ОБ УРОВНЯХ ДОВЕРИЯ АУТЕНТИФИКАЦИИ

А.Г. Сабанов

ЗАО «Аладдин Р.Д.»

В связи с выходом Постановления Правительства РФ от 28 ноября 2011 г. № 977, которое предписывает в весьма сжатые сроки ввести в эксплуатацию единую систему идентификации и аутентификации (ИА), актуальным становится вопрос о том, какие базовые принципы защиты будут заложены в основу создания национальной универсальной платформы защищенного доступа к различным информационным системам (ИС), используемым для предоставления государственных услуг. Исходя из анализа зарубежного опыта создания подобных систем, одним из ключевых принципов является введение определенных уровней строгости аутентификации для различных групп пользователей и уровней защищенности ИС, к которым соответствующие группы имеют права доступа. Фактически речь идет об уровнях доверия или уровнях гарантий (level of assurance).

На данном этапе развития информатизации российского общества предлагается ввести простую трехуровневую модель уровней доверия (и, соответственно, строгости) аутентификации. Такая модель наиболее полно согласовывается с текущим состоянием нормативной базы как в части оценки состояния защищенности ИС, обрабатывающих информацию ограниченного доступа, не содержащую гостайну, так и в части законодательства по защите персональных данных и электронной подписи. Так, в соответствии с Федеральным законом № 63-ФЗ на территории РФ с 1 июля 2012 г. вводится 3 вида электронной подписи: простая, усиленная неквалифицированная, усиленная квалифицированная. Условно можно ассоциировать массовое применение простой подписи с гражданами, усиленной неквалифицированной – с предприятиями и организациями, а усиленной квалифицированной – с государственными структурами различного уровня. Этот подход согласуется с основными положениями Федерального закона № 149-ФЗ, где сказано, что участниками электронного взаимодействия и обладателями информации могут являться 3 уровня пользователей: граждане (физические лица), организации (юридические лица), государство (государственные органы и органы местного самоуправления). Деление на три большие группы приемлемо как с точки зрения грубой оценки рисков (низкий, средний, высокий), так и для оценки надежности, а также последствий от ошибок ИА и атак (уровни: низкий, средний, высокий).

В сложившейся за период с 2002 г. практике применения аутентификаторов (токенов) также массово используется всего 3 распространенных типа: многоразовый пароль, технология одноразовых паролей OTP (One Time Password) и технология строгой двухфакторной аутентификации с применением смарт-карт, содержащих неизвлекаемый ключ электронной подписи, применение которого невозможно без ввода PIN-кода (по сути, в этом случае используется технология электронной

подписи). Таким образом, основываясь на приведенных рассуждениях, можно выделить три уровня строгости аутентификации.

Уровень 1. Разрешенным токеном при удаленной аутентификации является многоразовый пароль без требований контроля целостности. Пароль не должен в открытом виде передаваться по сети. Желательно соблюдать требования по длине пароля (не менее 6 символов). Разрешается использовать простую электронную подпись. Нет требований по надежности ИА. Основными обладателями информационных ресурсов на этом уровне являются граждане, которые определяют риски проникновения на их ресурсы мошенников самостоятельно. Приветствуется использование на этом уровне аутентификаторов и электронного удостоверения (ЭУ) с уровней 2 и 3.

Уровень 2. Рекомендуется применение технологии OTP или двухфакторной аутентификации (смарт-карта плюс PIN-код). При этом издание ЭУ разрешено не только аккредитованным удостоверяющим центрам. Основными обладателями информационных ресурсов являются организации с развитой инфраструктурой открытых ключей. Для аутентификации, предназначенной для внутренних нужд и согласованного электронного взаимодействия с контрагентами, разрешается использование открытых (международных) криптоалгоритмов. Для взаимодействия с государственными органами обязательно применение аутентификации уровня 3 и криптоалгоритмов ГОСТ 34.10-2001 и ГОСТ 34.11-2001.

Уровень 3. Рекомендуется использование только строгой, как минимум, двухфакторной взаимной (информационный ресурс − претендент) аутентификации с применением аутентификаторов с неизвлекаемым ключом электронной подписи (устройства класса SSCD). Это позволит обеспечить защиту ключа подписи от воспроизведения, он-лайн угадывания, имитации проверяющей стороны и атак класса «человек посредине».

