Правила оформления статей

Текстовый редактор: MS Word for Windows. **Имя файла** – фамилия автора на русском языке.

**Правила оформления текста**

– материалы статьи представляются в объеме от 3 полных страниц формата А4;

* параметры страницы: поля – левое, правое, верхнее и нижнее 2,2 см; колонтитулы отсутствуют.
* шрифт Times New Roman 15 pt, выравнивание по ширине, абзацный отступ 1 см, межстрочный интервал – 1,2.
* в тексте могут содержаться цветные или черно-белые рисунки. Элементы рисунка, выполненного с помощью Word «Вставка-Фигуры», должны быть сгруппированы. Если в тексте используются рисунки точечных форматов (\*.bmp, \*.jpeg) они должны иметь разрешение не менее 600dpi. Рисунки подписываются следующим образом <Рисунок 1 **-** Название рисунка >, подпись размещается снизу, по центру рисунка. В тесте должна быть ссылка на рисунок в виде «рисунок 1». Если рисунок один, то номер в обозначении не ставится;
* в тексте могут содержаться таблицы. Таблицы подписываются следующим образом <Таблица 1 **-** Название таблицы >, подпись размещается сверху таблицы, выравнивание по центру. В тексте должна быть ссылка на таблицу в виде «таблица 1». Если таблица одна, то номер в обозначении не ставится;
* формулы подготавливаются в встроенном редакторе формул Microsoft Word или в редакторе MathType. Все впервые встречающиеся в формуле обозначения должны быть расшифрованы сразу после формулы. Нумеруются только те формулы, на которые делаются ссылки в тексте. При нумерации формул использование букв и других символов не допускается. Вынесенные в отдельную строку формулы выравниваются посередине строки, номер заключается в круглые скобки и выравнивается по правому краю текста, как показано ниже:

, (1)

* шрифтовое начертание обозначений в формулах, в таблицах и в основном тексте должно быть полностью идентичным. Ссылки на формулы и таблицы даются в круглых скобках, ссылки на использованные источники (литературу) - в квадратных скобках, например, [3].

**Элементы заглавия публикуемого материала (шрифт полужирный)**

* УДК (выравнивание по левому краю)
* название статьи (заглавными полужирными буквами, выравнивание по центру).
* перечень авторов через одну строку (Фамилия, имя, отчество полностью, затем после запятой, ученая степень, должность, например – к.т.н., доцент; аспирант; студент; д.т.н., профессор; ст. преподаватель; к.э.н., ассистент), выравнивание по центру.
* аннотация и ключевые слова размещается с полями слева и справа – 2 см от края основного текста, абзацный отступ – 0,5 см, шрифт такой же как и в тексте, слова «Ключевые слова» выделить курсивом.
* **продублировать на английском языке название, авторов без указания** степени, должности через запятую на одной строке, аннотацию и ключевые слова. Перевод на английский язык должен быть тщательно выверен;
* каждый элемент заглавия приводится с пропуском одной строки от предыдущего элемента (см. пример оформления статьи).
* строка с текстом «Список литературы» через одну строку после основного текста.
* собственно список литературы: каждая ссылка с номером в отдельном абзаце. Выполняется по ГОСТ 7.1-2003. Библиографическое описание документа. Введ. 01.07.2004. М.: Изд-во стандартов, 2004.
* возможны ссылки на материалы, размещенные в сети Интернет (см. пример оформления элементов списка литературы ниже)
* приводятся только источники, на которые есть ссылки в тексте.

**Пример оформления элементов списка литературы.**

1. Иванов И.С. Банковское дело. – М.: Экономика, 2007. – 181 с.

2. [Теплых С.Ю.](http://elibrary.ru/author_items.asp?refid=241449789&fam=%D0%A2%D0%B5%D0%BF%D0%BB%D1%8B%D1%85&init=%D0%A1+%D0%AE), [Горшкалев П.А.](http://elibrary.ru/author_items.asp?refid=241449789&fam=%D0%93%D0%BE%D1%80%D1%88%D0%BA%D0%B0%D0%BB%D0%B5%D0%B2&init=%D0%9F+%D0%90), [Саргсян А.М.](http://elibrary.ru/author_items.asp?refid=241449789&fam=%D0%A1%D0%B0%D1%80%D0%B3%D1%81%D1%8F%D0%BD&init=%D0%90+%D0%9C) Современное состояние вопроса сбора и очистки поверхностного стока с железной дороги // [Научное обозрение](http://elibrary.ru/contents.asp?titleid=27971). 2014. № 4. С. 123-129.

3. Справочная книга по светотехнике / Под ред. Ю.Б. Айзенберга. – М.: Знак, 2010. – 972 с.

4. Костенко Е.М. Метод построения оптимальных планов многофакторного эксперимента на основе символьных последовательностей // Современные научные исследования и инновации. 2013. № 3 [Электронный ресурс]. – Режим доступа <http://web.snauka.ru/issues/2013/03/23024> (дата обращения: 11.02.12).

5. Рынок тренингов Новосибирска: своя игра / [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

6. Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: автореф. дис. ... канд. техн. наук. – Новосибирск, 2000. – 18 с.

7. Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкого региона : дис. ... канд. полит. наук. – М., 2002. – 267 с.

8. Ланских Д.М. Разработка ландшафтного плана как необходимое условие устойчивого развития города // Экология ландшафта и планирование землепользования: тезисы докл. Всерос. конф. (Иркутск, 11-12 сент.2012г.). Пенза, 2000. С.125–128.

