УДК 004.056

Е. В. БРЕЖНЕВ, В. В. БОРОДАВКА, Р. В. САЛАХОВ

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

РАЗРАБОТКА МЕТОДА НЕЧЕТКОГО ОЦЕНИВАНИЯ РИСКОВ КИБЕРБЕЗОПАСНОСТИ ТРАНСПОРТНЫХ СРЕДСТВ

Предлагается метод оценивания рисков кибербезопасности транспортных средств (ТС), который основан на использовании многоуровневого нечёткого вывода (Multi Fuzzy Inference System – MFIS), позволяющего снизить требования к полноте статистических данных, характеризующих отдельные элементы модели (угрозы, риски, активы, пр.), а также получить нечеткие оценки рисков кибербезопасности ТС, прогнозировать последствия взаимного влияния компонентов системы, а также сформировать множество контрмер, направленных на повышение кибербезопасности. Метод основан на модели угроз и рисков, учитывающей взаимовлияние между рисками активов и контрмерами, а также между узлами ТС и риск-факторами.

Ключевые слова: *кибербезопасность, транспортное средство, риск-анализ, угроза.*

Введение

Анализ направлений развития современной автомобильной индустрии демонстрирует тенденцию к усложнению движущихся технических средств (ТС), их трансформацию из примитивного механизма в "компьютер на колёсах". По оценкам специалистов, в 2014 г. число электронных блоков (узлов) на ТС составляет от 19 (SRT Viper) до 98(Range Rover) [1]. Все эти блоки активно взаимодействуют друг с другом, а также передают данные официальным дилерам, сервисам и прочим наблюдателям.

Однако внедрение информационных технологий (ИТ) в ТС также приводит к появлению новых видов угроз и уязвимостей. Так, например, в 2013 и 2015 году проводились тестирования кибербезопасности [2], в результате которых были получены данные об типовых уязвимостях ТС. В первом случае атака была проведена через подключение к бортовой сети автомобиля (OBD-II), а во втором - беспроводным путём [3].

Таким образом, двойственная роль ИТ обуславливает актуальность проблемы кибербезопасности ТС, поскольку помимо комфорта и других преимуществ, ИТ увеличивают риски, связанные с безопасностью ТС, пассажиров и других участников дорожного движения.

Проблема кибербезопасности ТС

Перечень основных критически важных для безопасности узлов ТС представлен на рис. 1.

В совокупности все узлы ТС образуют полноценную информационную систему (ИС) [4], которая без учета аспекта кибербезопасности является уязвимой для кибератак.

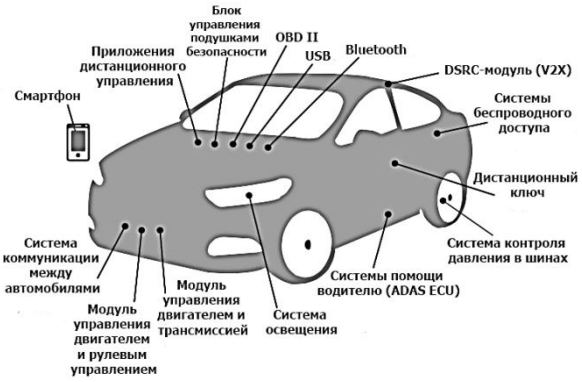

Рис. 1. Перечень основных критически важных узлов ТС

Анализ модели внутренней узловой архитектуры ТС (рис. 2, слева) подтверждает предположение, что обеспечение безопасности одного из главных узлов не может гарантировать безопасность ТС в целом, поскольку все узлы связаны с центром управления ТС по прямым каналам связи.

Вторая модель (рис. 2, справа) является менее уязвимой, поскольку, например, при доступе к модулям беспроводной связи, доступ к остальным системам остаётся невозможным, т.к. все узлы объединены в отдельные блоки, не связанные между собой.

Автомобильные концерны выпускают ТС с первой моделью узловой архитектуры [5], которая является небезопасной и имеет высокую вероятность взлома.

