УТВЕРЖДАЮ:

Проректор по исследованиям и разработкам,
ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»,
кандидат технических наук, доцент
Колесников П.Г.

«19» 05 2025 г.

м.п.

ЗАКЛЮЧЕНИЕ
федерального государственного бюджетного образовательного учреждения
высшего образования
«Сибирский государственный университет науки и технологий
имени академика М.Ф. Решетнева»

Диссертация «Метод защиты от стороннего исследования локальной сети передачи данных на основе реконфигурации топологии сетевого уровня» выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева».

В период подготовки диссертации соискатель Кушко Евгений Александрович работал в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» на кафедре безопасности информационных технологий, в должности старшего преподавателя.

В 2022 г. окончил аспирантуру в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный аэрокосмический университет имени академика М.Ф. Решетнева по специальности 10.06.01 Методы и системы защиты информации, информационная безопасность.

Удостоверение о сдаче кандидатских экзаменов выдано в 2025 г. в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева».

Научный руководитель – Золотарев Вячеслав Владимирович, кандидат технических наук, заведующий кафедрой безопасности информационных технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева».

По итогам обсуждения принято следующее заключение:

Оценка выполненной соискателем работы.

Диссертация Е.А. Кушко является научно-квалификационной работой, в которой содержится решение важной и актуальной задачи разработки модифицированного метода и модели, а также нового алгоритма, предназначенных для повышения защищенности за счет противодействия сетевой разведке злоумышленника за счет изменения поверхности атаки на каждой итерации предложенного метода.

Актуальность темы и направленность исследования.

История развития информационных технологий и их современное состояние позволяет сделать вывод о том, что чем раньше группа информационной безопасности окажет противодействие злоумышленнику, тем с меньшими последствиями они столкнутся. Согласно общепринятой модели MITRE ATT&CK разведка является первой стадией реализации атаки. Поэтому меры, применяемые группой информационной безопасности для защиты, должны включать в себя не только те меры, которые направлены непосредственно на реализацию атаки, но и те, которые направлены на сбор информации для планирования точной и эффективной атаки злоумышленником.

Одной из технологий, которая направлена на противодействие разведке, является технология Moving Target Defense. Moving Target Defense изменяет поверхность атаки таким образом, чтобы на момент реализации атаки информация, собранная злоумышленником, уже была устаревшей. В результате, злоумышленник тратит ресурсы на неверную информацию, таким образом Moving Target Defense подрывает эффективность всей атаки. Однако, существующие решения Moving Target Defense для защиты сетей оперируют ограниченным набором параметров и, зачастую, не изменяют их в действительности, а лишь подменяют их на фиктивные значения. В результате для противодействия Moving Target Defense злоумышленник может либо сконцентрироваться на других параметрах сети, либо попытаться установить их истинные значения.

В работе представлен метод защиты от стороннего исследования, который является модификацией класса методов технологии Moving Target Defense, которые направлены на изменение топологии сети, однако предлагаемый метод изменяет реальные значения более широкого по сравнению с другими решениями набора параметров топологии сетевого уровня, который включает в себя: физический и логический адреса, логическая топология сети, маршруты передачи данных.

Актуальность защиты локальных сетей от стороннего исследования во многом обусловлена высоким уровнем возникновения связанных с этим событий и инцидентов, что отмечается в аналитических отчетах ведущих организаций в области информационной безопасности как в России, так и в других странах.

Личное участие автора в получении результатов.

Все достигнутые в диссертации результаты получены автором лично. Постановка задач работы осуществлена совместно с научным руководителем В.В. Золотаревым. Разработанные метод, модель, алгоритм и их программная реализация, а также проведение эксперимента и интерпретация результатов выполнена автором лично под руководством В.В. Золотарева.

Научная новизна диссертации.

В диссертационной работе были разработаны:

1. Модифицированный итерационный метод для защиты локальной сети передачи данных от стороннего исследования, отличающийся от существующих подходом к созданию подвижных целей, основанном на перегруппировке хостов в сочетании с рандомизацией адресов и маршрутов.
2. Модифицированная математическая модель оценки защищенности предложенного метода, основанного на технологии Moving Target Defense, отличающаяся от существующих способом оценки защищенности через вероятность идентификации целевого хоста при каждой итерации метода.

3. Новый алгоритм формирования топологии сетевого уровня и реализующее его программное средство, предназначенные для защиты от исследования злоумышленником локальной сети передачи данных, отличающиеся от существующих способом создания отношений между хостами сети.

Практическая значимость диссертации.

Разработанная в ходе работы метод, модель, алгоритм и программный комплекс могут быть использованы в автоматизированных системах с требованиями по защите от стороннего исследования, не требующих низких задержек.

Результаты работы по повышению защищенности от стороннего исследования были внедрены в рабочий процесс АО «НПП «Радиосвязь», а также в образовательный процесс СибГУ им. М.Ф. Решетнева для студентов кафедры безопасности информационных технологий.

Ценность научных работ соискателя, полнота изложения материалов диссертации в опубликованных работах.

По материалам диссертации Е.А. Кушко опубликовано 19 работ, из них 5 статей в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных ВАК и 5 зарубежных статей, индексируемые в международных базах Scopus и Web of Science. В том числе получено 1 свидетельство о государственной регистрации программ для ЭВМ.

