ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора **СИНЕЩУКА Юрия Ивановича** на диссертационную работу **УШАКОВА Игоря Александровича**, выполненную на тему **«Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных»** и представленную на соискание учёной степени кандидата технических наук по специальности 05.13.19 - Методы и системы защиты информации, информационная безопасность.

1. Актуальность темы диссертационного исследования

Переживаемая в настоящее время четвёртая промышленная революция(«Индустрия 4.0»), характеризуется усиленной интеграцией киберфизических систем в различные технологические процессы и, как любой диалектический процесс, предполагает, наряду с достоинствами, появление новых проблем. В первую очередь это касается вопросов обеспечения безопасности. Интеграция физических систем с сетевыми информационными структурами делает их более уязвимыми к кибератакам.

Проблема обеспечения защиты информации, циркулирующей в компьютерной сети(КС), становится исключительно важной, требующей решения ряда специальных задач. Часть этих задач успешно решается аппаратно-программными средствами защиты информации. При этом вне поля зрения остаются наиболее реальные и многочисленные внутренние(инсайдерские) угрозы.

Для достоверного обнаружения той или иной подозрительной активности в сети необходимо контролировать большое число событий. Человек способен распознать эти события лишь при удобном отображении и на обозримых объемах информации. Для работы на таком масштабе данных становится целесообразным сочетать машинные методы обработки и методы(модели) структуризации массивов цифровой информации, использовать алгоритмы на основе экспертных правил для того чтобы явным образом выявить интересующее событие. Цифровая идентификация событий позволяет принимать более обоснованные(точные) решения, автоматизируя этот процесс. При этом, появляется возможность для контроля и мониторинга любых изменений сетевой активности (в том числе — нежелательной).

В связи с этим, можно утверждать, что диссертационное исследование, выполненное соискателем, по разработке специализированной технологии обработки сетевого трафика для обеспечения информационной безопасности, сочетающей существующие и новые способы анализа и обнаружения инсайдерской деятельности, является актуальным, имеющим существенное значение для народного хозяйства.

2. Новизна исследования и полученных научных результатов

Автор на защиту выносит следующие основные научные результаты:

1. Модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени.

2. Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак.

3. Методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.

4. Архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.

Учитывая важность повышения уровня защищенности КС, точности обнаружения инсайдеров, работу Ушакова И. А. можно рассматривать как новый шаг в направлении перехода от метода «проб и ошибок» к управлению инсайдерскими аспектами информационной безопасности на базе аналитического обоснования принимаемых решений.

При решении поставленных научных задач соискатель использовал современный подход, основанный на выявлении противоречий предметной области, декомпозиции целей, с последующим агрегированием задач.

При этом, принципиально новыми, ранее не использовавшимися в практике подобных исследований, являются:

- процедура научного обоснования задач исследования на основе выявления места и роли процедуры обнаружения инсайдеров в КС в общем цикле обработки информации в SIEM-системе;

- комплекс математических моделей: - представления больших данных(включая модель инсайдера), с возможностью хранения и анализа признаков пользователей характеризующих потенциальную инсайдерскую деятельность в компьютерных сетях, а также возможностью учета динамики изменения этих признаков; - комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак, с учетом признаков и свойств пользователей, устройств, приложений, сервисов, включая параметр времени;

- комплекс алгоритмов комбинированного применения экспертных правил и методов машинного обучения, а также архитектура системы обнаружения инсайдеров в компьютерных сетях;

- методика обнаружения инсайдеров, на основе предложенных моделей, и реализация на ее основе программного комплекса системы обнаружения инсайдеров в КС, обеспечивающего комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения;

- архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях.

3. Значимость полученных результатов для науки и практики

Теоретическая значимость полученных результатов - заключается в совершенствовании методов и моделей обеспечения информационной безопасности за счёт расширения классов атрибутов, необходимых для обнаружения инсайдеров, применения нового подхода к решению задачи обнаружения инсайдеров в КС путем комбинирования двух классов алгоритмов, основанных на экспертных правилах и на методах машинного обучения; - определяется применением системного подхода к решению задач анализа и синтеза сложных систем в части оценки слабоформализуемых параметров, в условиях высокой информационной неопределенности, характерной для процессов принятия решений по выявлению деструктивной инсайдерской деятельности.