Основными задачами информационной безопасности для «облачных» вычислений являются: обеспечение удаленной регистрации, безопасное ведение учетных записей пользователей, обеспечение безопасного делегирования аутентификации и доверия в облачные сервисы, управление доверием при взаимодействии облачных сервисов, разделение доступа и контроль доступа в привязке к методу аутентификации пользователя, его роли и требований к уровню доверия в облаке.

Показано, что для «облачных» вычислений необходимо следующее.

Для задачи «делегирование полномочий» нельзя использовать пароль (нельзя ограничить по времени) и технологию OTP (одноразовый пароль становится многоразовым, или получим «отказ в обслуживании» из-за невозможности сгенерировать следующий OTP). При использовании механизма электронной подписи делегирование проводится с применением стандартных функций PKI.

Для вычислений в «облаках», требующих разделения доступа, применение секретов классов «пароль» и OTP неприемлемо с точки зрения обеспечения безопасности пользователя.

Для обеспечения аутентификации в «облаках» необходимо применять только строгую двухстороннюю аутентификацию на основе электронной подписи.

ОБНАРУЖЕНИЕ ГРАФИЧЕСКОГО СПАМА С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ DATA MINING

О.В. Хачинян, О.И. Шкалябин

Нижегородский госуниверситет

Спам − одна из наиболее важных и актуальных проблем сети Интернет. В последнее время распространение получил так называемый графический спам – сообщения, текст которых находится внутри изображения. Наиболее актуальным и эффективным стало использование в спам-фильтрах методов Data Mining. Их особенность заключается в том, что они разделяют объекты на несколько категорий, используя для классификации модель, построенную заранее на базе прецедентной информации [1]. Целью данной работы является изучение возможности обнаружения графического спама с помощью методов Data Mining.

Методов Data Mining существует много, в том числе метод Байеса, нейронные сети, метод k-ближайших соседей. Наиболее эффективным является метод опорных векторов, основанный на теории статистического обучения [2]. Основная идея этого метода – перевод исходных векторов в пространство более высокой размерности и отыскание гиперплоскости в этом пространстве, которая разделяла бы объекты двух классов с максимальным зазором между ними.

Поскольку указанные методы применяются только для текстовых файлов, то проблему графического распознавания они решить не могут. Для решения задачи обнаружения графического спама предложено использовать комбинацию метода распознавания текста с изображения и метода опорных векторов (SVM).

Для выполнения первой части задачи широко применяются методы оптического распознавания символов (OCR) [3]. Данные методы переводят изображение с текстом в последовательность символов, использующихся для распознавания в текстовом редакторе. Распознавание изображения происходит следующим образом: программы OCR разбивают картинку на блоки и находят среди них те, которые содержат текст, затем выделенные блоки с текстом разбиваются на строки. Далее программа пытается разбить строку на области изображения, разделенные пробелами, предполагая, что каждая такая область и есть символ – буква или цифра.

В ходе данной работы разработан экспериментальный фильтр, содержащий в себе два модуля: OCR-преобразователь и SVM-классификатор.

Для практических исследований было взято два спам-фильтра: Kaspersky Anti-Spam 3.0, Spam Assassin 3.3.2 [4] и представленный экспериментальный фильтр. При анализе текста Spam Assassin и экспериментальный фильтр используют методы Data Mining: соответственно метод Naive Bayes и SVM. В Kaspersky Anti-Spam применяется новая технология обнаружения текстов и спама в растровых изображениях без необходимости машинного распознавания графических образов. Сравнительные характеристики фильтров приведены ниже, в табл. 1.

Табл. 1

Сравнительная	**Kaspersky**	**Spam Assassin**	**SVM-**

характеристика	Anti-Spam		классификатор
Обучение	не требуется	требуется	требуется
Время обучения	нет	25 писем/минута	21 письмо/минута
Требуемое количество писем для обучения	_____	200 спам-писем и 200 легальных писем	200 спам-писем и 200 легальных писем
Использование дополнительных модулей	не требуется	необходим модуль OCR	необходим модуль OCR

Тестовый набор состоял из 600 графических сообщений, из которых 260 – легальные, а 340 – спам. Получены следующие результаты.

