UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА «РИ-2014»

XIV САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 29-31 октября 2014 года

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2014

подготовки информации для принятия решений лицом принимающим решение (ЛПР). Для проведения работы создают рабочую группу (РГ), которая и организует по поручению ЛПР деятельность экспертов, объединенных в экспертную комиссию (ЭК).

Классическое представление роли и места участников процесса ЭО ИБ представляется последовательностью: ЛПР (запрос информации и создание РГ) -> РГ (создание ЭК и организация ее деятельности) -> ЭК (анализ проблемы) -> ЭК (предоставление результатов в РГ) -> РГ (обработка результатов ЭК и предоставление информации ЛПР) -> ЛПР (принятие решения на основании информации РГ).

Общеизвестна методологическая проблема, сопровождающая процесс решения слабоформализованных задач специалистами разных областей знаний: несоответствие тезаурусов различного уровня приводит к подмене понятий и отклонению от задачи исследования.

Для снижения влияния различия тезаурусов участников процесса ЭО предлагается формализовать деятельность РГ на основе следующего целевого цикла:

ФАЗА 1: Уточнение задачи: Проверка единого понимания задачи членами РГ и ЛПР.

ФАЗА 2: Уточнение цели: Для чего? (смысл); Для кого? (заказчик (ЛПР)); Что хотим получить? (результат) Как оценить результат? (критерии) К какому сроку? (время).

ФАЗА 3: Сбор информации: Факты, ресурсы, идеи, альтернативы, риски и т.д

ФАЗА 4: Принятие решения: Разделение задачи на части; расстановка приоритетов; выбор наилучшей альтернативы; составление перечня действий; планирование.

ФАЗА 5: Планирование: Кто делает; что делает; где делает; когда делает; как делает.

ФАЗА 6: Действие: реализация плана – выполнение действий, намеченных в предыдущей фазе.

ФАЗА 7: Анализ результата на основе критериев.

Формализация работ на каждом этапе, сопровождаемая подведением промежуточных итогов, препятствует отклонению от проблемы исследования, снижает временные затраты и риски неуспешного завершения ЭО.

Пантюхин И.С., Швед Д.В., Кочуров Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

СИСТЕМА ПОСТИНЦИДЕНТНОГО АНАЛИЗА ИНФОРМАЦИОННЫХ СИСТЕМ

Количество преступлений с применением средств вычислительной техники неуклонно растет. Существующие методы и средства проведения криминалистического анализа не соответствуют в достаточной степени требованиям и возможностям современных технологий компьютерной техники. В связи вэтим, становится все более актуальным разработка новых методов и средств проведения автоматизированного криминалистического анализа различных информационных систем.

Криминалистический анализ является неотъемлемой частью расследования инцидента информационной безопасности. Для более точного анализа, помимо исследования содержимого жесткого диска, может применятся и исследование содержимого оперативной памяти. В данных оперативной памяти, могут содержаться такие данные как: ключи шифрования, состояния сети и операционной системы, кэш программ и многое другое. Исследование в совокупности с жестким диском, может дать более детальную картину происходящего в информационной системе в конкретный момент времени.

Актуальность развития направления исследования инцидентов в области высоких технологий очень высока, особенно в России. Успех расследования инцидента во многом завит от знаний и умений эксперта. Поэтому для снижения уровня ошибок эксперта планируется разработка системы поддержки принятий решений, что в свою очередь позволит расследовать инциденты информационной безопасности менее квалифицированному персоналу.

Разработанная методика получения данных оперативной памяти с различных информационных систем позволит в совокупности с исследованием жесткого диска разработать методы повышения достоверности цифровых улик, а новые способы обработки позволят сократить время расследования инцидента информационной безопасности. С применением системы поддержки принятия решений, снизится вероятность утрат цифровых улик менее квалифицированным персоналом, что в свою очередь позволит увеличить скорость и качество проведения расследования инцидента информационной безопасности.

Целью работы является повышение достоверности цифровых улик и снижение времени расследования инцидента информационной безопасности.

