в проекте будет разработан функционал для генерации дополнительных отчетов для оценки загруженности сотрудников, а также обновления текущие отчетов в eazyBI.

Список литературы

1. JIRA documentation // Atlassian [Электронный источник]. URL: https://confluence.atlassian.com/jiracoreserver071/jira-core-documentation-802172329.html/ (дата обращения: 12.04.2019).

2. JIRA Software // TOPSAAS [Электронный источник]. URL: http://topsaas.ru/jira.html/ (дата обращения: 19.04.2019).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Д.В. Зезина, А.Ю. Хохлов

В работе рассматриваются основные меры, которые необходимо учитывать при проектировании системы защиты данных на предприятии. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности. Популярные инструменты и технологии современной повседневной жизни, такие как мобильные телефоны, веб-почта, службы мгновенных сообщений, съемные носители и беспроводной доступ к Интернету дали каждому возможность легко переносить и обрабатывать большое количество данных. Наряду с возможностью переноса данных многие организации создали информационные системы вокруг своих продуктов и услуг на основе открытых стандартов и интерфейсов совместимых с популярными устройствами. Кроме того, организации способствуют легкому доступу к данным как для персонала, так и для широкой публики через Интернет. Но недостатком этого удобства является большая вероятность передачи конфиденциальных корпоративных данных посторонним лицам. Поэтому актуальность рассматриваемой темы в том, что в наше время остро встает вопрос о необходимости защищать информацию своего предприятия различными методами, но многие не знают, что следует делать, дабы сохранить те или иные сведения в тайне, с выгодой реализовать их и не понести убытки от их утечки или утраты. Данные являются одним из наиболее важных активов любой организации и люди обычно считаются самым слабым звеном в цепи безопасности. Крайне важно чтобы сотрудники полностью осознавали свои обязанности, их ограничения на доступ к информации и дисциплинарные меры, которые будут приняты за любое нарушение безопасности. Все это может служить движущей силой для самосовершенствования с точки зрения безопасности данных.

УПРАВЛЯЕМОЕ КОДИРОВАНИЕ КОМБИНАЦИОННЫХ СХЕМ

Л.А. Золоторевич, А.В. Павлова

В последнем десятилетии значительно возрос ущерб от пиратства и других угроз в области производства аппаратного обеспечения и составляет около 4 млрд. долларов в год, что примерно в 10 раз превышает ущерб от пиратства в области ПО. Для решения проблемы в работе [1] предлагается подход к проектированию Design for-Trust (DfTr) как развитие теории контролепригодного проектирования (Design-for-Testability – DfT), который дополнительно включает средства для контроля и предотвращения аппаратных атак при проектировании и изготовлении СБИС.

В работе [2] проанализированы различные модели процесса злонамеренного искажения проекта, описывающие условия, при которых подобное искажение может внедриться в цифровую систему. В числе возможных источников искажений рассматриваются поставщики базовых функциональных блоков интеллектуальной собственности (IP's), которые приобретаются разработчиками СнК, собственно разработчики СнК, а также кремниевые фабрики – изготовители СнК.

Основная идея защиты проектов от неавторизованного пользователя основана на кодировании комбинационных схем цифровых устройств. Защита базируется на введении дополнительных логических элементов в структуру схемы, формировании ключевого кода, применение которого вводит схему в область правильного функционирования [3]. Основная задача, которая должна быть решена для эффективной практической реализации данной общей идеи, заключается в том, чтобы определить оптимальное множество внутренних линий схемы и количество ключевых элементов для создания максимальных трудностей для злоумышленника по поиску правильного ключа.

В докладе задача кодирования сводится к поиску неисправностей константного типа кодируемой структуры, обнаруживаемых на большем количестве выходных линий и на максимальном количестве входных векторов. Для решения задачи применяются методы и средства тестового диагностирования [4, 5].

Список литературы

1. Security analysis of integrated circuit camouflaging / J. Rajendran [et al.] // ACM SIGSAC conference on Computer & communications security. Berlin. 4–8 November 2013. P. 709–720.

2. Hardware Trojans: Lessons learned after one decade of research / K. Xiao [et al.] // ACM transactions on design automation of electronic system. 2016. Vol. 22. No. 1.

3. Weighted Logic Locking: A New Approach for IC Piracy Protection / N. Karousos [et al.] // IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). 2017. P. 221–226.

4. Золоторевич Л.А. Функциональный контроль СБИС типа СнК // Сб. науч. статей «Технологии автоматизации и управления». 2017. Вып. 3. В 2 кн. Книга 2. С. 216–225.

5. Золоторевич Л.А. Модели неисправностей при верификации проектов и контроле цифровых систем // Матер. Междунар. науч. конф. «Компьютерные науки и информационные технологии». Саратов, 2018. С. 160–163.

МЕТОДЫ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ В ПОСТРОЕНИИ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.М. Кадан

Модель вероятного нарушителя информационной безопасности важна для систематизации данных о возможностях и типах нарушителей, целях их несанкционированных воздействий и выработки адекватных организационных и технических методов противодействия. Правильно разработанная модель вероятного нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности: опираясь на построенную модель, можно строить адекватную систему информационной защиты. При разработке модели нарушителя обычно учитывают: категории лиц, к которым можно отнести нарушителя; цели, градации по степени опасности и важности; анализ его технических возможностей; предположения и ограничения о характере действий.

В докладе предлагается и демонстрируется построение модели вероятного нарушителя на основе анализа лог-файлов информационной системы. Анализ ведется с использованием методов поведенческой аналитики, среди которых выделяется метод когортного анализа [1]. Когортный анализ рассматривает данные из некоторого набора данных (например, платформы электронной коммерции, веб-приложения или онлайн-игры), и вместо того, чтобы рассматривать всех пользователей как единое целое, разбивает их на связанные группы. Идея когортного анализа состоит в том, чтобы выполнить такое разбиение по определенным признакам или похожему поведению, и отслеживать развитие этих групп во времени в течение определенных временных интервалов. Построение модели нарушителя было продемонстрировано на примере информационной системы, являющейся компьютерной игрой для социальных сетей. Использование лог-файлов такой системы позволило получить для исследования набор данных объемом более 600 ГБ, содержащий около 10^{10} записей о поведении более 35 млн. пользователей. В качестве основных характеристик рассматривалась минимизация финансовых потерь разработчика от применения целенаправленной рекламы.