. Уязвимости следует выбирать из БДУ ФСТЭК и (или) NVD NIST.

3. Для атак целесообразно явно описывать индикаторы компрометации и индикаторы атаки.

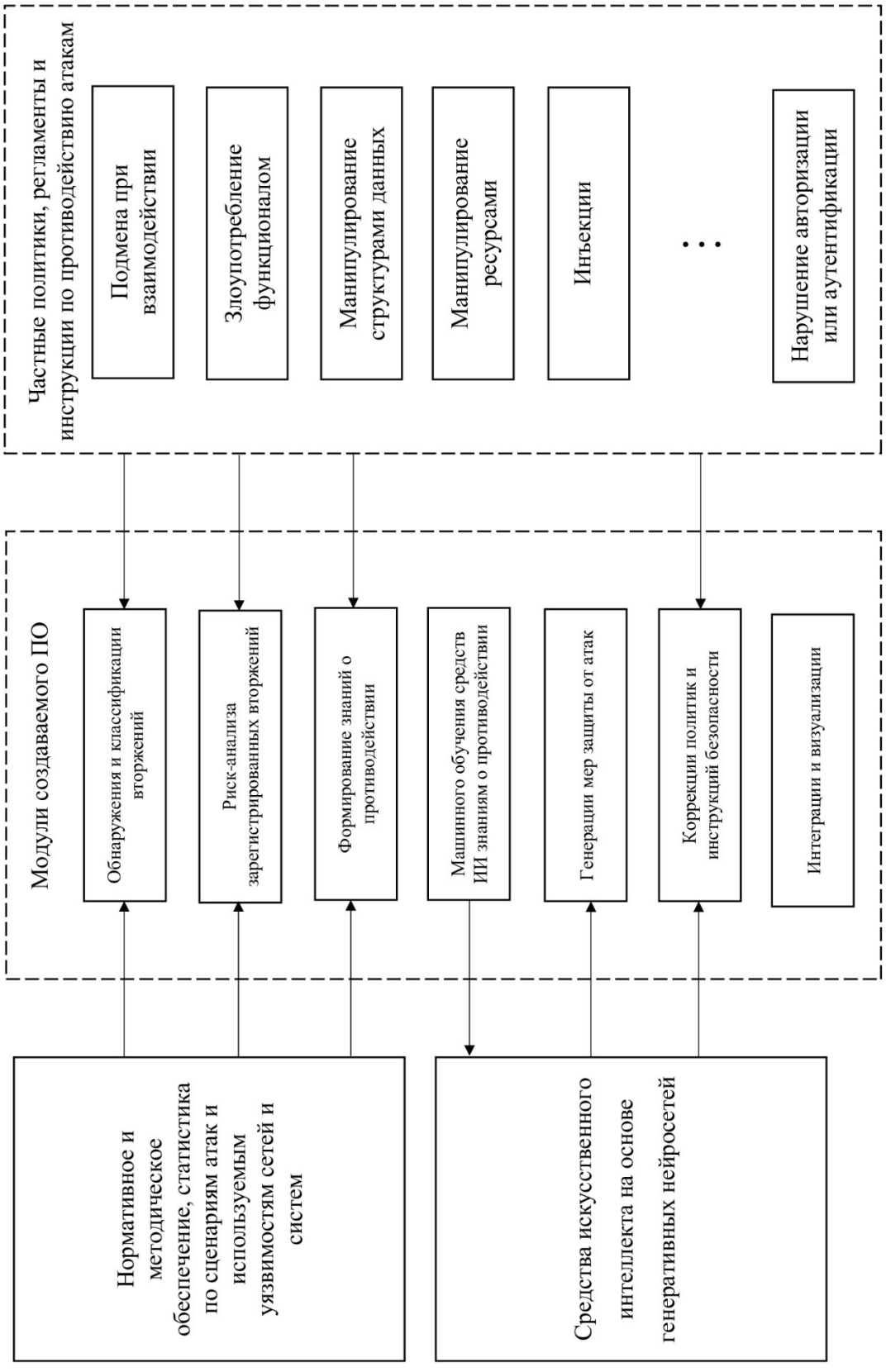

Рис. 1. Схема «командного» комплексного проектирования

Информационное обеспечение нейросетевой реализации

Для работы нейросети предлагается (применительно к каждой разновидности кибератаки) сформировать базу знаний в виде следующих таблиц (табл. 2-6).