Табл. 2

Характеристики	Kaspersky Anti-Spam	Spam Assassin	SVM-классификатор
Показатель обнаружения	0,988	0,747	0,776
Уровень ложных срабатываний	0,054	0,092	0,069

Как видно из результатов, самый высокий показатель обнаружения при минимальном уровне ложных срабатываний имеет Kaspersky Anti-Spam. Остальные фильтры показали результаты хуже. Это произошло из-за того, что преобразователь OCR не всегда корректно и точно переводит графическое изображение в текст.

Методы OCR ресурсоёмки и не обеспечивают требуемой точности детектирования. При этом методы Data Mining остаются мощным средством в борьбе с текстовым спамом. Для борьбы с графическим спамом необходимо искать более эффективные методы обнаружения и распознавания текста в изображениях.

[1] Witten J. Data Mining Practical Machine Learning Tools and Techniques − Burlington: Morgan Kaufmann Publishers, 2011. P.3.
[2] Розинкин А.Н. Разработка методов формирования оптимального тренировочного набора для системы классификации электронной почты на основе алгоритма опорных векторов – Москва: Изд-во МГУ им. Ломоносова, 2005. С.15.
[3] Online OCR. Что такое распознавание текста? http://www.onlineocr.ru/support/WhatIsOCR.aspx
[4] ApacheSoftwareFoundationTheApache Spam Assassin Public Corpus: http://spamassassin.apache.org/

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ ДЛЯ ЛИНЕЙНЫХ МОДЕЛЕЙ ДИСКРЕТНЫХ ДИНАМИЧЕСКИХ СИСТЕМ ПО ИХ ЭКСПЕРИМЕНТАЛЬНЫМ ДАННЫМ

А.А. Горбунов, М.С. Киселев

Нижегородский госуниверситет

При описании преобразователей текстовых последовательностей различной природы с помощью моделей дискретных динамических систем для класса линейных моделей имеется возможность решать задачи структурной идентификации, определяя не только базовые [1], но и другие рабочие параметры. Так, ответ на вопрос о возможности описания криптографического преобразователя при помощи линейной математической модели (ММ) существенным образом влияет на возможности и условия построения модели восстанавливающего преобразователя, а значит, и на оценку стойкости всей криптосистемы (КС) в целом. В работе [2] рассмотрен подход, представляющий собой схему идентификации ММ шифратора КС как линейную модель на основе его входного и выходного текстов.

В настоящей работе для реализации алгоритма параметрической идентификации преобразователя текстовых последовательностей (например, криптопреобразователя) его динамическая ММ представляется в виде детерминированной дискретной модели авторегрессии скользящего среднего (АРСС-модели):

$$\begin{aligned} y(t) = \alpha_1 y(t-1) + \alpha_2 y(t-2) + \ldots + \alpha_n y(t-n) + \\ + \beta_0 u(t) + \beta_1 u(t-1) + \beta_2 u(t-2) + \ldots + \beta_n u(t-n) \quad . \end{aligned} \tag{1}$$

Для определения значений коэффициентов АРСС-модели

$$\alpha_1 , \alpha_2 , \ldots , \alpha_n , \beta_0, \beta_1 , \beta_2 , \ldots , \beta_n \tag{2}$$

решается система линейных алгебраических уравнений в алгебраической структуре поля Галуа ($GF(q)$) [2].

Разработанный в рамках данной работы комплекс программных модулей позволяет определять по полученным экспериментально входным и выходным текстам преобразователя как параметр сложности n идентифицируемого объекта, так и набор (2) рабочих параметров модели. Программные модули были реализованы на языке C++ в среде разработки программного обеспечения Microsoft Visual Studio 2010.

При помощи написанных программных модулей осуществлялись компьютерные эксперименты по нахождению адекватных АРСС-моделей преобразователей текстовых последовательностей и их коэффициентов. Экспериментальные текстовые данные получались с входов и выходов следующих преобразователей: шифрующие линейные цифровые автоматы (для шифров Цезаря, Вижинера, гаммирования), нелинейные преобразователи текстов, шифраторы криптосистемы DES в различных режимах. Полученные результаты экспериментов подтвердили характер зависимостей порядка n ММ идентифицируемых преобразователей от количества

отсчетов в их входных и выходных текстах для случаев, приводимых и неприводимых к линейному.

