– 30000,0 тыс. руб. на оборотные средства.

Привлеченные средства могут быть покрыты за 60 месяцев деятельности проекта. Предполагается получение чистого дохода сумме 722080,5 тыс. руб.

Планируется после выполнения первого этапа проекта, привлечь дополнительное финансирование (кредитные и собственные средства ориентировочно 682000,0 тыс. руб.) для развития проекта (газификация, водоснабжение, подъездная дорога, строительство спортивных сооружений, бассейна, кафе, озеленение и благоустройство территории).

Оценки этих результатов были сделаны в условиях максимально возможной надежности:

– рассматриваются минимальные доходы и максимальные расходы;

– рабочий режим в проекте предусматривает непрерывный цикл при посменной работе персонала;

– цены, заложенные в проекте, соответствуют сложившимся рыночным ценам на момент проектирования.

В целом проект можно охарактеризовать как жизнеспособный в условиях данного региона. Не вызывает сомнений потенциал роста данного проекта через распространение на другие районы области. Практическая осуществимость данного проекта основывается на изучении рынка и опыте предыдущей работы в этом направлении.

Е. И. Ключинский, Н. Б. Осипенко
(ГГУ им. Ф. Скорины, Гомель)

СРЕДСТВА АНАЛИЗА ДАННЫХ О БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ

В тезисах описывается разработанное серверное приложение, предназначенное для анализа Android приложений на предмет наличия в них вредоносного кода, агрессивной рекламы, фишинга данных пользователя и другого подозрительного функционала.

Приложение работает на основе фреймворка Ruby On Rails, пользователь через фронт-енд задает APK-файл для анализа. Скачанная программа устанавливается на удаленный эмулятор, делаются скриншоты приложения. Далее сервер производит тройную декомпиляцию приложения: байткод для Dalvik декомпилируется в байткод Java, он же в свою очередь декомпилируется в Java-код. Отдельно декомпилируются ресурсы приложения, хранящиеся в формате XML (строковые

константы, цвета, слои) и файл приложения Android Manifest.xml. После декомпиляции сервер анализирует полученные данные, выявляются подозрительные и опасные разрешения, фоновые сервисы, ресейверы. На базе этих данных формирует отчет для пользователя.

Для разработки серверного приложения был освоен Ruby On Rails – фреймворк, написанный на языке программирования Ruby. Ruby on Rails предоставляет архитектурный образец Model-View-Controller (модель-представление-контроллер) для веб-приложений, а также обеспечивает их интеграцию с веб-сервером и сервером базы данных.В качестве базы данных было принято решение использовать MySQL – свободную объектно-реляционная систему управления базами данных (СУБД).Для декомпилирования байткода Dalvik в байткод Java будет использоваться dex2jar – консольная утилита для работы с байткодом Android. Для получения исходного Java – кода используется консольная утилита JD. В качестве эмулятора взят родной эмулятор Android из SDK, предоставляемым Google.

Данное приложение может использоваться пользователями для проверки подозрительных файлов, скачанных вне сервиса Google Play. С ростом числа пользователей смартфонов Android увеличивается количество вредоносных программ, способных как похищать данные, так и отправлять SMS-сообщения незаметно для пользователя.

Е. В. Кончиц
(ГГУ им. Ф. Скорины, Гомель)

ТЕХНОЛОГИЯ «IBM COGNOS BUSINESS INTELLIGENCE»

Система управления данными «IBM Cognos Business Intelligence» является единой платформой для анализа и отчетности, которая обеспечивает полную функциональность инструментов Business Intelligence (BI). Канадская компания Cognos – одна из первых разработчиков пробных программных продуктов, существующая с 1969 года под названием Quasar Systems Limited (с 1982 года − под названием Cognos). Система BI разрабатывалась как единая платформа, основанная на трех принципах: эффективность, гибкость и простота. Кроме того, Cognos имеет упрощенный интерфейс, не требует установки дополнительного программного обеспечения.

IBM Cognos BI – это система с возможностью быстрого реагирования на изменения отчётности на любом уровне. Данная платформа