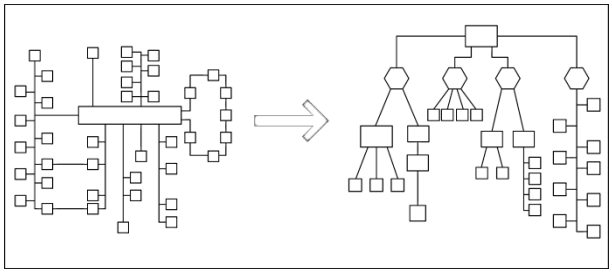

Рис. 2. Модели архитектуры ТС

Анализ подходов и методов риск-анализа кибербезопасности ТС

Под кибербезопасностью ТС понимается поддержание свойств безопасности его ресурсов, пользователей, гарантии, набор средств, которые используются для защиты киберсреды ТС [6].

Риск кибербезопасности ТС представляет собой возможность использования ее уязвимостей с целью вторжения и нанесения ущерба. На сегодняшний день отсутствуют какие-либо стандарты, регулирующие допустимые уровни рисков кибербезопасности ТС [7]. Современные методы оценки рисков подразделяются на две категории – количественные и качественные (рис.3).

Количественные методы анализа рисков основываются на оценке риска для каждой угрозы по двум параметрам:

1. Вероятность реализации вторжения за определённый период времени.

2. Величина ущерба в случае успешной реализации вторжения.

Качественные оценки рисков, в отличие от количественных, не предусматривают расчёт точных значений параметров. Оценки выражаются качественными параметрами, такими как "Высокая", "Средняя" или "Низкая" [8].

К наиболее популярным программным методикам (ПМ) оценивания рисков можно отнести CRAMM, ГРИФ, RiskWatch, CORAS, MSAT, FuzzyLogic [9].

Информационно-логические модели систем, построенные на основе теории нечётких множеств и нечёткой логики, находят широкое применение в приложениях управления, принятия решений, системного моделирования, где алгоритмы принятия решений, эвристические алгоритмы управления, знания относительно функционирования рассматриваемого объекта обобщаются и представляются в виде множества нечётких логических правил.

В данной работе предлагается использовать качественный метод анализа рисков на основе нечёткой логики, поскольку на данный момент в свободном доступе отсутствует статистическая информация о реализации различных видов атак на ТС, а также данный метод предоставляет достаточную оценку для принятия контрмер по предотвращению угроз.

Цель работы – повышение точности и достоверности оценки кибербезопасности ТС путём разработки метода, учитывающего ограничения по статистике киберинцидентов ТС.

