DOI 10.36622/1682-7813.2024.27.3.005
УДК 004.056

ИСПОЛЬЗОВАНИЕ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ХОДЕ ИССЛЕДОВАТЕЛЬСКОГО И УЧЕБНОГО ПРОЦЕССОВ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Г.А. Остапенко, А.О. Калашников, А.Г. Остапенко, Е.А. Москалева, Д.О. Карпеев, О.В. Поздышева, Ю.В. Макаров

В статье обсуждается актуальная тема формирования компетенций по использованию технологий искусственного интеллекта и нейросетевых инструментов при подготовке специалистов по защите информации. В результате совместного проекта Финансового университета при Правительстве Российской Федерации Института проблем управления РАН и Воронежского государственного технического университета были выработаны практико-ориентированные составляющие учебного процесса. В учебный процесс включены вопросы построения риск-ланшафтов и атласа компьютерных кибератак и уязвимостей для обеспечения безопасности информационных систем и сетей, разработки модулей: агрегирования и риск-анализа данных киберинцидентов; базы знаний и машинного обучения по мерам противодействия кибератакам; выработки интеллектуальных подсказок лицу, принимающему решения, регламентов реагирования и ликвидации последствий в отношении компьютерных инцидентов. Эти вопросы реализовываются в вузовском учебном процессе в ходе проектной деятельности и практик.

Ключевые слова: защита информации, атлас кибератак, нейросеть, риск-анализ, информационная безопасность, проектная деятельность.

Введение

Специалисты по защите информации должны идти в ногу со временем и реагировать на изменения существующих и внедрения новых информационных технологий, ресурсов, инструментов. Для этого подготовка специалистов по защите информации предусматривает соответствующие компетенции. Уже в процессе обучения студент должен уметь осваивать и применять в своей деятельности любые программные и автоматизированные инструменты, каким-либо образом относящийся к информационной безопасности. В настоящее время особую актуальность приобрели навыки работы с нейросетевыми инструментами и технологиями искусственного интеллекта. Причем использование этих инструментов и технологий не подразумевает генерацию текстов для курсовых, дипломных и других квалификационных работ, а впоследствии регламентов, инструкций и других технических документов. Здесь имеется ввиду использование нейросетевых инструментов для повышения эффективности профессиональной деятельности в плане сбора и обработки информации об атаках, уязвимостях, угрозах. То есть они должны облегчать процесс сбора нужной информации, ее систематизации, визуализации, составления баз данных. Получить навыки применения подобных инструментов студент может во время обучения при разработке курсовых работ и проектов, в рамках дисциплины «Проектная деятельность». И наконец продемонстрировать полученные компетенции при подготовке выпускной квалификационной работы.

Важным моментом при этом является вовлечение студентов в процесс создания и модернизации средств проектирования с целью внедрения в имеющийся инструментарий технологий искусственного интеллекта. В итоге студенты приобретают компетенции разработки программных средств и программно-аппаратных комплексов, используя технологии искусственного интеллекта для сбора

актуальных данных, формирования баз данных, машинного обучения нейросети, использования интеллектуальных подсказок и т. п.

В настоящей статье авторы делятся опытом работы на кафедрах информационной безопасности по формированию вышеуказанных компетенций.

Проект по созданию атласа кибератак

Финансовый университет при правительстве Российской Федерации, Институт проблем управления РАН и Воронежский государственный технический университет (ВГТУ) объединили свои усилия для решения описанной выше задачи [1, 2]. С этой целью был реализован проект по созданию атласа кибератак.

Изначально планировалось осуществить сбор и систематизацию данных о кибератаках и эксплуатируемых уязвимостях [3]. В первую очередь это требовалось в качестве методических материалов для подготовки выпускных квалификационных работ. Для удобства и наглядности методические материалы были разработаны в виде таблиц, которые упрощали студентам и аспирантам выбор направления деятельности, ознакомление с имеющимися наработками по выбранной тематике, формирование цели работы и разработку задач проектирования [3]. Старшекурсники и аспиранты активно подключились к решению поставленных задач. Анализировались технологии генерации видео, аудио и графического контентов социальных сетей. Разрабатывались алгоритмы и программные средства риск-анализа активности пользователей социальных сетей. Проводились исследования по выявлению deepfake и разработка соответствующего инструментария. Была проведена работа по выявлению и регулированию рисков девиантного поведения сотрудников с помощью систем видеонаблюдения и распознавания и создан инструментарий. В ходе работы вскрылись дополнительные проблемы, как например [4]:

- неполнота и разнородность существующих баз данных?
- некорректное объединение ущербов, рассчитываемых для оценки нарушения конфиденциальности, целостности и доступности (это сложная задача в связи с разной сущностью объединяемых данных),
- отсутствие возможности введения в расчет рисков дополнительных параметров, учитывающих ценность информации,
- неразборчивость в ситуациях полной и частичной потери функциональности атакуемой системы,
- местами некорректное использование математического аппарата для расчета метрик и факторов нарушения конфиденциальности, целостности, доступности.

В рамках проектной и научной работы студентов и аспирантов была расширена номенклатура сведений и характеристик кибератак [5], были разработаны алгоритмы и инструменты автоматизации парсинга, базы данных уязвимостей и атак, описания и базы данных векторов «атака-уязвимость» [2, 5], модули автоматизированного инструментария.

Мультиразмерность собираемых и генерируемых сведений потребовала применения средств искусственного интеллекта [6]. В результате проект получил больший масштаб и был перенесен в проектную плоскость учебного процесса. Это позволило, с одной стороны, решать поставленные задачи, с другой – расширить учебные задачи в соответствии с современными технологиями, которые могут облегчить, ускорить разработку средств защиты информации и повысить их эффективность.

Были проработаны вопросы повышения эффективности средств противодействия кибератакам с помощью использования средств искусственного интеллекта. Разработанный нейросетевой модуль [6] представляет эффективный сервис автоматизированного противодействия кибератакам с интеллектуальной адаптацией к изменяющимся угрозам.

В настоящее время работа по созданию атласа кибератак продолжается. К примеру, на уровне кафедры систем информационной

безопасности ВГТУ организационно-правовая составляющая интеллектуализации учебного процесса видится в следующем.

1. Популяризация нейросетей за счет сбора сведений о них и рассылки таковых преподавателям и студентам, проведение мастер-классов.

2. Создание профессиональных баз знаний и данных по специальностям кафедры как основы для систематического машинного обучения нейросетей.

3. Формирование интеллектуального атласа кибератак и его развитие в соответствии с трендами сфер информационной безопасности и искусственного интеллекта.

4. Ориентация курсового и дипломного проектирования кафедры на вышеперечисленные инструменты с соответствующей модернизацией рабочих программ и заданий для студентов.

5. Организация повышения квалификации преподавателей кафедры в сфере искусственного интеллекта в соответствии с перечнем, предусматривающим первоначально полностью или частично бесплатное обучение по столичным программам.

6. Формирование на каждом курсе рабочих групп студентов с углубленными компетенциями в вопросах пользования нейросетями и распространение этого опыта среди начинающих.

7. Использование глобальных нейросетей при подготовке обзоров информационных источников для отчетов по практикам, курсовым и дипломным работам.

8. В рамках эффективного контракта подготовка совместно со студентами материалов по нейросетевой тематике для участия в конкурсах, научно-технических конференциях и выставках.

9. Обеспечение необходимой публикационной активности преподавателей, аспирантов и студентов кафедры в сфере искусственного интеллекта, включая издание монографий и учебных пособий, а также научных статей по тематике использования нейросетевого инструментария в задачах обеспечения информационной безопасности.

10. Ориентация аспирантских планов, производственных практик и профориентационной работы кафедры на перспективы широкого и эффективного использования нейросетевых технологий будущими специалистами по защите информации.

11. Развитие партнерских связей с РАН и вузами страны по программе нейросетевого обеспечения кибербезопасности, включая модернизацию специализированной нейросети коллективного дистанционного пользования для учебных целей и проектной деятельности.

12. Синхронизация настоящего проекта с планами ректората ВГТУ и партнеров.

