МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»
(ГУАП)

Большая Морская ул., д. 67, лит. А, Санкт-Петербург, 190000, Тел. (812) 710-6510, факс (812) 494-7057
E-mail: common@aanet.ru; http://www.guap.ru; ОКПО 02068462; ОГРН 1027810232680; ИНН/КПП 7812003110/783801001

_____ № _____

На № _____ от _____

ОТЗЫВ
ОФИЦИАЛЬНОГО ОППОНЕНТА

БЕЗЗАТЕЕВА Сергея Валентиновича на диссертацию **МИНЯЕВА Андрея Анатольевича** на тему «Методика оценки эффективности системы защиты территориально-распределенных информационных систем», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертационного исследования

В настоящее время информационная безопасность (ИБ) становится все более значимой и важной сферой. Одновременно с ростом и развитием информационных технологий растет и множество методов и средств нарушений состояния ИБ. Изменить ситуацию можно путем разработки новых подходов к обеспечению ИБ, способных предоставить надежную защиту от современных угроз безопасности информации (УБИ). Существует необходимость разработки новых и совершенствования существующих подходов к обеспечению ИБ, способных предоставить надежную защиту от современных УБИ. Одновременно с этим, современные информационные системы в большинстве случаев являются территориально-распределенными

(ТРИС). Одной из важных задач по обеспечению ИБ в ТРИС является оценка эффективности СЗИ ТРИС.

В связи с вышесказанным, диссертационная работа Миняева Андрея Анатольевича, посвященная повышению качества оценки эффективности СЗИ ТРИС, является **актуальной**.

Автором сформулирована **цель диссертационного исследования** – повышение качества оценки эффективности систем защиты территориально-распределенных информационных систем за счет определения необходимых и достаточных показателей. В работе определены: **объект исследования** – угрозы безопасности и требования по защите информации, **предмет исследования** – методы и методики моделирования актуальных угроз безопасности информации и оценки эффективности систем защиты информации. В работе сформулирована и решена актуальная **научная задача**, заключающаяся в том, чтобы повысить качество оценки эффективности СЗИ ТРИС, предложив автоматизированные метод и методики определения актуальных УБИ и оценки эффективности СЗИ, основанные на адаптивных нечетких нейронных продукционных системах, за счет определения необходимых и достаточных показателей и адаптации параметров таких систем. Тема диссертационного исследования, цель, предмет и объект исследования, научные задачи соответствуют паспорту искомой специальности – «Методы и системы защиты информации, информационная безопасность» по пунктам 1, 3, 10.

2. Научная новизна

Научная новизна результатов исследования заключается в следующем:

1. Предложенная методика определения актуальных угроз безопасности информации, в отличие от известных, в автоматизированном режиме формирует перечень актуальных УБИ, гипотетически исключая ошибки экспертов.

2. Предложенный метод оценки эффективности систем защиты информации, в отличие от известных, основан на теории адаптивных

нечетких нейронных продукционных системе и алгоритме нечеткого вывода Такаги-Сугено-Канга с применением технологий Data Science.

3. Разработанные методические рекомендации по оценке эффективности систем защиты информации в территориально-распределенных информационных системах, в отличие от известных, позволяют сократить количество не учтенных актуальных угроз безопасности информации, снизить финансовые затраты на создание системы защиты информации, применимы на всех этапах жизненного цикла систем, могут быть адаптированы под требования владельцев ТРИС. Использование рекомендаций не требует привлечения высококвалифицированных специалистов по информационной безопасности, тем самым исключает недостатки существующих методик, не требует больших вычислительных ресурсов, предлагает автоматизированный режим работы, что, в совокупности, повышает эффективность систем защиты информации в территориально-распределенных информационных системах.