Развитие данного направления, способно привнести вклад в модернизацию экономики России, поскольку позволит не только сократить расходы на проведение расследований, но и потери частного сектора. Полученные разработки позволят сделать существенный вклад в обеспечение безопасности граждан, организаций и государства в целом. Накопленный опыт, знания и разработки можно привнести в науку о раскрытии преступлений связанных с компьютерной информацией.

Полученные наработки могут применяться для создания программного комплекса для автоматизаций проведения криминалистического анализа. Данный программный продукт будет востребован компаниями занимающимися вопросами расследования инцидентов информационной безопасности, позволит повысить достоверность цифровых улик и снизить скорость расследования инцидентов информационной безопасности.

Таким образом, для повышения достоверности цифровых улик и снижения времени расследования инцидента информационной безопасности необходимо: разработка системы сбора данных с информационной системы, создание средств и методов извлечения, обработки и загрузки данных, создание базы знаний, создание системы аудита и принятия решений.

Старков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МЕТОД ПОСТРОЕНИЯ СЕМЕЙСТВА ПРОФИЛЕЙ ЗАЩИТЫ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных. Наряду с задачей построения информационной системы персональных данных возникает необходимость документального подтверждения того, что данная система отвечает предъявляемым к ней требованиям безопасности. Именно в этот момент возникает вопрос сертификации информационной системы в соответствии с необходимым классом защищенности. Процедуру сертификации информационных систем персональных данных можно упростить благодаря созданию семейства профилей защиты для данных систем.

Предметом данной работы является комплекс вопросов обеспечения информационной безопасности персональных данных. Объектом исследования являются модель семейства профилей защиты для информационной системы персональных данных и метод построения семейства профилей защиты для информационной системы персональных данных с учетом требований безопасности ГОСТ Р ИСО/МЭК 15408.

В качестве желаемой цели ставится задача выделения группы критериев, на основе которых будет производиться оценка безопасности персональных данных и соотнесение этих критериев с функциональными требованиями безопасности.

Итогом работы должен стать метод построения семейства профилей защиты для информационных систем персональных данных, основанный на действующем законодательстве Российской Федерации в области защиты персональных данных.

Таранов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ПОСТРОЕНИЕ КОДОВ, ИСПРАВЛЯЮЩИХ ОШИБКИ, НА СПЛАЙН-ВЭЙВЛЕТНЫХ РАЗЛОЖЕНИЯХ И ИХ ИСПОЛЬЗОВАНИЕ ДЛЯ ЗАЩИТЫ ОТ АТАК ПО СТОРОННИМ КАНАЛАМ

По мере развития информационных технологий появляются новые атаки, использующие уязвимости в практической реализации криптосистем. Такие атаки получили название атак по сторонним каналам (sidechannelattacks). Одним из методов защиты от данного типа атак является использование в криптосистемах помехоустойчивых надежных кодов.

Надежные коды, в отличие от линейных кодов, не зависят от распределения ошибок, их кратности и количества, и поэтому не чувствительны к атакам по ошибкам вычислений. Надежные коды направлены на обеспечение равновероятной защиты против всех возможных ошибок, таким образом, злоумышленник не сможет выбрать совокупность ошибок для внедрения, которая может привести к выполнению внештатных операций на защищаемомкриптоустройстве.

В работе представлены алгоритмы получения надежных кодов с помощью сплайн-вэйвлетных разложений. Предлагаются различные способы построения данного класса кодов, проанализированы их преимущества по сравнению с существующими надежными кодами.

Математической основой разработанных алгоритмов являются формулы декомпозиции сплайн-вэйвлетных разложений первого порядка.

В данной работе было предложено несколько способов получения избыточности надежного кода с помощью сплайн-вэйвлетных разложений, а именно:

- использование сплайн-вэйвлетных разложений без выбрасывания элементов;
- использование нескольких сеток для одной кодовой комбинации;
- использование сплайн-вэйвлетных разложений относительно элементов с различными порядковыми номерами.