Создание сервисов риск-анализа студентами в учебном процессе

Работа по использованию технологий искусственного интеллекта в интересах информационной безопасности привлекла внимание студентов и аспирантов, увидевших дальнейшие перспективы использования и развития разработанного нейросетевого модуля. Были объединены результаты исследований многообразия кибератак, их систематизации, успешности их воздействия на информационные системы и сети [4]. В результате был выработан новый подход к риск-анализу информационных сетей [7], базирующийся на выявлении наиболее опасных пар «вектор атаки-уязвимость» и построении по ним риск-ландшафта сетевых атак с использованием нейросетевого модуля.

Это позволило задать направление совершенствования организационно-правового обеспечения информационной безопасности и формализовать задачу формирования политик, регламентов и инструкций информационной безопасности [7].

Для реализации формального описания [7] была предложена нейросетевая реализация сервиса противодействия кибератакам [6]. В том случае, когда вид вектора атаки удалось идентифицировать и нам понятно множество уязвимостей, ей

соответствующих, представляется возможным обратиться к аккумулированным (с помощью модуля агрегирования) знаниям, положенным в основу машинного обучения нейросети. При этом сервис имеет возможность автоматизировано выполнять вышеуказанное исследование с учетом ценности защищаемой информации, а также в случаях одновременного использования нескольких уязвимостей атакуемого объекта. Практическая значимость модуля в том, что получаемые результаты риск-анализа служат основой для выработки политик, регламентов и инструкций информационной безопасности защищаемых предприятий, в том числе и предприятий и организаций критический информационной инфраструктуры (КИИ), где требования защищенности используемых ресурсов особенно высоки.

Предлагаемый в [6] инструментарий был успешно освоен нашими студентами в ходе разработки курсовых проектов, проектной и преддипломной практик. Таким образом, студенты приобретают компетенции оценки и регулирования рисков при помощи автоматизированных средств, использующих искусственный интеллект и разработки таких средств для будущей профессиональной деятельности.

Архитектурные решения для подобного инструментария состоят в следующем [6]:

1. Прежде всего необходима база знаний и данных о компьютерных атаках и уязвимостях. Здесь подспорьем выступает описанный выше модуль автоматизированного парсинга и аккумуляции данных из баз открытого доступа. В целях эффективного хранения и доступа, данные сведения подлежали форматированию согласно этапности реализации кибератак, предложенному в MITRE ATT&CK. Удобство оперирования информацией достигается соблюдением взаимно однозначного соответствия каждому этапу атаки по компонентам противодействия [2].

Пары «вектор атаки-уязвимость» генерируются модулем агрегирования и риск-анализа с использованием баз CAPEC и БДУ.

2. Сформированная база знаний и данных служит основой для машинного обучения нейросети. Пори этом сохраняется возможность дообучения с использованием текущих наработок по противодействию, догружаемых в базу.

3. В отношении используемой нейросети было решено отказаться от глобальных нейросетевых структур, обученных плохо по кибербезопасности и зачастую платных. К тому же, насыщение их собственным опытом противодействия кибератакам с неисключенной возможностью последующей утраты доступа к собранным знаниям, представляется весьма опрометчивым решением и довольно затратным удовольствием.

Поэтому для атласа на консолидированных ресурсах партнеров проекта была развернута и обучена подконтрольная нейросеть (подобно «ИИ в коробке»), в дистанционном режиме обеспечивающая доступ пользователей партнерствующих организаций к возможностям автоматизированной генерации интеллектуальных подсказок администратору безопасности для регламентации реагирования и ликвидации последствий в отношении компьютерных инцидентов, выявляемых и регистрируемых в защищаемой системе или сети. Оперативность нейросетевого исполнения запросов в данном случае является важнейшим фактором успешности не только защиты в реальном противоборстве, но и практико-ориентированности подготовки будущих специалистов по защите информации.

Дистанционный доступ к нейросетевому модулю открывает широкие возможности для его использования в курсовом и дипломном проектировании, а также в ходе производственных практик, в том числе на предприятиях и в организациях КИИ. При этом удается значительно (в разы) сократить трудозатраты студентов-разработчиков и проверяющих их результаты преподавателей. Это особенно актуально для сохранения качества обучения при увеличившейся нагрузке на преподавателей вследствие увеличения численности студентов в группах.