3. Обоснованность и достоверность

Обоснованность и достоверность результатов, выносимых на защиту диссертационного исследования, выводов научного характера подтверждаются математическим обоснованием результатов исследований, системным подходом к решению поставленных задач, обоснованием выбранных методов и показателей определения актуальных УБИ и оценки эффективности СЗИ, доказательствами и результатами экспериментальной проверки предложенных метода и методик, анализом работ существующих зарубежных и отечественных практик решения аналогичных задач, апробацией результатов работы на международных и российских конференциях, а также подтверждением о внедрении предложенных метода и методик в организациях и предприятиях.

4. Практическая ценность

Практическая ценность работы заключается в следующих результатах:

1. Проведенный анализ ТРИС выявил основные аспекты технологии обработки информации и ИТ-инфраструктуры систем. Анализ атак и угроз безопасности информации в ТРИС, требований по ИБ, анализ СЗИ ТРИС, анализ существующих методов и методик моделирования УБИ и оценки эффективности СЗИ ТРИС позволил использовать полученные результаты при определении необходимых и достаточных показателей определения актуальных УБИ и оценки эффективности СЗИ.

2. Предложенная методика определения актуальных угроз безопасности информации позволяет определять большее количество актуальных УБИ, гипотетически исключая недостатки экспертов и минимизирует трудоемкость процесса и вычислительные ресурсы, в отличие от известных методик.

3. Предложенные метод и методические рекомендации по оценке эффективности СЗИ ТРИС позволяют проводить оценку эффективности СЗИ на основе необходимых и достаточных показателей, определенных в настоящем диссертационном исследовании, предоставляют владельцам ТРИС возможность оценивать эффективность СЗИ в реальном времени на всех этапах жизненного цикла существования ТРИС, гипотетически исключая ошибки экспертов, что, в свою очередь, позволяет своевременно вносить корректировки в проектные решения СЗИ для нейтрализации УБИ и выполнения требований по защите информации, учитывая финансовую составляющую при создании СЗИ. Показатели оценки эффективности могут быть изменены в зависимости от целей и потребностей владельца ТРИС в проведении оценки эффективности СЗИ ТРИС.

4. Разработанные в рамках диссертационного исследования программы для ЭВМ «Модель угроз и нарушителя» и «Оценка системы защиты информации» автоматизируют процессы определения перечня актуальных УБИ и проведения оценки эффективности СЗИ.

5. Апробация результатов исследования

Результаты, полученные в рамках работы над диссертацией, представлялись и обсуждались на международных и российских конференциях, а также подтверждаются актами внедрения в организациях и предприятиях. Работа выполнена при поддержке гранта для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга (Россия, Санкт – Петербург, 2015 г.). Диплом № 15542 от 27.11.2015 г. Подготовлено учебно-методическое пособие «Сертификация средств защиты информации» (Россия, Санкт – Петербург, СПбГУТ).

6. Публикации.

По теме диссертации опубликованы шестнадцать печатных работ, шесть из которых – в изданиях из перечня рецензируемых научных журналов ВАК при Минобрнауки России, в том числе две из них без соавторства; две – в международных изданиях, индексируемых в базах данных Web of Science и Scopus; два свидетельства о государственной регистрации программы для ЭВМ; шесть работ, опубликованных в других изданиях.

7. Личный вклад автора.

Представленные в диссертационном исследовании основные результаты получены автором лично.

8. Анализ диссертационного исследования

Анализ диссертации показал, что её структура характеризуется внутренним единством и логической связанностью. Работа состоит из содержания, введения, 4 глав, заключения, списка сокращений, списка литературы и приложений. По содержанию диссертация соответствует паспорту искомой специальности – «Методы и системы защиты информации, информационная безопасность», по оформлению соответствует требованиям, предъявляемым к научным работам, направляемым в печать.

В введении приводиться обоснование актуальности темы диссертационного исследования, определяются цели и задачи исследования,

предмет и объекты исследования. Обоснованы новизна и практическая ценность выносимых на защиту результатов.

В первой главе приведены результаты проведенного анализа моделей и методов построения систем, моделирования угроз безопасности информации и атак, анализ ИТ-инфраструктуры ТРИС и выявление специфических аспектов с точки зрения архитектуры таких ИС.

