Отзыв официального оппонента

Заведующего кафедрой систем информационной безопасности ФГБОУ ВО ««Казанский национальный исследовательский технический университет им. А.Н.Туполева-КАИ» доктора технических наук, профессора **Аникина Игоря Вячеславовича**

на диссертационную работу **Жука Романа Владимировича** на тему «Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы исследования

На сегодняшний день существует достаточно ограниченное количество методик определения угроз информационной безопасности (ИБ). В международной практике определение угроз ИБ является частью этапа оценки рисков в процессе менеджмента ИБ. При этом понятие актуальности угрозы ИБ как таковое не используется.

В начале 2021 года изменился подход к определению угроз ИБ в сторону разработки сценариев их возникновения и использования. Однако, на сегодняшний день существующий банк угроз, разработанный ФСТЭК России, а также основные методические документы не готовы к полноценному применению данного подхода. В частности, существуют определенные сложности в идентификации перечня активов ИСПДн, определения потенциала нарушителя и перечня актуальных уязвимостей для нарушителя с заданным потенциалом.

Для устранения данного противоречия необходимо осуществить унификацию подходов к определению нарушителей ИБ и подготовке перечня угроз ИБ в информационных системах, в частности в ИСПДн.

Таким образом, тема диссертационной работы Жука Романа Владимировича, посвящена разработке методики и алгоритмов определения актуальных угроз информационной безопасности в информационных системах персональных данных, преодолевающих выше указанные сложности является ***актуальной***.

Общая оценка структуры и содержания работы

Диссертационная работа состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы и 9 приложений. Работа изложена на 157 станицах машинописного текста. Список использованных источников содержит 70 наименований литературы.

Во введении обоснована актуальность темы диссертации, сформулирована цель, объект и предмет исследования, изложена научная новина и практическая ценность полученных результатов, приводятся сведения об апробации работы.

В первой главе произведены обзор и анализ современных отечественных и международных методик, методов, алгоритмов, программных средств определения угроз безопасности информации (УБИ) в информационных системах.

Во второй главе представлена разработанная методика определения актуальности возможных УБИ в ИСПДн, включающая: алгоритм выбора активов ИСПДн, алгоритм выбора уязвимостей ПО, критерии и алгоритм выбора уязвимостей ПО, которые могут быть реализованы выбранным нарушителем ИБ. В рамках разрабатываемой методики унифицирован перечень нарушителей ИБ, предложен способ расчета потенциала нарушителей ИБ с использованием метрик уязвимостей ПО. Предложен перечень критериев для расчета коэффициента исходной защищенности ИСПДн. Разработан алгоритм выбора типа актуальных УБИ в зависимости от наличия недекларируемых возможностей в ПО. Подготовлены продукционные правила для автоматизации разработанной методики.

В третьей главе приведен способ определения актуальных УБИ с применением математического аппарата искусственных нейронных сетей. Подготовлена обучающая выборка для тестовых ИСПДн и проведено обучение выбранной нейросетевой модели.

В четвертой главе проведена сравнительная оценка временных затрат на определение актуальных угроз в ИСПДн с помощью известных и разработанной автором методики.

В приложениях к диссертационной работе представлены опросные листы, листинги разработанных программ, свидетельства о регистрации базы данных и программы для ЭВМ, акты внедрения.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертационной работе

Обоснованность основных научных положений диссертационной работы подтверждается тем, что автором исследуются и анализируются известные подходы к решению поставленных задач, изучен российский и международный опыт определения актуальных угроз. Вводимые модернизации основаны на известных методах и алгоритмах.

При решении поставленных в работе задач использовались широко известные подходы и методы обеспечения информационной безопасности, экспертного оценивания, метода анализа иерархий, искусственных нейронных сетей, средства и технологии программирования и разработки баз данных Решение поставленных в работе задач базируется на результатах предыдущих исследований.

Достоверность и новизна полученных результатов

Научная новизна работы заключается в получении автором следующих результатов:

1. Для организации взаимосвязи параметров потенциала нарушителя ИБ и уязвимости ПО, метрики уязвимостей ПО спроецированы на

возможности нарушителя ИБ. Предложенный способ позволяет дать количественную оценку потенциалу нарушителя ИБ.

2. Предложен способ автоматизации определения актуальных угроз ИБ посредством применения математического аппарата нейронных сетей.

Достоверность результатов диссертационной работы подтверждается их реализацией в виде программы для ЭВМ и базы данных, сравнением полученных временных затрат с затратами, полученными при использовании существующих методик определения угроз ИБ, а также актами о внедрении результатов диссертационной работы. Основные положения, выносимые на защиту, прошли успешную апробацию на научных конференциях различного уровня.