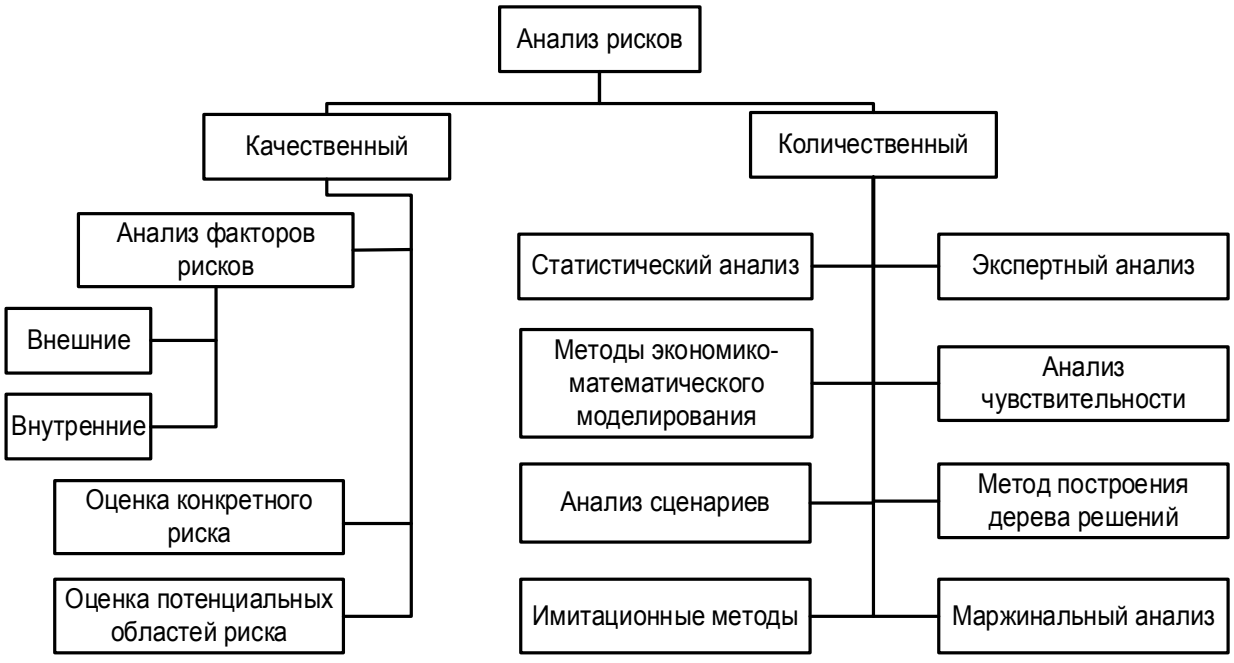

Рис. 3. Существующие методы анализа рисков

Этапы метода нечёткого оценивания кибербезопасности ТС

Злоумышленники и хакеры могут проникнуть в систему ТС как удалённо, так и непосредственно при помощи его интерфейсов [10], что может привести к ущербу. Модель угроз и рисков приведена на рис.4.

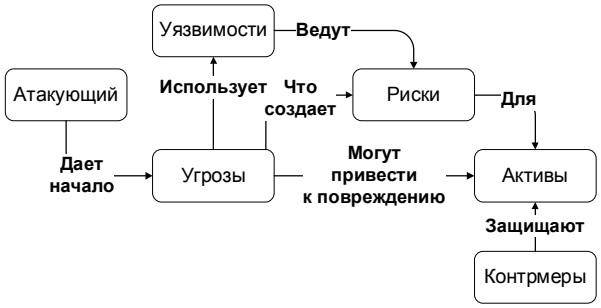

Рис. 4. Модель угроз и рисков

Модель риска позволяет сформировать зависимости между параметрами нечёткого вывода, используемого для получения оценок риска.

Метод нечёткой оценки кибербезопасности ТС разработан с использованием нескольких FIS - Multi Fuzzy Inference System (MFIS) [11], для определения степени риска, используя факторы, связанные с каждым риском. Основные этапы метода приведены на рисунке 5.

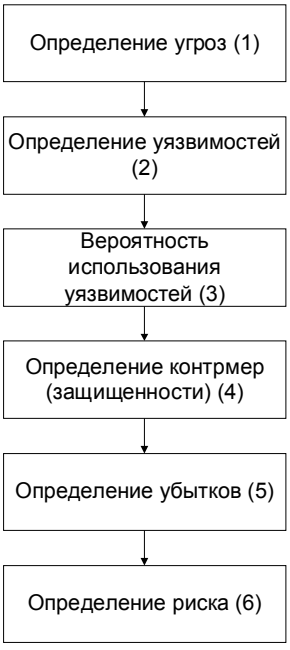

Рис. 5. Основные этапы метода

В предлагаемом методе MFIS используется Mamdani Fuzzy Models, так как она лучше всего подходит для адаптации метода.

Риски зависят от уязвимостей ТС (Vulnerability), вероятности использования этих уязвимостей (Action likelihood), и, наконец, вероятности успеха (Success likelihood).

Предлагается оценить риски в зависимости от каждой лингвистической переменной: {Overall Capabilities, (High, Moderate, Low), trapmf, trimf}, {Overall Likelihood, (High, Moderate, Low), trapmf, trimf}, остальные по аналогии, где общие возможности – Overall Capabilities, общая вероятность атаки – Overall Likelihood, безопасность (контрмеры) - Security, возможности атаки на уязвимость – Possible and probable, воздействие на активы - Impact, High – высокий уровень, Moderate – средний уровень, Low – низкий уровень, trapmf - трапециевидная функция принадлежности, trimf – треугольная функция принадлежности.

На основе модели угроз и рисков, представленной на рисунке 4, предлагается MFIS, которая состоит из пяти систем нечёткого вывода для оценки риска, как показано на рис. 6.

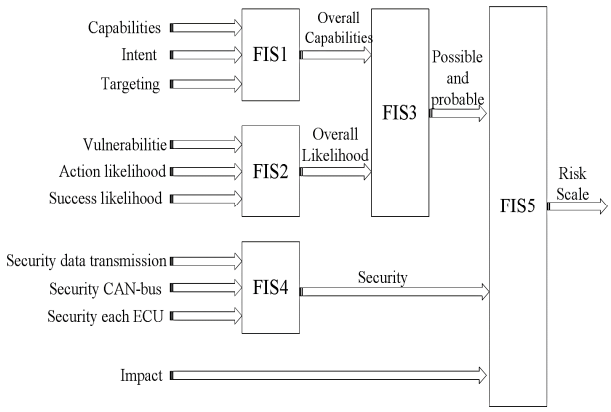

Рис. 6. Предлагаемая Multi Fuzzy Inference System (MFIS)

Первому этапу метода (см. рис. 5) соответствует первая нечёткая система логического вывода (FIS1), которая вычисляет Overall Capabilities источника угрозы (экстремистская группа, террористическая группа, хакер или группа хакеров) на основе (возможностей, намерений и ориентации).