Во второй главе предложена методика определения актуальных угроз безопасности информации, основанная на теории адаптивных нечетких нейронных продукционных систем и алгоритмах нечеткого вывода, в отличии от известных, использует определенные в настоящей работе необходимые и достаточные показатели, автоматизирована и гипотетически исключает ошибки экспертов. Отличия предложенной методика от известных заключается в следующем:

- отсутствие необходимости привлечения высококвалифицированных специалистов в области ИБ;
- предложенная методика позволяет определять перечень актуальных УБИ в ИС различных типов и классов;
- позволяет выполнять требования регуляторов в области обеспечения безопасности информации, учитывает БДУ ФСТЭК России;
- может быть адаптирована для работы с международными базами данных УБИ (MITRE CVE, OSVDB, NVD, Secunia).

В третьей главе определены необходимые и достаточные показатели и предложен метод оценки эффективности систем защиты информации, основанный на адаптивной нечеткой нейронной продукционной системе и алгоритме нечеткого вывода Такаги-Сугено-Канга, в отличии от известных, позволяет достигать меньшего значения среднеквадратической ошибки работы системы, таким образом повышает эффективность СЗИ ТРИС, уменьшение финансовых затрат на создание системы защиты информации.

Предложенный метод позволяет владельцам систем автоматически оценивать эффективность СЗИ в режиме реального времени на всех этапах жизненного цикла системы, что позволяет своевременно внести корректировки в проектные решения СЗИ для нейтрализации актуальных УБИ и выполнения требований по защите информации.

В четвертой главе предложены методические рекомендации по оценке эффективности систем защиты информации в территориально-распределенных информационных системах, в отличии от известных, позволяют владельцам ТРИС в режиме реального времени оценивать эффективность СЗИ, снизить финансовые затраты на создание системы защиты информации, количество не учтенных актуальных угроз безопасности информации сокращается, использование методических рекомендаций не требует привлечения высококвалифицированных специалистов по ИБ, больших вычислительных ресурсов.

9. Замечания по диссертационной работе

1. Информация на Рисунках 2.1, 2.2 и 2.3, к сожалению, в представленном виде абсолютно не информативна и требует пояснения, так как автором введены цветные обозначения, однако не дано пояснение какую информацию несет конкретный цвет.
2. На представленном на странице 95 графике (Рисунок 2.11) не определено значение отсчетов по оси абсцисс. Остается неясным, что автор подразумевал под «заданным интервалом». Это же замечание относится и к графику, представленному на рисунке 3.9 (страница 138).
3. Приведение автором в основной части работы 15-ти страниц (стр. 118-133) программного кода видится абсолютно нецелесообразным. При желании автор мог вынести текст программного кода в приложение.

4. Заключение

Перечисленные замечания по диссертационному исследованию не влияют на полученные автором результаты, теоретическую и практическую значимости.

Диссертация Миняева А.А. на тему «Методика оценки эффективности системы защиты территориально-распределенных информационных систем» является научно-квалификационной работой. Полученные результаты и положения, выдвигаемые автором на публичную защиту, имеют научную новизну, теоретическую и практическую значимости. Диссертация выполнена единолично, имеет внутреннее единство. Результаты работы свидетельствуют о личном вкладе автора в науку.

Диссертационная работа удовлетворяют требованиям ВАК при Минобрнауки России и пунктам 9 – 14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к кандидатским диссертациям, а соискатель **Миняев Андрей Анатольевич** заслуживает присуждения ему степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

«11» октября 2021 года.
заведующий кафедрой технологий защиты информации
федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»,
доктор технических наук, доцент

[redacted] Беззатеев Сергей Валентинович

Подпись руки Беззатеева Сергея Валентиновича удостоверяю:

Подпись работника ГУАП [redacted]
Заверяю
Начальник Управления персонала [redacted]
«11» 10 2021 г.

Почтовый адрес: 190000 Санкт-Петербург, ул. Б. Морская, д. 67 лит.А.
Тел.: 8 (812) 710-65-10.
e-mail: common@aanet.ru