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.