Статьи, опубликованные в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных ВАК:

1. Паротькин Н.Ю., Панфилов И.А., Золотарев В.В., **Кушко Е.А.**, Панфилова Т.А. Разработка и экспериментальное исследование протокола динамического адресного пространства на основе мультикаст-групп // Сибирский журнал науки и технологий. – 2017. – Т. 18, №4. – С. 779-787.
2. **Кушко Е.А.** Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. 2020. № 4. С. 39-52.
3. **Кушко Е.А.**, Грачев Д.А., Паротькин Н.Ю., Золотарев В.В. О вопросах безопасности киберфизических систем // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2022. – Т. 25, № 4. – С. 101-109.
4. **Кушко Е.А.**, Паротькин Н.Ю., Золотарев В.В. Организация защищенного обмена внутри программно-управляемой локальной сети // Вестник СибГУТИ. – 2023. – Т. 17, № 4. – С. 62-73.
5. **Кушко Е.А.**, Трофимычев И.И. Метод защиты от исследования локальной вычислительной сети на основе реконфигурации топологии сетевого уровня // Прикаспийский журнал: управление и высокие технологии. – 2024. – № 3(67). – С. 63-72.

Статьи, индексируемые в международной базе Scopus:

6. **E.A. Kushko**, N.Yu. Parotkin. The research of technologies for secure data communication in dynamic networks // IEEE Xplore Digital Library, Dynamics of Systems, Mechanisms and Machines (Dynamics). 2017.
7. **E.A. Kushko**, N.Yu. Parotkin. Software implementation details of the secure data communication protocols stack based on the dynamic network topology // Journal of Physics: Conference Series 1399, IOP Publishing, 2019.
8. **E.A. Kushko**, N.Yu. Parotkin. Efficiency Evaluation of Secure Data Communication Protocols Stack Based on Dynamic Network Topology // 2019 International Russian Automation Conference, Rusautocon, IEEE, 2019.

9. **E.A. Kushko**, N.Yu. Parotkin. Method of hiding the architecture and configuration of the sensor network based on the dynamic topology // IOP Conference Series: Materials Science and Engineering. 2020. 862. 052024.

10. **E.A. Kushko**, N.Yu. Parotkin. Concealment of sensor network node interaction // IOP Conference Series: Materials Science and Engineering. III International Scientific Conference. Krasnoyarsk, 2021. С. 12058.

Прочие публикации:

11. Паротькин Н.Ю., **Кушко Е.А.**, Арифанова Н.В. Реализация элементов динамического адресного пространства // Актуальные проблемы авиации и космонавтики. 2016. Т. 1. № 12. С. 760-762.

12. **Кушко Е.А.** О решении задачи обеспечения защищенного обмена данными в локальной сети // Актуальные проблемы авиации и космонавтики. 2018. Т. 2. № 4 (14). С. 229-231.

13. **Кушко Е. А.** Метод обеспечения защиты передаваемых данных на основе плавающей топологии сети // Решетневские чтения. 2018. Т. 2. С. 337-338.

14. **E.A. Kushko.** Ways to improve the performance of secure data communication protocols stack based on the dynamic network topology // Актуальные проблемы авиации и космонавтики. 2019. Т. 2. С. 237-238.

15. **Кушко Е.А.** Детали технического решения по обеспечению сокрытия архитектуры и конфигурации сенсорной сети // Решетневские чтения. 2020. Т. 2. С. 526-527.

16. **Кушко Е.А.** Способ реализации сокрытия архитектуры и конфигурации сенсорной сети // Актуальные проблемы авиации и космонавтики. 2020. Т. 2. С. 233-235.

17. **Кушко Е.А.** О вопросах безопасности передачи данных в сенсорной сети // Актуальные проблемы авиации и космонавтики. 2021. Т. 2. С. 384-386.

18. **Кушко Е.А.** Обеспечение защищённого обмена данными методами нестационарной топологии взаимодействия узлов // Теоретические и прикладные вопросы реализации проектов в области информационной безопасности. Материалы межвузовской научно-теоретической конференции (в рамках Сибирского форума "Информационная безопасность - 2021"). 2021. С. 90-95.

19. **E.A. Kushko**, N.Yu. Parotkin. Formalization of secure data communication implementation method based on dynamic network topology // Наука, техно-логии, общество - НТО-II-2022. 2022. – P. 78-87.

Свидетельства о государственной регистрации программы для ЭВМ и БД:

1. 2022669450, 01.11.2022, «Программный модуль реализации защищенного обмена данными на основе динамической топологии сети».

Соответствие содержания диссертации избранной специальности.

Диссертационная работа Е.А. Кушко по своему содержанию соответствует профилю специальности 2.3.6 Методы и системы защиты информации, информационная безопасность, в частности, по следующим пунктам:

пункту 6. «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях».

пункту 10. «Модели и методы оценки защищенности информации и информационной безопасности объекта».

Диссертация «Метод защиты от стороннего исследования локальной сети передачи данных на основе реконфигурации топологии сетевого уровня» Кушко Евгения Александровича рекомендуется к защите на соискание учёной степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Заключение принято на расширенном заседании научно-технического семинара кафедры безопасности информационных технологий, института информационных технологий и телекоммуникаций Федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

Присутствовало на заседании 18 чел. Результаты голосования: «за» – 18 чел., «против» – 0 чел., «воздержалось» – 0 чел., протокол № 10 от «16» мая 2025 г.

Председатель семинара
д.ф.-м.н., профессор, директор института информатики и телекоммуникаций _____ / К.В. Сафонов