Теоретическая и практическая значимость полученных автором результатов

Теоретическую значимость заключается в разработана методика определения актуальности УБИ в ИСПДн, включающая в себя: подход по выбору активов ИСПДн для определения перечня уязвимостей ПО; способ количественной оценки потенциала нарушителя ИБ с использованием параметров оценки уязвимостей ПО; алгоритм выбора уязвимостей ПО, которые могут быть реализованы нарушителем ИБ в ИСПДн; алгоритм выбора типа актуальных УБИ, а также алгоритм определения актуальности УБИ.

Практическая значимость заключается в том, что:

- осуществлена автоматизация разработанной методики определения актуальности УБИ с использованием программного средства и математического аппарата ИНС;

- временные затраты на определение актуальности УБИ в ИСПДн при использовании разрабатываемой методики могут быть сокращены более чем в 1,5 раза по сравнению с существующими подходами;

- результаты диссертационной работы могут быть применены при разработке моделей УБИ в ИСПДн в различных организациях и предприятиях независимо от их организационно-правовой формы.

Основные результаты диссертационной работы перечислены в 13 печатных работах, в том числе 9 публикациях в ведущих рецензируемых научных изданиях, рекомендованных ВАК при Минобрнауки России, 1 публикация в научном издании, индексируемом в библиографической базе «SCOPUS», 3 публикация в трудах научных конференций. Получено 1 свидетельство о государственной регистрации баз данных, а также 1 свидетельство о государственной регистрации программы для ЭВМ.

Соответствие содержания диссертации паспорту научной специальности

Содержание диссертации соответствует следующим пунктам паспорта специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность:

– п.3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса»;

– п.7 «Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения».

Недостатки диссертационной работы

1. Во введении диссертационной работы не сформулирован перечень задач, решаемых для достижения поставленной цели, что несколько нарушает логическую стройность изложения. Перечень данных задач вынесен в раздел 1.4. диссертации, а также представлен в соответствующем разделе автореферата, однако более логично было бы их привести после формулирования цели диссертационного исследования.

2. Для решения отдельных задач в диссертационной работе (в частности, присвоения потенциала нарушителям ИБ) автором использован метод анализа иерархий (МАИ). Однако, в диссертационной работе не сказано, производилась ли оценка согласованности матрицы парных сравнений. При описании МАИ, в формуле (2.1) присутствует опечатка, запись должна быть представлена в виде $x_{ji}=1/x_{ij}$.

3. Матрицы парных сравнений желательно было бы вынести в приложение диссертационной работы.

4. Необходимо большее внимание уделить вопросу подготовки обучающей выборки для искусственной нейронной сети, представленной в Главе 3, например, оценить, насколько обучающая выборка (Таблица 49) является репрезентативной.

5. При общей положительной оценке качества изложения и подготовки иллюстрационной части в диссертационной работе имеются отдельные опечатки и стилистические неточности.

Выводы

Приведенные выше недостатки никаким образом не снижают научную ценность диссертационной работы и не ставят под сомнение основные научные результаты диссертационного исследования.

Структура и содержание диссертации находятся в логическом единстве и соответствуют поставленным целям и задачам исследования. Текст диссертации изложен достаточно грамотно, цель исследования достигнута, поставленные задачи решены. Автореферат диссертации достаточно полно раскрывает ее основное содержание и положения, выносимые на защиту. Содержание автореферата соответствует основным положениям диссертационной работы. В нём изложены все основные результаты, выносимые на защиту, дано достаточно подробное представление о научно-практической значимости работы

Диссертация Жука Романа Владимировича, представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, в которой содержится решение актуальной задачи, заключающейся в разработке методики определения актуальности УБИ в ИСПДн, позволяющей уменьшить нагрузку на персонал и сократить временные затраты на разработку перечня актуальных УБИ в ИСПДн. Решение данной задачи имеет существенное значение для информационной безопасности.

Диссертационная работа является научно-квалификационной работой и соответствует п.п. 9-14 «Положения о присуждении учёных степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 №842, а её автор, Жук Роман Владимирович, заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:

доктор технических наук, профессор

Аникин Игорь Вячеславович,

заведующий кафедрой систем информационной безопасности Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ

25.10.2021

Докторская диссертация защищена
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность
Кандидатская диссертация защищена
по специальностям 05.13.01 – Системный анализ, управление и обработка информации, 05.13.18 - Математическое моделирование, численные методы и комплексы программ

Адрес места основной работы: г. Казань, ул. К. Маркса, 10

Рабочий телефон: +7 (843) 231-01-09

Адрес эл. почты: anikinigor777@mail.r

Подпись Аникина И.В.
заверяю. Начальник управления
делами КНИТУ-КАИ