СПИСОК ЛИТЕРАТУРЫ:

1. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000. — 448 с.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4 (18). С. 116–121.

REFERENCES:

1. *Sachkov V.N., Tarakanov V.E.* Kombinatorika neotricatelnih matric. M.: TVP, 2000. — 448 p.
2. *Kogos K.G., Fomichev V.M.* Polojitelnie svoystva neotricatelnih matric // Prikladnaya diskretnaya matematika. 2012. № 4 (18). P. 116–121.

I. M. Azymshin, V. O. Chukanov

The Methods of Determining the Probability of Appearance of Error for Modified Reliability Models of Software by Jelinski — Moranda and Schick — Wolverton

Key words: software reliability

In the modified models Jelinski — Moranda and Schick-Wolverton probabilities of errors are used. This article discusses the definitions of these probabilities.

И. М. Азымшин, В. О. Чуканов

МЕТОДИКА ОПРЕДЕЛЕНИЯ ВЕРОЯТНОСТИ ПОЯВЛЕНИЯ ОШИБОК ДЛЯ МОДИФИЦИРОВАННЫХ МОДЕЛЕЙ НАДЕЖНОСТИ ПО ДЖЕЛИНСКОГО – МОРАНДЫ И ШИКА – ВОЛВЕРТОНА

В модифицированной модели Джелинского — Моранды и модифицированной модели Шика — Волвертона [1] используются вероятности возникновения ошибок. В данной статье рассматривается вопрос определения этих вероятностей.

В результате проведенных исследований опытным путем было доказано, что соотношение количества ошибок, возникших в результате исправления, ранее обнаруженных, константно на небольшом промежутке времени.

$$\frac{a}{i} = const \ ,$$

где a — количество ошибок, возникших в результате исправления, ранее обнаруженных;

i — общее число исправляемых ошибок.

Из этого утверждения и полученных данных следует, что соотношение количества единичных ошибок к общему числу исправляемых ошибок константно. Аналогично для двоичных, троичных и более ошибок.

$$P_j = \frac{a_j}{i},$$

где a_1 — количество единичных ошибок, возникших в результате исправления, ранее обнаруженных;

i — общее число исправляемых ошибок;

P_j — вероятность возникновения ошибки.

Предлагается методика получения вероятностей возникновения ошибок, основанная на приведенных соотношениях.

Согласно теории разработки программного обеспечения, большие задачи необходимо решать с использованием метода декомпозиции. Учитывая это, можно создать специальную тестовую задачу для группы разработчиков, которая даст возможность оценить качество безошибочного программирования каждого разработчика из команды. Предлагается создать такую тестовую задачу, при которой будут затрагиваться задания, аналогичные задачам, которые потребуются при выполнении требований целевой задачи. Тестовая задача должна включать в себя как разработку отдельных модулей, так и организацию их взаимодействия между собой. Задача должна решаться в 2 этапа. На первом этапе идет разработка ПО, на втором — исправление ошибок. По результатам выполнения тестового задания можно получить вероятности возникновения единичных, двоичных и более ошибок.

Так как все же существует некоторая флуктуация в соотношениях количества ошибок, появившихся в результате исправления ошибок, к общему числу исправляемых ошибок, то вводится коэффициент недоверия. Учитывая, что мы оцениваем интенсивность отказов не точно, а только ее верхнюю границу, предлагается к соотношению количества ошибок, появившихся в результате исправления ошибок, к общему числу исправляемых ошибок прибавлять коэффициент недоверия. Коэффициент недоверия зависит от величины отклонения соотношений ошибок к среднему значению. Таким образом, вероятность возникновения ошибки стоит рассчитывать по формуле:

$$P_j = \frac{a_j}{i} + x \ ,$$

где a_1 — количество единичных ошибок, возникших в результате исправления, ранее обнаруженных;

i — общее число исправляемых ошибок;

P_j — вероятность возникновения ошибки;

x — коэффициент недоверия.

Коэффициент недоверия определяется по методу максимального правдоподобия.

Так как со временем навыки разработки ПО членами команды разработчиков увеличиваются, то рекомендуется пересчитывать вероятности возникновения ошибок. Исходными данными для этого могут служить значения, полученные на предыдущем этапе разработки.

Определение коэффициента опыта команды f. Если команда не меняется на всем протяжении разработки, то коэффициент опыта команды можно приравнять к 1. В случае изменения состава команды надо решить тестовую задачу с участием нового члена команды.