[1] Кирьянов К.Г. //Тр. III-й Международной конференции «Идентификация систем и задачи управления SICPRO'04» – М.: ИПУ РАН, 2004. С.187.
[2] Горбунов А.А. //Тр. XIV-й научной конференции по радиофизике. 7 мая 2010 г. /Под ред. С.М. Грача, А.В. Якимова. – Нижний Новгород: ННГУ, 2010. С.286.

МОДИФИКАЦИЯ АЛГОРИТМА ПОСТРОЕНИЯ ГЕНЕТИЧЕСКОЙ КАРТЫ ДАННЫХ ДЛЯ СЛУЧАЯ РЕГУЛИРУЕМОЙ АЛГЕБРАИЧЕСКОЙ СТРУКТУРЫ

А.А. Горбунов, А.С. Коновалов, А.О. Маченко

Нижегородский госуниверситет

Проблема идентификации источников текстовых данных в рамках математической модели генетической карты (ГК) экспериментальных данных, введенной в работах К.Г. Кирьянова (например, [1, 2]), возникает при решении целого ряда практически важных задач функционирования информационных систем. Среди них можно обозначить вопросы оценки параметров стойкости криптосистем, прогнозирования цифровых рядов данных, автоматизированной идентификации текстовых последовательностей спам-рассылок и другие.

В рамках настоящей работы ставилась задача осуществить исследование различных методов построения ГК текстовых данных. В работе представлен подход, основанный на понятиях «источника экспериментальных данных» или «прогнозирующего оператора» участка стационарности (гена) текстовой последовательности

$$y(t+1) = f\,(\,y(t),\,\ldots\,,\,y(t-n+1),\,u(t+1),\,u(t),\,\ldots\,,\,u(t-n+1)\,). \qquad (1)$$

При этом динамическая математическая модель источника задается либо в самом общем виде при помощи таблицы истинности прогнозирующего оператора, либо представляется разностным уравнением в определенной алгебраической структуре (АС).

При реализации алгоритмов построения ГК текстовых последовательностей рассматривались следующие линейные математические модели, описывающие источники текстовых данных для каждого из участков стационарности.

Детерминированная дискретная авторегрессионная модель имеет вид:

$$y(t+1) = \alpha_1 y(t) + \alpha_2 y(t-1) + \ldots + \alpha_n y(t-n+1). \qquad (2a)$$

Линейный цифровой автомат, представимый в *ABCD*-формализме (или в пространстве состояний [3, 4]) описывается системой уравнений:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \\ x(0) = x_0 \end{cases} . \qquad (2б)$$

При этом на входе алгоритма имеется возможность задания алгебраической структуры, описывающей функционирование рассматриваемых моделей источников данных.

Алгоритмы построения ГК текстовых последовательностей были программно реализованы на языке программирования C++ в среде разработки программного обеспечения Microsoft Visual Studio 2010. Реализованная компьютерная программа позволяет строить ГК текстовых данных, рассчитывать статистические характеристики по полученным генам и осуществлять регулирование автокорреляционных функций (АС), в которых задаются линейные модели источников данных.

В результате проведенных компьютерных экспериментов для ряда генетических текстовых последовательностей было осуществлено сравнение средней длины получаемых генов для случая фиксированной АС (модулярное поле Галуа – $GF(q)$) и структуры, выбираемой для обрабатываемой текстовой последовательности. Продемонстрировано уменьшение средней длины участка стационарности при задании соответствующей АС по сравнению со случаем изначально фиксированной структуры.

[1] Кирьянов К.Г. Генетический код и тексты. – Нижний Новгород: ТАЛАМ, 2002, 100 с.
[2] Кирьянов К.Г. //Тр. III-й Международной конференции «Идентификация систем и задачи управления SICPRO'04». – М.: ИПУ РАН, 2004. С.187.
[3] Стрейц В. Метод пространства состояний в теории дискретных линейных систем управления. − М.: Наука, 1985, 296 с.
[4] Гилл А. Линейные последовательностные машины. − М.: Наука, 1974, 288 с.

РАЗРАБОТКА МЕТОДА СТОХАСТИЧЕСКОЙ ТРАССИРОВКИ ПУТЕЙ ДЛЯ АРХИТЕКТУРЫ GPU

Д.Р. Богров, Д.К. Боголепов

Нижегородский госуниверситет

Одним из первых алгоритмов глобального освещения стал алгоритм стохастической трассировки пути, представленный в 1986 году Джеймсом Кайя [1]. Алгоритм позволяет учитывать все эффекты реалистичной имитации света, включающие все возможные взаимодействия между различными типами поверхностей.