Второму этапу метода (см. рис. 5) соответствует вторая система нечёткого логического вывода (FIS2), которая вычисляет Overall Likelihood угрозы в результате воздействия злоумышленника на основе факторов риска (уязвимости, воздействия на уязвимость и вероятности успеха).

Третьему этапу метода (см. рис. 5) соответствует (FIS3), которая вычисляет Possible And Probable уязвимости на основании выхода (FIS1) и (FIS2).

Четвёртому этапу метода (см. рис. 5) соответствует (FIS4), которая вычисляет Security ТС на основе (уровня защищённости передачи данных,

уровня защищённости CAN-шин, уровня защищённости отдельных ECU).

Шестому этапу метода (см. рис. 5) соответствует (FIS5), которая вычисляет Risk Scale на основании выхода FIS3, FIS4 и уровня воздействия события угрозы, то есть величина ущерба, который можно ожидать (Impact), который соответствует пятому этапу метода (см. рис. 5).

Все нечёткие переменные выражаются грамматически в термах нечётких множеств, «Low», «Moderate», «High», как показано на рис. 7.

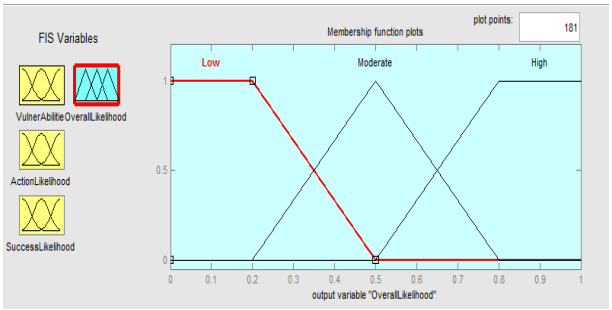

Рис. 7. Термы нечётких множеств

В этом исследовании функции принадлежности лингвистических термов характеризуются трапециевидной функцией принадлежности для «Low» и «High» и треугольной функцией принадлежности для «Moderate», поскольку именно такой набор функций позволяет дать оценку, наиболее приближенную к количественным методам оценивания [12]. Таблицы 1, 2, …, 6 показывают значение термов функций принадлежности для каждого выхода MFIS.

Таблица 1

Overall Capabilities

Терм	Значение
High (H)	Злоумышленник имеет высокий уровень знаний, ресурсы и возможности для поддержки нескольких успешных скоординированных атак.
Moderate (M)	Злоумышленник имеет умеренные ресурсы, опыт и возможности для нескольких успешных атак.
Low (L)	Злоумышленник имеет ограниченные ресурсы, опыт и возможности для поддержки успешной атаки.

Данный метод реализован при помощи Matlab Fuzzy Toolbox, на основе применения умышленного сценария атаки на рис. 4. Редактор FIS в Fuzzy Toolbox используется для определения ввода, вывода переменных для FIS1, FIS2, FIS3, FIS4 и FIS5, как показано на рис. 9 и рис. 10 соответственно (FIS2, FIS3, FIS4 по аналогии с FIS1 и FIS5).

Таблица 2

Overall Likelihood

Терм	Значение
High (H)	Злоумышленник с высокой вероятностью использует уязвимость для успешной атаки.
Moderate (M)	Злоумышленник с умеренной вероятностью использует уязвимость для успешной атаки.
Low (L)	Злоумышленник вряд ли использует уязвимость для успешной атаки.

Таблица 3

Security

Терм	Значение
High (H)	Высокий уровень защищённости ECU, интерфейсов, CAN-шин, каналов передачи в ТС.
Moderate (M)	Умеренный уровень защищённости ECU, интерфейсов, CAN-шин, каналов передачи в ТС.
Low (L)	Низкий уровень защищённости ECU, интерфейсов, CAN-шин, каналов передачи в ТС.