Практическая значимость результатов основных положений и результатов диссертации Ушакова И. А. состоит в создании методического обеспечения и научно-прикладного инструментария аналитической поддержки специалистов по информационной безопасности, при решении задачи обнаружения инсайдеров, с целью повышения защищенности КС.

3. Степень обоснованности и достоверность полученных научных результатов

Достаточная обоснованность и достоверность полученных в диссертации научных результатов:

- обеспечивается корректностью постановки задач на исследование, строго обоснованной совокупностью ограничений и допущений, применением апробированных методов исследования, учетом в моделях факторов, адекватных реальной ситуации;

- подтверждается непротиворечивостью основных положений работы результатам, полученным при проведении экспериментов в рамках диссертационного исследования, а также полученным ранее в других работах, широкой апробацией научных результатов, внедрением их в деятельность Роскомнадзора и профильных организаций, в учебный процесс ВУЗов Санкт-Петербурга.

4. Недостатки и рекомендации:

Давая общую положительную оценку выполненного автором исследования, следует отметить ряд недостатков, выявленных при оппонировании работы:

1) Формулируя актуальность, цели и задачи научного исследования, в явной форме, не показано место рассматриваемых средств и методов в общей системе мероприятий защиты информации;

2) Решая задачу разработки научно-методического обеспечения процесса обнаружения инсайдера, целесообразно больше внимания уделить социально-психологическим аспектам поведения нарушителя информационной безопасности, и оценке возможных издержек, связанных с применением предложенных средств;

3) В рамках описания архитектуры и программной реализации системы отсутствуют инструкция оператора и формы интерфейса;

4) В работе используются термины «информационная безопасность», «компьютерная безопасность», «кибербезопасность» без определения их соотношения;

5) Выводы по главам носят описательный, перечислительный характер без четкой формулировки результатов, выносимых на защиту с указанием работ, где они опубликованы и мест их апробации;

6) С точки зрения оформления работы, следует отметить: в списке литературы не указаны нормативно-правовые документы в сфере информационной безопасности, за исключением «Банка данных угроз безопасности информации ФСТЭК России»; в работе не представлен список используемых аббревиатур, а по тексту не все из них раскрыты(стр.19); в отличие от реферата в диссертационной работе отсутствует нумерация формул.

Отмеченные недостатки не носят принципиального характера, не влияют на общую положительную оценку работы, не ставят под сомнение основные научные результаты работы и являются скорее пожеланием по дальнейшему планированию исследований.

5. **Выводы.**

Автореферат отражает основное содержание диссертационной работы.

Диссертация является законченной научно-квалификационной работой, в которой, на основании выполненных автором исследований, содержится решение важной научной задачи разработки новых и совершенствовании имеющихся методов и средств защиты информации.

Диссертация обладает внутренним единством, имеет четкую структуру, написана понятным языком. Результаты диссертационного исследования опубликованы автором с необходимой полнотой и свидетельствуют о личном вкладе автора диссертации в науку. По материалам диссертационной работы опубликовано 40 работ, в том числе 9 - в рецензируемых изданиях из перечня ВАК, 2 - в изданиях, индексируемых в международных базах Scopus и Web of Science, получено 3 свидетельства о государственной регистрации программ для ЭВМ.

Все это характеризует соискателя как вполне сложившегося исследователя, умеющего самостоятельно ставить и решать сложные научно-технические задачи.

Актуальность и важность поставленных и решенных в диссертации задач, современный технических и методический уровень их решения позволяют сделать заключение, что данная работа отвечает требованиям пп. 9-14 "Положения о присуждении ученых степеней", предъявляемым к кандидатским диссертациям.

По своей теме, содержанию и полученным результатам диссертация соответствует п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» паспорта специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность», а её автор **УШАКОВ Игорь Александрович** заслуживает присуждения ученой степени кандидата технических наук по данной специальности.

Официальный оппонент:
профессор кафедры специальных информационных технологий
ФГКОУ ВО «Санкт-Петербургский университет МВД Российской Федерации» ,
Заслуженный работник высшей школы РФ, доктор технических наук, профессор

Синещук Юрий Иванович

«23» марта 2020 г.

Подпись руки
Синещука Ю
ЗАВЕРЯ
Начальник отдел
Санкт-Петербургского униве
подполковник
«23» марта 2020 г.

Федеральное государственное казенное образовательное учреждение высшего образования
«Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»
198206, Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1
Тел.: +7 (812) 744-7024, Факс.: +7 (812) 744-7042
E-mail: sinegal53@mail.ru