Алгоритм трассировки путей заключается в следующем: через каждый пиксель экранной плоскости испускается первичный луч, для которого определяется ближайшая точка соударения x. Яркость данного пикселя вычисляется из уравнения визуализации

$$L(x \to \Theta) = L_e(x \to \Theta) + L_r(x \to \Theta) , \qquad (1)$$

для численного решения которого используется метод Монте-Карло. В целях повышения эффективности вычислений, уравнение отраженной от поверхности яркости разделяется на прямое и вторичное освещение

$$L_r(x \to \Theta) = L_{\text{direct}}(x \to \Theta) + L_{\text{indirect}}(x \to \Theta) =$$
$$= \int_{A_{\text{sources}}} L_e(y \to \overline{yx}) f_r(x, \Theta \leftrightarrow \overline{xy}) G(x,y) V(x,y) dA_y + \tag{2}$$
$$+ \int_{H_x} L_r(r(x,\Psi) \to -\Psi) f_r(x, \Theta \leftrightarrow \Psi) \cos(N_x, \Psi) d\omega_\Psi,$$

где $f_r(x, \Psi \to \Theta)$ – функция двунаправленной отражательной способности, $V(x,y)$ – функция видимости, $G(x,y)$ – геометрический член.

Прямое освещение L_{direct} $(x \to \Theta)$ поступает в точку x непосредственно от источников света. Вторичное освещение $L_{indirect}$ $(x \to \Theta)$ попадает в точку x после, по крайней мере, одного отражения от другой поверхности сцены (см. рис.). Такая декомпозиция ускоряет расчет прямого освещения, поскольку область интегрирования для него включает только поверхности источников света.

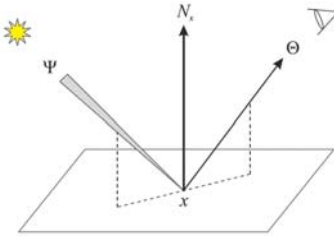

Рис.

Расчет конечного изображения – процесс вычисления энергетической яркости, выполняющийся для каждого пикселя. Примитивно его можно разделить на несколько этапов:

1. конструируется луч, начальной точкой которого будет соответствующий пиксель на экране, а направление − случайным;
2. находится ближайшая точка пересечения луча с геометрией сцены, при отрицательном результате возвращаемся на пункт 1;
3. конструируется новый луч из точки пересечения в направлении к выбранному из нескольких источнику света, и если пересечений нет, рассчитывается прямое освещение;
4. рассчитывается вторичное освещение: конструируем новый луч из точки пересечения в произвольном направлении, переходим к пункту 2, пока не достигнуто максимальное количество отражений.

Используемый при вычислении энергетической яркости метод Монте-Карло[2] для прямого и вторичного освещения при заданных плотностях вероятности дает следующие оценки соответственно:

$$\left\langle L_{\text{direct}}(x \to \Theta) \right\rangle = \frac{L_e(y_i \to \bar{y}_i \bar{x}) f_r(x, \Theta \leftrightarrow \overline{xy_i}) G(x, y_i) V(x, y_i)}{p_L(k) p(y_i \mid k)} \tag{3}$$

$$\left\langle L_{\text{indirect}}(x \to \Theta) \right\rangle = \frac{L_r(r(x,\Psi) \to -\Psi) f_r(x, \Theta \leftrightarrow \Psi) \cos(N_x, \Psi)}{p(\Psi)} \tag{4}$$

где $p_i(k)p(y_i|k)$ – комбинированная плотность вероятности для выбора случайной точки y_i на объединенной поверхности источников; $p(\Psi)$ – плотность вероятности случайных направлений Ψ на полусфере.

Представленный выше метод для вычисления энергетической яркости, основывается на физических законах распространения и взаимодействия света с объектами, что позволяет назвать моделирование, использующее данный метод, физически корректным [2]. Все существующие физически корректные модели можно условно разделить на два класса: смещенные (biased) – допускающие систематическую ошибку при накоплении кадров в финальном изображении и несмещенные (unbiased). Разработанная графическая система расчета глобального освещения, использует физически корректную модель освещения, визуализация объектов происходит без смещения конечного изображения. Разработанная на языке GLSL (OpenGL Shading Language), данная система позволяет задействовать для расчетов графический процессор (GPU), выполняющих графический рендеринг. Моделирование материала объекта осуществляется путем изменения соответствующих параметров отраженного луча так, что можно получить диффузную, глянцевую и зеркальную поверхность, либо их комбинацию.

