ОТЗЫВ

на автореферат диссертации Абрамовой Таисии Вячеславовны на тему «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков», представленную на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Темпы изменения мировой экономики и международных отношений обуславливают острую потребность внедрения современных информационных технологий в производственные процессы технологических объектов критической информационной инфраструктуры Российской Федерации. Данное обстоятельство неминуемо ведет к появлению новых угроз безопасности информации (далее — БИ), необходимости постоянного совершенствования применяемых систем защиты информации (далее — СЗИ) и разработки новых эффективных и высокопроизводительных средств защиты.

Защита информации в распределенных в пространстве автоматизированных систем управления технологическими процессами (далее — АСУ ТП) транспортировки нефтегазового сырья имеет свою специфику, связанную с особенностями таких систем: географическим расположением и условиями их эксплуатации, переменным характером угроз БИ на всей протяженности технологического объекта.

Указанные обстоятельства подтверждают актуальность проблемы, выбранной автором для исследования в рамках диссертационной работы.

Среди основных результатов исследования можно выделить следующее:

1. Разработана концепция снижения риска информационной безопасности (далее — ИБ) за счет высокопроизводительных методов и средств оперативного и достоверного обнаружения, распознавания аномальных состояний АСУ ТП, как проявлений инцидентов ИБ, нейтрализации связанных с ними угроз на основе исследования и интеллектуальной обработки сетевого трафика.

2. Разработан метод матричной кластеризации угроз БИ и моделей угроз БИ на основе статистической обработки значений рисков, позволивший определить характер изменения угрозы на последовательности подсистем распределенной

АСУ ТП, оценить степень актуальности угроз, провести приоритезацию их обработки.

3. Предложен метод построения математических и имитационных моделей и разработаны модели для обнаружения аномалий и распознавания состояния компьютерных сетей (далее — КС) АСУ ТП на основе данных мониторинга сетевого трафика, позволяющие повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз.

4. Разработаны алгоритмы, методики и программно-аппаратная реализация методов и средств обнаружения аномалий и нейтрализации угроз БИ по данным сетевого трафика на основе принципов построения ассоциативных процессоров, позволяющие повысить производительность, достоверность, универсальность средств защиты информации и снизить риски от угроз БИ.

5. Проведена экспериментальная оценка эффекта от использования разработанных методов, в результате которой выявлено снижение рисков от угроз распространения вредоносного кода в КС, несанкционированных действий персонала АСУ ТП не менее чем в 2 раза, потери информации о состоянии объекта защиты не менее чем на 14% при использовании разработанных методов и средств.

Полученные результаты обладают научной новизной и практической значимостью, расширяют методологию построения СЗИ КС распределенных АСУ ТП, позволяют усовершенствовать методы и средства защиты информации на основе дихотомического и ассоциативно-мажоритарного подходов с применением интеллектуальной обработки данных сетевого трафика. Практическая значимость результатов работы заключается в разработке научно обоснованных методов и средств, позволяющих снизить риски от угроз БИ в распределенных АСУ ТП.

Достоверность результатов исследований подтверждена их апробацией в процессе проведения экспериментов, на научных конференциях, публикацией результатов в ведущих рецензируемых научных изданиях. По материалам исследования опубликовано 43 работы, в том числе 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 1 научная работа в издании, включенном в базу Scopus, коллективная монография, получены патент на изобретение, свидетельства о регистрации программ для ЭВМ.

Автореферат диссертации соответствует требованиям Положения ВАК о порядке присуждения ученых степеней. Результаты диссертационной работы, судя по автореферату, соответствуют паспорту научной специальности 2.3.6.

«Методы и системы защиты информации, информационная безопасность».

Замечания по автореферату:

- в автореферате не раскрыты подробно детали реализации комплекса разработанных программных средств;
- не приводятся характеристики требуемых вычислительных ресурсов для применения результатов работы.

Высказанные выше замечания объясняются ограниченным объемом автореферата и не снижают высокого уровня проведенной соискателем работы.

Учитывая вышеизложенное, считаю, что диссертация Абрамовой Таисии Вячеславовны, представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, а ее автор заслуживает присуждения ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Отзыв составил:

Кандидат технических наук,
Директор Корпоративного центра мониторинга информационной безопасности средств и систем информатизации
ООО «УЦСБ»

Мушовец
Константин Владимирович

19.08.2024

Даю согласие на обработку персональных данных.

Почтовый адрес основного места работы: 620100, г. Екатеринбург, ул. Ткачей, 6
Тел: +7 (343) 379-98-34
E-mail: info@ussc.ru

Кандидатская диссертация защищена
по специальности 05.13.01 - системный анализ, управление и обработка информации

Подпись К.В. Мушовца заверяю:

Руководитель группы
Езова М.Ю.

Общество с ограниченной ответственностью «Уральский центр систем безопасности» USSC ОГРН 1076672021194 Российская Федерация г. Екатеринбург