Разработанный инструментарий имеет практическую значимость, поскольку дает возможность настройки программно-технических модулей, применяемых для предотвращения вторжений и минимизации рисков автоматизированных информационных и телекоммуникационных сетей. Применение нейросетей повышает эффективность администрирования в контексте обеспечения информационной безопасности.

Привлечение профильных предприятий к сотрудничеству с образовательными организациями

Сотрудничество вузов с базовыми профильными организациями обеспечивает обоюдную выгоду. В рамках производственных практик, выполнения курсовых и дипломных проектов по заказам данных организаций, вполне возможен синергетический эффект совместного применения профессиональных и нейросетевых компетенций, значительно повышающий качество подготовки специалистов и конкурентоспособность практикующего такую работу вуза. В результате вузы выпускают востребованных специалистов, а предприятия получают помощь в разработке программных средств, программно-аппаратных комплексов, повышая тем самым эффективность производственного процесса. Темпы и масштабы нынешней ИИ-революции неотвратимо требуют этого, особенно в современных условиях реализации «цунами кибератак», систематически обрушающихся на КИИ и другие отечественные объекты информатизации.

В этой связи отметим некоторые важные для специалиста по информационной безопасности компетенции, которые могут формироваться в ходе производственных практик. При этом предприятие получает содействие научных кадров вуза и рабочие руки и пытливый ум молодого специалиста. К таким компетенциям можно отнести:

1. Знание и умение работать со средствами и приложениями искусственного интеллекта.
2. Знание стандартов и нормативных документов.
3. Умение формировать политики, регламенты и инструкции по защите от угроз с использованием инструментов искусственного интеллекта в части аналитики данных об угрозах.
4. Умение оценивать защищенность данных, выявлять риски, проводить риск-анализ.
5. Умение управлять рисками и шансами.
6. Умение осуществлять мониторинг с применением автоматизированных средств.

В ходе научной деятельности студентов были разработаны инструментарии автоматизированного риск-анализа для корпораций. Разработанный программно-технический комплекс по выявлению deepfake с помощью парсеров собирает данные из социальных сетей об активности работников корпорации. Анализ видео контента проводится с применением нейросети. Модуль интеллектуальных подсказок облегчает анализ, формируя рекомендации по снижению риска. Анализ аудиоконтента проводится по параметрам, учитывающим техническое состояние аудиозаписи и эмоциональное состояние пользователя. Здесь нейросеть используется для оценки эмоций. Анализ графического контента также использует нейронные сети. По результатам расчетов риска происходит информирование оператора. Инструментарий автоматизированного выявления и регулирования рисков девиантного поведения сотрудников корпорации производит анализ по совокупности психоэмоциональных характеристик, обнаружение опасных субъектов, представляющих угрозу, и распознавание субъектов, находящихся в неадекватном состоянии. Здесь нейросеть используется для распознавания эмоций. В результате могут быть выданы соответствующие рекомендации администрации (руководству) корпорации.

Подобные исследования выдают инструменты для снижения рисков утечки данных с предприятий путем выявления персонала, которому нежелательно давать допуск с конфиденциальной, критической

или секретной информации; выявлением персонала, которому необходима психологическая помощь вследствие стресса и т. п.

Конечно, круг задач исследований должен быть расширен в интересах предприятий, что должно определяться в совместной работе с вузом.

Распределение проектной деятельности студентов и аспирантов по учебному плану

В практическом плане авторы сконцентрировали свое внимание на формировании нейросетевых компетенций в области противодействия кибератакам [6].

Выпускная квалификационная работа представляет собой серьезный научный труд, показывающий в то же время профессиональные компетенции студента/аспиранта. Подготовка квалификационной работы может (и должна) начинаться не с началом преддипломной практики, а объединять все усилия и наработки по ходу учебы в вузе. Таким образом, должен осуществляться междисциплинарный подход в ходе всего обчения к планированию научно-исследовательских работ студентов.

