Надежность любой системы криптографической защиты информации (СКЗИ) в значительной степени определяется качеством используемых генераторов случайных и псевдослучайных последовательностей. Генератор, используемый в СКЗИ, должен порождать выходную последовательность, неотличимую от равномерно распределенной случайной последовательности (РРСП) [1]. Для обнаружения отклонения от модели РРСП используются статистические тесты. Статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются заключения о степени близости свойств анализируемой случайной последовательностей и РРСП.

Для выявления зависимостей высокого порядка и выявления скрытых зависимостей требуются дополнительные исследования. Основными математическими моделями, используемыми в таких исследованиях, являются марковские модели. В НИИ ППМИ БГУ были разработаны методы и алгоритмы статистического тестирования выходных последовательностей, основанные на цепи Маркова порядка $s$ с $r$ частичными связями (ЦМ($s$, $r$)) и цепи Маркова условного порядка (ЦМУП).

Данный доклад посвящен разработке программного комплекса, реализующий эффективные алгоритмы статистического анализа выходных последовательностей, основанные на оценивании таких марковских моделей, как однородная цепь Маркова, однородная цепь Маркова порядка $s$, скрытая марковская модель, двойная марковская модель.

**Литература**

1. Криптология / Ю.С Харин [и др.]. Минск: БГУ, 2013. 511 с.

## СВЕТОДИОДНЫЕ СИСТЕМЫ ВЫСОКОЙ МОЩНОСТИ НА АЛЮМИНИЕВОЙ ПЛАТЕ С КОМБИНИРОВАННЫМ ДИЭЛЕКТРИКОМ

Т.Х. Динь, И.А. Врублевский, К.В. Чернякова, А.К. Тучковский

Обеспечение оптимальных температурных режимов работы активных радиоэлектронных элементов является одной из наиболее важных задач при разработке конструкций плат с высоким тепловыделением. Это особенно актуально для светодиодных модулей освещения высокой мощности. Теплота, выделяемая при *p-n* переходе светодиода, проходит от корпуса элемента к теплоотводу, а затем рассеивается в окружающем пространстве. При перегреве светодиода значительно уменьшается эффективность его светоотдачи: падает световой поток, изменяется цветовая температура, и срок службы светодиода сокращается в несколько раз. Поэтому в случае плат с высоким тепловыделением очень важно обеспечить максимальное рассеивание выделяемой теплоты. Решение этой задачи зависит от характеристик печатной платы, которые определяются как конструктивными особенностями платы, так и материалом, из которого она изготовлена. Один из способов снижения уровня тепловой нагруженности плат и эффективного отвода тепла от электронных компонентов является использование печатных плат с алюминиевым основанием.

В данной работе в качестве диэлектрического покрытия плат с алюминиевым основанием использовался комбинированный диэлектрик, состоящий из слоя пористого анодного оксида алюминия и слоя препрега, стеклоткани, пропитанной эпоксидными смолами. С целью повышения теплопроводности в слой препрега вводился керамический наполнитель. Для этого были использованы различные керамические наполнители с высокой теплопроводностью – порошки оксида алюминия, нитрида бора, оксида магния, оксида цинка и оксида титана. Тепловые характеристики печатных плат на алюминиевом основании с диэлектрическим покрытием на основе комбинированного диэлектрика исследовались с помощью термограмм поверхности, получаемых с использованием тепловизионных измерений.