9. Оптико-электронный аппарат // Патент РФ № 2122745. 1998. Бюл. № 33. / Еськов Д.Н., Бонштедт Б.Э., Корешев С.Н.

**Образец**

**УДК 004.451.9**

**ОЦЕНКА УЯЗВИМОСТЕЙ МОБИЛЬНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID МЕТОДОМ РЕГРЕССИОННОГО АНАЛИЗА**

**Меликов К.М., к.т.н., доцент**

**Сардаров Р.Т., студент**

Проведен анализ открытой мобильной операционной системы Android, базирующейся на ядре Linux, на подверженность воздействию вредоносного программного обеспечения. На базе статистических данных по динамике появления новых вредоносных продуктов построен прогноз дальнейшего распространения угроз для операционной системы Android с использованием регрессионной модели.

*Ключевые слова:* операционная система Android, регрессионная модель, уязвимость, вредоносное программное обеспечение.

Количество приложений, созданных для работы в среде операционной системы (ОС) Android, с каждым годом растет лавинообразно, вместе с тем это открывает широкие возможности для злоумышленников создавать и внедрять вредоносное программное обеспечение (ПО), предназначенное, во-первых, для хищения персональных данных пользователей, во-вторых, для хищения денежных средств, как со счета мобильного телефона, так и со счетов электронных платежных систем[1].

Однако многие владельцы смартфонов и планшетов продолжают игнорировать киберугрозы. Согласно исследованиям, проведенным «Лабораторией Касперского» совместно с компанией B2B International в 2014 году, почти половина мобильных устройств в России, а именно 46% смартфонов и 41% планшетов Android, не защищены никаким антивирусным продуктом, 26% смартфонов и 18% планшетов не защищены даже паролем (таблица).

Стоит напомнить о некоторых видах вредоносного ПО, делающих приложения на базе ОС Android весьма уязвимыми. Например, появились программы, способные получать доступ к информации на SD-карте, собирать данные о пользователе и отправлять информацию на удаленный сервер; программы, использующие микрофон мобильного устройства, при помощи специального алгоритма распознающие номера кредитных карт и данные для их использования [2, 3].

Таблица – Динамика роста компьютерных угроз за 2011-2015 гг.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Годы | 2011 | 2012 | 2013 | 2014 | 2015 |
| Количество угроз, тыс. | 1350 | 1456 | 1567 | 1876 | 2063 |

На базе статистических данных по динамике появления новых вредоносных продуктов построен прогноз дальнейшего распространения угроз для ОС Android с использованием регрессионной модели (рисунок). Прогнозная кривая в виде степенной функции

*y* = 5298,5*x*1,281

показана пунктирной линией, достоверность аппроксимации составляет *R*2=0,834. Согласно прогнозу количество вредоносных программ для ОС Android может достигнуть к середине 2015 года более 134 тыс.

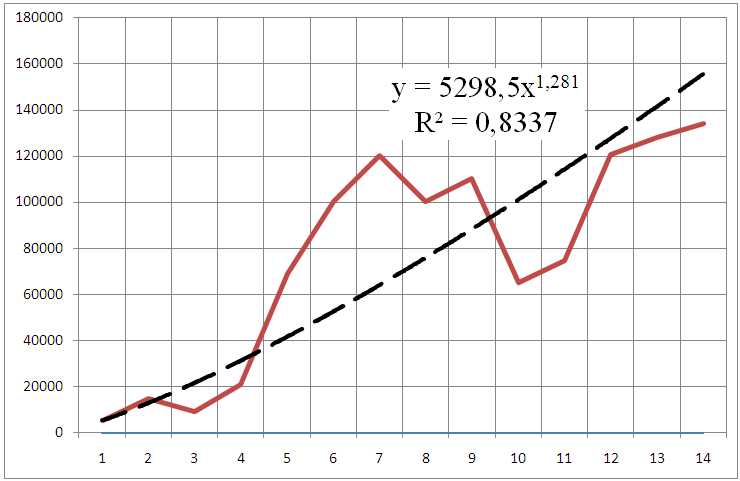
****

Рисунок – Прогноз появления вредоносных программ для ОС (точки 12, 13, 14), построенный в виде регрессионной модели

На основе экспертного опроса специалистов IT-безопасности составлен классификатор, отражающий значимость уязвимостей ОС Android по шкале 0…1. В качестве мер предлагается ужесточение политики безопасности, тщательное слежение за безопасностью разрабатываемого ПО и за контентом, предлагаемым пользователям для установки на AndroidMarket.

**Список литературы**

1. Сорокин И.В. Вредоносное программное обеспечение в среде Android. – М.: Форум, 2013. – 342 с.

2. Незнание не освобождает: более трети российских пользователей не задумываются об угрозах для мобильных устройств / [Электронный ресурс]. – Режим доступа: http://www.kaspersky.ru/about/news/virus/2015/ (дата обращения: 06.03.15).

3. Голиков Г.В. Экспертный метод оценки уязвимостей операционных систем // Вестник Дагестанского государственного технического университета. Технические науки. – 2013. – Т.1. – № 28. – С. 24-36.

Автор несет личную ответственность за оригинальность текста, а также за достоверность приведенных данных и точность цитируемых текстов.

|  |
| --- |
| **Заявка на участие в конференции**  Фамилия |
| Имя |
| Отчество |
| Место работы |
| Должность |
| Ученая степень |
| Звание |
| Адрес  (для высылки сборника) |
| Контактный телефон |
| E-mail |
| Тема доклада |
| Направление |
|  |

|  |
| --- |
|  |
|  |

***Благодарим за проявленный интерес и надеемся***

***на плодотворное сотрудничество.***