Уже со второго учебного семестра при выполнении курсовой работы по дисциплине «Введение в специальность» предполагается задание, включающее поиск соответствия между идентифицированными видами атак и уязвимостями, которые они могут проэксплуатировать при вторжении [4, 5]. Далее проектант обязан рассчитать вероятности успеха единичной атаки для каждой установленной (на предыдущем этапе) пары «вид атаки-уязвимость» [4], что позволит построить соответствующие гистограммы риска, который представляется возможным оптимизировать по своему значению с использованием нейросетевых технологий. Данный учебный этап представляет собой некоторую репетицию для отработки последующего организационно-правового противодействия кибератакам на старших курсах.

В частности, на третьем и четвертом курсах в рамках дисциплины «Проектная деятельность» реализуемый здесь практикум позволяет для установленных пар «вид атаки-эксплуатируемая уязвимость» с помощью обученной нейросети формировать регламенты реагирования и ликвидации последствий вторжения [6]. В рамках курсовых проектов по другим дисциплинам, как например, «Языки программирования», «Базы данных» и т. д. могут разрабатывать подзадачи, ведущие к глобальной цели.

В свою очередь преддипломная практика (пятый и шестой курсы) ориентирована на рассмотрение множественных атак и построение риск-ландшафта для совокупности вышеупомянутых пар, в том числе и автоматизированно выявленных кибератак [7], где нейросети позволяют выяснить причинно-следственные связи факторов риска (оценив их чувствительность) и обеспечить рутинный многовариантный вероятностный анализ.

Следует заметить, что обучение будущих специалистов по защите информации синхронизируется с аспирантской программой по специальности «Методы и системы защиты информации, информационная безопасность», где аспиранты активно вовлекаются в студенческий учебный процесс со своей тематикой, а задания формируются и контролируются с учетом приобретения нейросетевых компетенций и совместной публикационной активности (в отношении полученных результатов) в научном журнале «Информация и безопасность» и сборнике научных трудов «Управление информационными рисками инфо-телекоммуикационных систем», издаваемых кафедрой систем информационной безопасности Воронежского государственного технического университета.

На основании вышеизложенного можно заключить, что уже в начале обучения студент должен выбрать направление научной деятельности, сформулировать глобальную цель исследований (целеполагание научных исследований) и в рамках этого направления планировать дальнейшую научную исследовательскую деятельность, формируя подцели на конкретные задачи. Удобнее всего составить таблицу, как например, табл. 1.

Таблица 1

Целеполагание научных исследований по теме «...»

Выявлены противоречия между	Задачи	Предполагаемые результаты	Новизна	Практическая ценность	Теоретическая ценность

В рамках дисциплины «Введение в специальность» может быть выбрано направление исследований, по которому студент будет продолжать двигаться и в рамках других дисциплин, «по кирпичикам» складывая разные стороны глобального проекта, который впоследствии перерастет в выпускную квалификационную работу.

К примеру, если студент выбирает исследование, посвященное анализу сетевых атак, то примерная тема «Разработка инструментария противодействия сетевым атакам класса ... в ... системах». Выявлены противоречия между необходимостью классификации таких атак по типам уязвимостей в сетевом пространстве и отсутствием такого рода классификации. Задачи: установление соответствия между атаками рассматриваемого класса и известными уязвимостями защищаемых систем, описание сценариев атак, разработка регламентов защиты. Предполагаемые результаты: разработка графовых моделей атак с ребрами-атаками и вершинами-уязвимостями, проработка сценариев атак на полученной модели, разработка автоматизированного модуля расчета риск-ландшафта рассматриваемого класса атак на рассматриваемую систему, формулирование регламентов по информационной защите системы. Новизна: в отличие от аналогов предложены ... метрики для систематизации пар «атака-уязвимость». Практическая значимость: разработка графа ... атак на ... систему, разработка автоматизированного средства расчета рисков и построения риск-ландшафта ... атак. Теоретическая значимость: масштабируемость представленной модели, применимость для проведения риск-анализа и последующей разработки регламентов по информационной безопасности системы. В курсовом проекте по дисциплине «Введение в специальность» разработать основу исследования, рассмотреть и систематизировать атаки. В курсовом проекте по дисциплине «Языки программирования» написать модель воздействия атаки на систему, описав их в виде классов. В курсовом проектировании по «Базам данных» создать базу данных пар «вектор атаки-уязвимость». И т. д. Курсовые работы и проекты по дисциплинам проводятся в зависимости от специальности и учебного плана. Но в любом случае можно выбрать траекторию движения к общей цели, согласовав с преподавателями тему, одновременно соответствующую и дисциплине и выбранному научному исследованию.

