Проект РНФ № 21-71-20078. Описание выполненных на 3-м этапе работ и полученных научных результатов

1. Разработаны **методы, модели, методики и алгоритмы проведения расследований компьютерных инцидентов на основе аналитической обработки больших массивов гетерогенных данных о кибербезопасности**.

Модель проведения расследований компьютерных инцидентов описывает основные множества и подмножества элементов киберпреступлений. Алгоритмы и методики этапов расследования используют этапы модели и её подмножества. Метод проведения расследований компьютерных инцидентов позволяет повысить эффективность работы специалистов при расследовании компьютерных инцидентов информационной безопасности. Он предполагает возможность своего использования для различных видов компьютерных инцидентов в качестве универсального метода расследования. Модельно-алгоритмическая часть метода специфицирует процедуры, используемые для описания этапов расследования, их состава и последовательности действий специалиста.

2. Разработаны **архитектура и программные прототипы компонентов обнаружения в реальном времени атак на основе имитационного и графо-ориентированного моделирования**.

Архитектура и программные компоненты включают следующие программные модули: (1) предобработки событий, отвечающий за извлечение информационных признаков из входного потока данных и их нормализацию с приведением к единому формату событий безопасности; (2) кластеризации событий для построения ограниченного числа агрегированных состояний системы на основе методов кластеризации; (3) построения графов состояний и переходов с определением допустимых переходов между агрегированными состояниями системы; (4) анализа графа состояний и переходов, отвечающий за обход графа по фактическому потоку событий от системы с целью определения текущего состояний системы; (5) нейросетевого прогнозирования состояний, основанный на рекуррентной нейронной сети и включающий элементы имитационного моделирования на основе правил и статистик.

3. Разработаны **архитектура и программные прототипы компонентов обнаружения в реальном времени аномальной активности и нарушений критериев и политик безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности**.

Модельно-алгоритмическая часть включает модули предобработки данных, выявления аномалий, генерации объяснений решений, выдаваемых аналитическими моделями, и реализована с использованием библиотек TensorFlow и PyTorch (для работы с глубокими нейронными сетями, в частности pyOD и pyGOD). Обучение моделей анализа осуществлялось в вычислительной среде СКЦ.

Исходные данные включают набор данных от физических сенсоров и набор данных с системными событиями от службы аутентификации ОС Windows.

Для анализа системных событий разработан компонент их предобработки, который строит граф событий для заданного интервала времени и формирует вектор анализируемых признаков, представленные как структурно-топологическими характеристиками графа, так и статистическими характеристиками событий.

Для выявления аномалий в потоке данных от физических сенсоров использована связка двух моделей-классификаторов: DeepSVDD и модели случайного леса. Для объяснения прогноза используются два локальных метода объяснений - LIME и SHAP, среди которых SHAP является наиболее приемлемым в задаче объяснений аномалий для набора данных SWaT.

4. Разработаны **архитектура компонентов оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов на основе аналитической обработки больших массивов гетерогенных данных**.

Архитектура включает два уровня: высокий и низкий. Высокий уровень составляют модули, непосредственно выполняющие оперативную оценку защищенности ресурсов с использованием возможностей СКЦ. В их состав входят следующие модули: построения модели сети; формирования путей риска; оценки рисков; выбора пути высокого риска. В состав модулей низкого уровня входят модули, выполняющие обеспечивающие функции: сбора и предварительной

обработки исходных данных; ведения рабочей базы данных; взаимодействия с другими компонентами и с пользователями.

Прототип компонента реализован на языке Python с библиотек networkx, psycopg2, joblib и picle. Для хранения данных используется СУБД PostgreSQL. Для интеграции с компонентом оперативной визуализации используется фреймворк Flask. Для возможности тестирования прототипа компонента на данных сетевых информационных систем большого размера дополнительно разработан генератор сетевых графов.

5. Разработаны **архитектура и программные прототипы компонентов оперативного анализа и управления рисками информационной безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности.**

Архитектура включает следующие функциональные модули: формирования интегральной оценки риска в статическом режиме; формирования интегральной оценки риска в динамическом режиме; сравнения интегральной оценки с критерием; постановки задачи компонентам обнаружения атак и аномалий; постановки задачи компоненту поддержки принятия решений. Имеются связи с другими компонентами системы, а также высокопроизводительным кластером. Уточнены форматы входных данных, включая события безопасности, профили устройств и пользователей, и связи между ними, вычисленные значения метрик защищенности для устройств и для пользователей, данные о количестве и типе аномалий, данные о количестве и типе кибератак, историческая информация об оценках рисков, введенные экспертами критерии уровней риска. Программные прототипы реализованы на языке python. Для тестирования и экспериментальной оценки прототипа использован набор данных SWaT.

6. Разработаны **архитектура и программные прототипы компонентов оперативной визуализации больших массивов гетерогенных данных о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования инцидентов**, которые обеспечивают ручной визуальный анализ данных о событиях информационной безопасности при отображении больших объёмов гетерогенных исходных данных, отображение логов аутентификации пользователей, оценку состояния защищенности компьютерной сети и отображение метрик оценки рисков. Архитектура обеспечивает сопряжение модулей системы поддержки принятия решений с модулем оперативной визуализации для решения задач по визуальному поиску аномалий. Программные прототипы компонентов оперативной визуализации входят в систему поддержки принятия решений и обеспечивают возможность визуального поиска оператором аномалий в данных о событиях кибербезопасности.

7. Уточнена **архитектура системы аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности, использующая возможности СКЦ.**

Дополнительно разработаны следующие подсистемы: (1) управления, (2) экспериментальной среды, (3) инжиниринга, (4) создания, обучение и валидации моделей, (5) эксплуатации и переобучения моделей.

Выбраны элементы и стеки технологий, которые обеспечивают наиболее высокий уровень производительности и ресурсоэффективности. В качестве основной СУБД выбрана ClickHouse. Для управления потоками выбрана технология Apache Kafka, с которой связана СУБД MongoDB. Для унификации данных созданы модели унификации для User и Hosts. Данные, получаемые от внешних систем, сведения об уязвимостях, об оценках защищенности сохраяются в оперативном хранилище, построенном на базе СУБД MongoDB.

Результаты исследований опубликованы в 15 статьях, индексируемых в WoS и Scopus (среди них 2 статьи Q1), в 2 статьях, индексируемых в RSCI, и 20 статьях и тезисах докладов, индексируемых в РИНЦ.

При выполнении проекта получены исключительные права на РИД: 1 патент на изобретение, 5 свидетельств о государственной регистрации программ для ЭВМ.

Члены коллектива участвовали в апробации результатов на 14 российских и международных конференциях и семинарах.

URL: http://comsec.spb.ru/ru/projects/
URL: http://comsec.spb.ru/en/projects/