## ПРЕДСКАЗАНИЕ ОЦЕНОК CVE УЯЗВИМОСТЕЙ НА ОСНОВЕ ИХ ТЕКСТОВОГО ОПИСАНИЯ

А.К. Доронин, В.А. Липницкий

В мире с каждым днем появляются все новые уязвимости компьютерных систем. Американская национальная база данных уязвимостей CVE содержит около 100000 записей

о различных уязвимостях компьютерных систем почти за 20 лет развития компьютерных технологий [1]. Каждой уязвимости экспертами выставлены оценки от 0 до 10. Кроме того, содержится краткое словесное описание всех уязвимостей. Современные методы машинного обучения позволяют автоматизировать процесс выставления оценок и могут помочь найти закономерности в появлении наиболее опасных (критических уязвимостей). Использовав векторные представления слов (например, использовав словарь алгоритма GloVe [2], представляющий 400000 слов английского языка в 50-мерном векторном пространстве), получена возможность применения методов машинного обучения к задаче автоматизированного выставления оценок на основе их текстового описания. В частности, разработана модель, использующая в своей основе многослойную нейронную сеть с 2 выходами. На вход подается список из слов в виде соответствующих им индексов из словаря GloVe. Далее следуют три сверточных слоя, после них – 3 полносвязных слоя. Между тремя полносвязными слоями имеется слой, исключающий 40 % данных для лучшего обучения нейронов. По существу, построенная нейронная сеть решает задачу бинарной классификации: выход 0 означает оценку меньше 7,5, выход 1 – оценку от 7,5 до 10 включительно. Таким образом мы решили увеличить точность предсказания, оставив вместо 10 классов всего 2. После 10 эпох обучения точность модели (accuracy) на отложенной выборке составила 85 %, площадь под AUC-ROC кривой – 91 %. Дальнейшие исследования, вероятно, могут улучшить данный результат.

**Литература**

1. National Vulnerability Database [Электронный ресурс]. – URL: https://nlp.stanford.edu/projects/glove/ (дата обращения: 16.05.2018).

2. GloVe: Global Vectors for Word Representation [Электронный ресурс]. – URL: https://nlp.stanford.edu/projects/glove/ (дата обращения: 16.05.2018).

## ВИРТУАЛЬНАЯ ЛАБОРАТОРНАЯ РАБОТА ПО ОЦЕНКЕ УЯЗВИМОСТИ ХРАНЕНИЯ ПАРОЛЕЙ В БРАУЗЕРАХ НА ОСНОВЕ ДВИЖКА CHROMIUM

И.А. Евсеенко

В настоящее время каждый пользователь Интернета имеет пароли для множества учетных записей, начиная от социальных сетей и завершая онлайн-банкингом. Одним из наиболее распространенных способов хранения паролей является система хранения в браузерах. Виртуальная работа рассматривает ситуацию, когда нужно сделать резервную копию всех паролей браузера, или нужно вспомнить давно забытые пароли, которые сохранены в браузере. Однако с другой стороны эта ситуация рассматривается как модель злоумышленника для кражи паролей в браузере.

Браузеры на движке Chromium используют систему шифрования Data Protection Application Programming Interface (DPAPI). В виртуальной лабораторной работе демонстрируются 2 режима: с использованием машинного ключа и с использованием ключа пользователя. Предусмотрена демонстрация принципа работы DPAPI, суть которой заключается в следующем. Приложение обращается к операционной системе задавая параметры Mysecret и Entropy. На выходе получаем BLOB. Приложение сохраняет его, а в дальнейшем, при необходимости, расшифровывает. DPAPI также включает криптопровайдер – это набор алгоритмов для хеширования, шифрования, ключевого обмена и ЭЦП в форме модуля и криптопровайдер объединяет их. Например, в РФ приняты ГОСТовские алгоритмы, поэтому если передать его системе, то вместо стандартных AES, SHA, RSA будут использоваться Российские ГОСТы шифрования. Все это настраивается в реестре. Для DPAPI нет разницы с какими алгоритмами работать, что делает систему универсальной.

Оценка уязвимости по перехвату и расшифровке паролей предусматривает два варианта выполнения: с использование существующих программ и написание студентами программы для расшифровки паролей как на языке высокого уровня, так и на скриптовых языках.

В данной работе рассмотрены возможные негативные последствия использования системы хранения данных в браузерах для авторизации и проведена оценка уязвимости с разработкой специализированного программного обеспечения в рамках лабораторных работ по дисциплине «Защита информации» специальности 09.03.04 «Программная инженерия» БРУ.