В процессе учебы эта матрица может дополняться, конкретизироваться. Однако общая цель, как было отмечено выше, не должна меняться. Все исследования должны быть направлены на приближение к ней.

В порядке практической иллюстрации методики, продемонстрированной в табл. 1, предлагается вариант построения матрицы целеполагания для исследований множественных кибератак (табл. 2).

Таблица 2

Вариант матрицы целеполагания исследований множественных кибератак

№	Противоречия между:	Задачи исследования	Результаты исследования	Новизна результатов	Практическая ценность результатов	Теоретическая ценность результатов
1	Объективной потребностью установления соответствия элементов множества рассматриваемого класса атак и уязвимостей и отсутствием таковых в проектном пространстве обеспечения безопасности защищенных … систем	Установление полного соответствия между … атаками и уязвимостями … защищаемых … систем, включая их сценарное описание и паспортизацию вредоносов	Лес древовидных графов с корнями в виде … атак и вершинами в качестве уязвимостей … защищаемых … систем, дополненный сценариями и паспортами средств вторжения	Исключительно для … атак впервые предложена графовая локализация, иллюстрирующая корреляцию их с уязвимостями … защищаемых … систем	Роща графов-деревьев, практически отражает географию причинно-следственных связей пар «атака-уязвимость» в проектной деятельности защиты … систем от … атак	Топология построенного леса древовидных графов в ходе проектной деятельности может быть расширена на смежные объекты исследования, либо сужена лишь до актуальных множеств пар «атака – уязвимость»
2	Необходимостью наличия достаточного объема экспертных и статических данных и иных актуальных сведений относительно пар «атака - уязвимость» для атакуемых … систем и отсутствием подобного массива, аккумулированного из открытых источников	Организация парсинга открытых интернет-источников и суммаризации данных относительно пар «атака – уязвимость» в отношении … защищаемых … систем	База данных … атак и уязвимостей … защищаемых … систем, аккумулирующих их статистические и экспертные метрики, которые присутствуют в интернет – пространстве	В отличие от аналогов, впервые аккумулированы экспертные и статистические метрики частот реализации … атак и критичности … уязвимостей защищаемых … систем	Созданная база данных метрик … атак и уязвимостей … защищаемых … систем является практической основой для риск-калькуляции единичных вторжений	Сформированная база метрик открыта для ее расширения на другие атакуемые объекты и для многовариантного анализа корреляций входящих в нее данных
3	Объективной потребностью в расчетах вероятностей и ущербов единичных атак рассматриваемого класса и отсутствием калькуляторов, обеспечивающих получение	На основе суммированных данных создание автоматизированного калькулятора для расчета вероятности и ущерба единичных … атак на … защищаемые … системы	Методическое, алгоритмическое и программное обеспечение калькуляции рисков единичных … атак на уязвимости … защищаемых … систем в ходе обеспечения их безопасности	В отличие от аналогов, сконструированный калькулятор ориентирован на специфику … атак и уязвимостей …, имеющих непосредственное отношение к защищаемым … системам	Калькулятор позволяет оперативно вычислять параметры риска единичных … атак на уязвимости … защищаемых … систем в ходе проектной деятельности по обеспечению	Открывается перспектива управления рисками успешности единичных вторжений за счет разработки методик варьирования метрик … атак и уязвимостей … защищаемых