Таблица 2

Таблица соответствия действий злоумышленника и меры противодействия им в рамках частной политики обеспечения безопасности при реализации сетевой атаки

Последовательность и содержание действий злоумышленника в целях реализации сценариев атак типа «…»	Меры защиты Организации от сетевой атаки типа «…», адекватные действиям злоумышленника по каждому сценарию
…	…

Таблица 3

Таблица соответствия действий злоумышленника и мер регламентации защиты корпоративной сети на стадии «Обнаружения и регистрации инцидентов безопасности при реализации сетевой атаки»

Тип инцидента, который может возникнуть при реализации атаки	Описание инцидента	Средства для обнаружения заданного типа инцидента
…	…	

Таблица 4

Таблица соответствия действий злоумышленника и мер регламентации защиты корпоративной сети на стадии «Реагирование на инциденты безопасности при реализации сетевой атаки»

Произошедший инцидент, в ходе реализации атаки	Первоочередные меры по предотвращению инцидента	Негативные последствия, вызванные инцидентом безопасности
…	…	

Таблица 5

Таблица соответствия действий злоумышленника и мер регламентации защиты корпоративной сети на стадии «Ликвидация последствий инцидента безопасности при реализации сетевой атаки»

Негативные последствия, вызванные инцидентом безопасности	Меры по устранению инцидента
…	…

Таблица 6

Таблица соответствия умений и знаний администратора безопасности при защите от сетевой атаки

Функциональные знания администратора, которыми он должен обладать, чтобы успешно защитить сеть Организации	Требования к умениям администратора, которыми он должен владеть, чтобы успешно защищать сеть Организации
…	…

Заключение

Рассматривая проектную деятельность студентов [1-7] как одну из важнейших форм практических и проблемно-ориентированных разработок, предваряющих дипломное проектирование и служащих основой для создания творческих бригад, предполагается подключить для консалтинга аспирантов кафедры, успешно проявивших себя в рамках кибердружины,

имеющих весомые публикации, именных стипендиатов во время обучения в вузе. Задача данных консультантов будет заключаться в следующем:

- актуальная персонификация проектных заданий;
- календарное планирование текущих результатов проектирования и организация по ним студенческих научно-технических конференций;
- формирование среди проектантов творческих бригад и подключение к научному руководству ими ведущих профессоров и доцентов кафедры;
- обеспечение публикационной активности творческих бригад в изданиях кафедры;
- формирование для проектантов горизонтов тематики последующих производственных практик и дипломного проектирования;
- активное внедрение в проектирование средств искусственного интеллекта;
- установление тесной связи с вероятными работодателями с целью актуализации тематики проектирования и привлечения студентов для работы по совместительству на региональных предприятиях (по тематике проектирования).

Список литературы

1. Эпидемии в телекоммуникационных сетях / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 1).

2. Атакуемые взвешенные сети / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Сер. «Теория сетевых войн»; вып. 2).

3. Социальные сети и деструктивный контент / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Сер. «Теория сетевых войн»; вып. 3).

4. Социальные сети и риск-мониторинг / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2019. – 284 с. (Сер. «Теория сетевых войн»; вып. 4).

5. Социальные сети и психологическая безопасность / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2020. – 284 с. (Сер. «Теория сетевых войн»; вып. 5).

6. Сетео-информационная эпидемиология / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2021. – 284 с. (Сер. «Теория сетевых войн»; вып. 6).

7. Картография защищаемого киберпространства / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2022. – 372 с. (Сер. «Теория сетевых войн»; вып. 7).

Воронежский государственный технический университет
Voronezh State Technical University

Московский государственный университет
Moscow State University

Поступила в редакцию 20.09.2023

Информация об авторах

Остапенко Александр Григорьевич – д-р техн. наук, заведующий кафедрой, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Щербакова Дарья Владимировна – аспирант, Московский государственный университет, e-mail: alexanderostapenkoias@gmail.com

Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Нархов Дмитрий Андреевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

PROJECT ACTIVITIES: SCIENTIFIC AND METHODOLOGICAL DEVELOPMENT IN THE DIRECTION OF THE INTRODUCTION OF ARTIFICIAL INTELLIGENCE TOOLS TO ENSURE ORGANIZATIONAL AND LEGAL PROTECTION OF CORPORATE NETWORKS

A.G. Ostapenko, D.V. Shcherbakova, A.A. Ostapenko, D.A. Narhov

The goal-setting of project activities implemented on the basis of artificial neural networks is considered. The tasks and modules of such implementation, its normative support are described. To create information support for neural networks, tables are proposed that form a knowledge base on organizational and legal support (private policies, regulations and security instructions) for the protection of corporate networks. Also, students are offered options for tasks for a wide variety of computer attacks, for which it is required to develop the necessary policies, regulations and instructions. In case of registration of one of them, the neural network gives the administrator of the corporate network an intelligent hint on effective counteraction to intrusion. Machine learning of a neural network will increase the accuracy of its decisions as artificial intelligence tools are used.

Keywords: artificial intelligence, security, attacks, organizational and legal protection, project activity.

Submitted 20.09.2023

Information about the authors

Alexander G. Ostapenko – Dr. Sc. (Technical), Head of the Department, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Darya V. Shcherbakova – graduate student, Moscow State University, e-mail: alexanderostapenkoias@gmail.com

Alexander A. Ostapenko – graduate student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Dmitry A. Narhov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com