Для оценки производительности воспроизводились сцены, получившие широкое распространение при анализе методов глобального освещения. Визуализация производилась на GPU NVIDIA GeForce 460 GTX под управлением ОС Kubuntu Linux 11.10 и выполнялась в разрешении 768×768. По результатам проведенных измерений можно сделать вывод, что представленная интерактивная реализация метода стохастической трассировки путей на GLSL, хоть и не обладает эффективной скоростью сходимости, но имеет весьма высокую скорость визуализации и хорошую точность.

[1] Kajiya J.T. The Rendering Equation // SIGGRAPH Comput. Graph. 1986. V.20, No.4, P.143.
[2] Dutre P., Bala K., Bekaert P. Advanced Global Illumination – Wellesley, Massachusetts: A K Peters Ltd, 2006, 366 p.

СРЕДСТВО МОНИТОРИНГА БЕСПРОВОДНЫХ СЕТЕЙ С НАБОРОМ ФУНКЦИЙ ОПОВЕЩЕНИЯ

И.С. Исупов, А.А. Рябов

Нижегородский госуниверситет

В настоящее время в сфере информационных технологий широкое распространение получили беспроводные сети. Их стали использовать очень часто и практически повсеместно, особенно в местах большого скопления людей. В связи с этим весьма актуальным стал вопрос защищенности беспроводных сетей, как для локальных (домашних), так и для корпоративных пользователей (на крупных предприятиях, в банках, в компаниях, предоставляющих информационные услуги).

В проводной части локальной сети уже создано большое количество систем обнаружения вторжений со всевозможными структурами защиты и анализа сети, тогда как в беспроводной её части выбор способов защиты весьма ограничен. Целью работы является создание приложения для UNIX-систем на основе программного пакета Aircrack-ng 1.1 [1], способного анализировать беспроводные сети и оказывать помощь в мониторинге беспроводных сетей.

Создаваемое приложение основано на консольном программном продукте Aircrack-ng 1.1 и включает в себя следующие основные функции:

- мониторинг всех беспроводных сетей, находящихся в радиусе действия приёмной антенны (BSSID, ESSID, номер канала, мощность, вид шифрования);
- мониторинг всех беспроводных устройств, находящихся в радиусе действия приёмной антенны (BSSID точки, к которой подключено, MAC устройства, мощность, количество передаваемых/потерянных пакетов, беспроводную сеть, к которой пытается подключиться);
- мгновенное отключение пользователя от любой беспроводной сети (например, в момент определения попытки взлома);
- запись и отображение всех событий, которые происходят в беспроводной сети (только для определенной/выбранной сети; подключение пользователя к сети, появление нового пользователя, исчезновения пользователя);
- создание правил для вновь появившихся пользователей (например, заносить пользователя в черный список, до выяснения его происхождения);
- управление пользователями в соответствии с правилами списков (чёрный, белый);
- возможность ввести для определённого пользователя дополнительную информацию (Иван Сергеевич – начальник смены производственного цеха).

В разрабатываемом приложении можно отметить следующие положительные качества:

- помогает системным администраторам предотвратить попытки взлома;
- создаёт список пользователей, подключенных к определённой сети;
- даёт просматривать подробную информацию о каждом пользователе;

Кроме того можно отметить и ряд недостатков, а именно:

- приложение работает только с определёнными адаптерами, которые поддерживают приложение Aircrack-ng 1.1;
- мгновенное отключение пользователя от определённой сети выполняется посредством непрерывной посылки ему пакетов на переподключение к сети от имени точки доступа, путём подмены физического адреса;
- для более полной информации необходимо иметь устройство с возможностью подключения внешней антенны (чтобы охватить всю зону покрытия сети);
- для работы приложения нужен отдельный компьютер с беспроводным интерфейсом и UNIX системы.

Таким образом, разработан удобный инструмент администратора беспроводной сети. В дальнейшем планируется его модернизация с целью устранения (уменьшения) перечисленных выше недостатков.

[1] Домашняя страница программы Aircrack-NG: http://www.aircrack-ng.org.