Продолжение табл. 2

№	Противоречия между:	Задачи исследования	Результаты исследования	Новизна результатов	Практическая ценность результатов	Теоретическая ценность результатов
	таких данных в автоматизированном режиме				их безопасности	… систем
4	Необходимостью риск-анализа множественных атак … на уязвимости … и отсутствием такого методического, алгоритмического и программного обеспечения для построения риск-ландшафта защищаемых … систем	С использованием вышеуказанной калькуляции создание автоматизированного инструментария риск-анализа успешности реализации массированных … атак на уязвимости … защищаемых … систем	Программный инструментарий автоматизированного формирования риск-ландшафта множественных атак … на уязвимости … защищаемых … систем	Для массированных атак впервые построен риск-ландшафт в трех измерениях: … атака, уязвимость … и риск успешности использования этих элементов в отношении защищаемой … системы	В ходе проектной деятельности для специалиста, защищающего … системы, предлагается наглядная и емкая картина успешности … атак на имеющиеся уязвимости	С использованием построенного ландшафта представляется возможным выявить наиболее опасные сочетания «атака - уязвимость» и организовать управление индуцированными ими рисками
5	Объективной потребностью управления риск-ландшафтом рассматриваемого множества атак и уязвимостей и отсутствием подобного инструментария, включая моделирование регулировки параметрами ландшафта	Организация управления риск-ландшафтом массированных … атак на … защищаемые … системы, включая машинное моделирования оптимизационных процедур регулирования	Методики, алгоритмы и программы регулирования рисков построенного ландшафта за счет варьирования параметров атак и уязвимостей, включая машинное моделирование процесса управления	Впервые предлагается инструментарий управления рисками массированных … атак на уязвимости … защищаемых … систем, доведенный до автоматизации	Созданное обеспечение с помощью функций чувствительности позволяет осуществлять движение рисков множественных атак в пространство допустимых для них значений	С использованием теории чувствительности и методов множественного анализа открывается перспектива оптимизации риск – ландшафта для защищаемых систем различного назначения
6	Сложившейся практикой формирования регламентов применения мер защиты в отношении единичных атак и	Формирование политики и регламентов реагирования и ликвидации последствий в отношении множественных … атак	Комплекс политики и регламентов реагирования и ликвидации последствий в отношении … атак массированного	Впервые предложены политики и регламенты противодействия множественным … атакам на уязвимости …	Предложенная регламентация является инструментом практического управления риск-ландшафтом успешности	В порядке развития методологии управления риск-ландшафтом успешности множественных … атак на

Окончание табл. 2

№	Противоречия между:	Задачи исследования	Результаты исследования	Новизна результатов	Практическая ценность результатов	Теоретическая ценность результатов
	объективной необходимостью регламентации противодействия массированным вторжениям в защищаемую … систему	на уязвимости … защищаемой … системы	характера на уязвимости … защищаемых … систем	защищаемых … систем	множественных … атак на защищаемые … системы	уязвимости … защищаемых … систем предоставляется возможность формирования соответствующих инструкций для персонала

Многоточия в табл. 2 делают универсальной настоящую матрицу целеполагания. Вместо этих многоточий проектант может поместить класс (вид) рассматриваемых атак, разновидность атакуемых компонентов в исследуемых системах заданного им же назначением (все от всего защищать невозможно).

Примером подобного исследования может служить анализ и регулирование рисков массированных атак на средства машинного обучения специализированных нейронных сетей.

Заключение

В статье рассмотрены особенности проектной деятельности студентов и аспирантов по информационной безопасности и защите информации в современных условиях обучения. Приведены результаты совместной работы Финансового университета при правительстве Российской Федерации, Института проблем управления РАН и Воронежского государственного технического университета по созданию атласа кибератак. Показаны возможности использования междисциплинарного подхода к формированию профессиональных компетенций.

Продемонстрированы результаты использования нейросетейвых технологий и средств искусственного интеллекта в научной работе и проектной деятельности студентов и аспирантов по защите информации. Показаны результаты совместной деятельности вузов с базовыми профильными организациями.

Представленный в статье материал допустимо рассматривать в качестве прообраза очередных книг «Теория сетевых войн» издательства Горячая линия – Телеком.

Список литературы

1. Остапенко А.Г. Научно-проектная деятельность кафедры систем информационной безопасности в рамках программы «киберполигон» / А.Г. Остапенко, С.С. Куликов, А.А. Остапенко, Е.А. Москалева, Е.С. Петрова // Информация и безопасность. 2023, Т. 26, Вып. 3. С. 391-402.

2. Остапенко Г.А. Формализация знаний и данных кибератак и уязвимостей / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Д.С. Покудин, Н.Н. Корвяков, А.А. Ноздрюхин // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 231-238.