СПИСОК ЛИТЕРАТУРЫ:

1. *Азымшин И. М., Чуканов В. О.* Анализ безопасности программного обеспечения // Безопасность информационных технологий. 2014. № 1. С. 45–47.

2. *Чуканов В. О.* Надежность программного обеспечения и аппаратных средств систем передачи данных атомных электростанций: Учебное пособие. М.: МИФИ, 2008.

3. *Гуров В. В., Чуканов В. О.* Основы теории и организации ЭВМ. М.: БИНОМ. Лаборатория знаний, 2012.

4. *Александрович А. Е., Бородакий Ю. В., Чуканов В. О.* Проектирование высоконадежных информационно-вычислительных систем. М.: Радио и связь, 2004.
5. *Коваленко И. Н., Кузнецов Н. Ю.* Методы расчета высоконадежных систем. М.: Радио и связь, 1988.
6. *Половко А. М., Маликова И. М.* Сборник задач по теории надежности. М.: Советское радио, 1972.
7. *Половко А. М., Гуров С. В.* Основы теории надежности. СПб.: БХВ-Петербург, 2006.
8. *Майерс Г.* Надежность программного обеспечения. М.: Мир, 1980.
9. *Боэм Б., Браун Дж., Каспар Х. и др.* Характеристики качества программного обеспечения. М.: Мир, 1981.
10. *Тейер Т., Липов М., Нельсон Э.* Надежность ПО. М.: Мир, 1981.
11. *Липаев В. В.* Надежность программных средств. М.: СИНТЕГ, 1998.

REFERENCES:

1. *Azymshin I. M., Chukanov V. O.* Analysis of safety of software // Bezopasnost Informatsionnykh Tekhnology. 2014. № 1. P. 45–47.
2. *Chukanov V. O.* Nadezhnost programmnogo obespecheniya i apparatnykh sredstv sistem peredachi dannykh atomnykh elektrostantsy: Uchebnoye posobiye. M.: MEPhI, 2008.
3. *Gurov V. V., Chukanov V. O.* Osnovy teorii i organizatsii EVM. M.: BINOM. Laboratoriya znany, 2012.
4. *Aleksandrovich A. E., Borodaky Yu. V., Chukanov V. O.* Proyektirovaniye vysokonadezhnykh informatsionno-vychislitelnykh sistem. M.: Radio i svyaz, 2004.
5. *Kovalenko I. N., Kuznetsov N. Yu.* Metody rascheta vysokonadezhnykh sistem. M.: Radio i svyaz, 1988.
6. *Polovko A. M., Malikova I. M.* Sbornik zadach po teorii nadyozhnosti. M.: Sovetskoye radio, 1972.
7. *Polovko A. M., Gurov S. V.* Osnovy teorii nadyozhnosti. SPb.: BKhV-Peterburg, 2006.
8. *Myers G.* Software reliability. M.: Mir, 1980
9. *Boem B., Braun Dzh., Kaspar Kh. i dr.* Kharakteristiki kachestva programmnogo obespecheniya. M.: Mir, 1981.
10. *Teyer T., Lipov M., Nelson E.* Nadezhnost PO. M.: Mir, 1981.
11. *Lipayev V. V.* Nadezhnost programmnykh sredstv. M.: SINTEG, 1998.

E. B. Aleksandrova, E. A. Kuznetsova

User Revocation and Joining in the Lattice-based VLR Group Signature

Key words: lattice-based group signature, verifier local revocation, joining

Modified lattice-based VLR group signature is proposed, allowing user's signature revocation and joining the new group member. This new scheme guarantees selfless anonymity and traceability.

Е. Б. Александрова, Е. А. Кузнецова

ОТЗЫВ И ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯ В РЕШЕТОЧНОЙ VLR-СХЕМЕ ГРУППОВОЙ ПОДПИСИ

В ряде прикладных областей для защиты информации требуется анонимное подтверждение ее достоверности. Для решения этой задачи используются специальные схемы цифровой подписи, обеспечивающие анонимность подписывающего, – групповые подписи [1].

Важными составляющими протокола групповой подписи являются процедуры отзыва права подписи и добавления пользователя в группу. Наиболее эффективным вариантом отзыва является отзыв, локальный для проверяющего (verifier local revocation, VLR). В таких схемах сообщения, содержащие информацию об отозванных членских сертификатах, обрабатываются только проверяющими. Основным преимуществом VLR-схем групповой подписи является