3. Остапенко А.Г. Методические основы проектной деятельности при выполнении научно-исследовательской работы студентами специалитета в сфере обеспечения информационной безопасности / А.Г. Остапенко, А.С. Пахомова, Д.А. Нархов, А.А. Остапенко, А.И. Шеншин // Информация и безопасность. 2023, Т. 26, Вып. 2. С. 169-176.

4. Остапенко Г.А. Автоматизированный банк знаний и калькулятор рисков реализации кибератак и уязвимостей (Часть I) / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Д.С. Нестеров, А.С. Дубов, В.А. Старцев // Информация и безопасность. 2024. Т. 27. Вып. 1 С. 7-30.

5. Остапенко Г.А. Модернизация методического обеспечения

автоматизированного сервиса агрегации данных и риск-анализа уязвимостей / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Н.Н. Корвяков, Д.С. Покудин, А.А. Ноздрюхин // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 219-230.

6. Остапенко Г.А. Модуль нейросетевой регламентации мер противодействия кибератакам / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, А.А. Ноздрюхин, Д.С. Покудин, Н.Н. Корвяков // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 239-246.

7. Остапенко Г.А. Совершенствование организационно-правового обеспечения информационной безопасности предприятия: формирование риск-ландшафта сетевых атак / Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.Ю. Пекло // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 203-210.

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

Институт проблем управления РАН
Institute for Management Problems of the Russian Academy of Sciences

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 09.09.2024

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, проректор, Финансовый университет при Правительстве Российской Федерации, e-mail: ostg@mail.ru

Калашников Андрей Олегович – д-р техн. наук, профессор, заместитель директора, Институт проблем управления РАН, e-mail: tigrilla1962@mail.ru

Остапенко Александр Григорьевич – д-р техн. наук, профессор, заведующий кафедрой, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, доцент, Воронежский государственный технический университет, e-mail: ea.vrn@yandex.ru

Карпеев Дмитрий Олегович – канд. техн. наук, зам. начальника управления, Финансовый университет при Правительстве Российской Федерации, e-mail: alexanderostapenkoias@gmail.com

Поздышева Оксана Валентиновна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Макаров Юрий Вадимович – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

USE OF ARTIFICIAL INTELLIGENCE IN THE COURSE OF RESEARCH AND EDUCATIONAL PROCESSES IN THE TRAINING OF INFORMATION SECURITY SPECIALISTS

A.G. Ostapenko, A.O. Kalashnikov, A.G. Ostapenko, E.A. Moskaleva, D.O. Karpeev, O.V. Pozdysheva, Yu.V. Makarov

The article discusses the current topic of developing competencies in the use of artificial intelligence technologies and neural network tools in the training of information security specialists. As a result of a joint project of the Financial University under the Government of the Russian Federation, the Institute of Control Sciences of the Russian Academy of Sciences and the Voronezh State Technical University, practice-oriented components of the educational process were developed. The educational process includes issues of constructing risk landscapes and an atlas of computer cyber-attacks and vulnerabilities to ensure the security of information systems and networks, developing modules: aggregation and risk analysis of cyber-incident data; a knowledge base and machine learning on measures to counter cyber-attacks; developing intelligent tips for decision-makers, response regulations and elimination of consequences in relation to computer incidents. These issues are implemented in the university educational process during project activities and practices.

Keywords: information protection, cyberattack atlas, neural network, risk analysis, information security, project activities.

Submitted 09.09.2024

Information about the authors

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

Andrey O.Kalashnikov – Dr. Sc. (Technical),), Deputy Ddirector, Institute for Management Problems of the Russian Academy of Sciences, e-mail: tigrilla1962@mail.ru

Alexander G. Ostapenko – Dr. Sc. (Technical), Head of Department, Voronezh State Technical University, e-mail: alexostap123@gmail.com

Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: ea.vrn@yandex.ru

Dmitrii O. Karpeev – Cand. Sc. (Technical), Deputy Head of Department, Financial University under the Government of the Russian Federation, e-mail:alexanderostapenkoias@gmail.com

Oxana V. Pozdyshtva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Yurii V. Makarov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com