Таблица 4

Possible and probable

Терм	Значение
High (H)	Злоумышленник имеет высокую вероятность для успешной атаки на выявленную уязвимость.
Moderate (M)	Злоумышленник имеет среднюю вероятность для успешной атаки на выявленную уязвимость.
Low (L)	Злоумышленник имеет низкую вероятность для успешной атаки на выявленную уязвимость.

Таблица 5

Impact

Терм	Значение
High (H)	Событие угрозы может привести к серьезным или катастрофическим неблагоприятным последствиям.
Moderate (M)	Событие угрозы может привести к умеренным негативным последствиям.
Low (L)	Событие угрозы может привести к незначительным отрицательным последствиям.

Кроме того, чтобы указать нечёткие операции, такие как AND (min) и OR (max), и методы, используемые для определения Implication (min), Aggregation (max), and Defuzzification (centroid). После этого используется Rule Editor (редактор правил) FIS для

редактирования, добавления, удаления или изменения правил. Редактор FIS также может быть использован для изменения типа подключения (AND, OR) и веса (важности) в правилах, значение по умолчанию равно 1 (т.е. weight (вес) = 1).

Таблица 6

Risk Scale

Терм	Значение
High (H)	Данный риск означает, что событие угрозы может привести к серьёзным или катастрофическим последствиям для ТС, пассажиров и других участников дорожного движения.
Moderate (M)	Данный риск означает, что событие угрозы может привести к умеренным негативным последствиям для ТС и пассажиров.
Low (L)	Данный риск означает, что событие угрозы может привести к незначительным отрицательным последствиям для ТС.

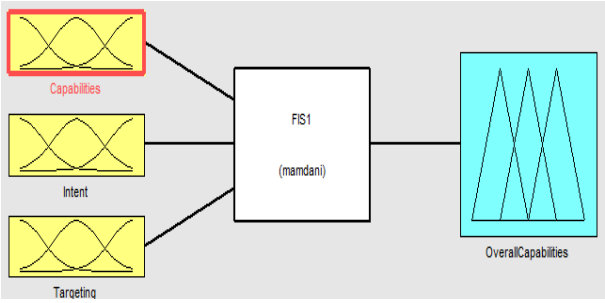

Рис. 9. Редактор FIS для Overall Capabilities (FIS1)

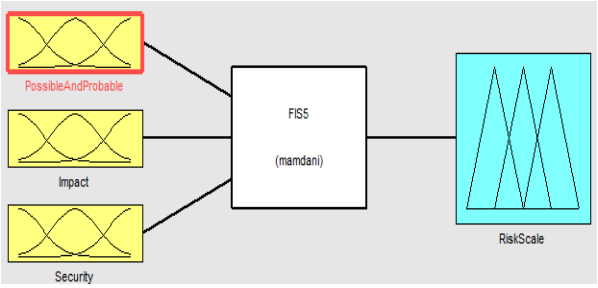

Рис. 10. Редактор FIS для Risk Scale (FIS5) - Inputs, Output и Setting параметры

Rule Viewer показывает графическое представление каждой из переменных через все правила, представление комбинаций правил. Например, как показано на рис. 11, для входов Possible and probable 73.2, Impact 69, и Security 70,6 - выходной уровень риска Risk Scale равен 62.6. Surface Viewer для FIS отображает 3-D граф, который показывает соотношение между входными переменными и выходной переменной. Surface Viewer показывает график возможных диапазонов входных переменных и возможный диапазон выхода.

На рис. 12 изображён 3D график для конечного результата Risk Scale в зависимости от Impact и Possible And Probable. Видно, что значение переменных свыше 50% существенно и резко повышает риск кибербезопасности ТС.

На рис. 13 изображён 3D график для конечного результата Risk Scale в зависимости от Possible And Probable и Security. Показано, что значение Security сравнивает влияние переменной Possible And Probable на общий риск кибербезопасности ТС.

На рис. 14 изображён 3D график для конечного результата Risk Scale в зависимости от Security и Impact. Показано, что значение Impact хоть и растёт, но существенно не влияет на общий риск ввиду высокого уровня Security.

Для увеличения точности нечёткую модель необходимо обучать, т.е. итерационно изменять её параметры с целью минимизации отклонения результатов логического вывода от экспериментальных данных. Обычно настраивают веса правил и функции принадлежности нечётких термов.

Задача обучения может рассматриваться и как задача аппроксимации функциональной зависимости, частично определённой имеющейся выборкой данных [13]. Способность к обобщению принципиально имеется у нечётких систем, благодаря свойству универсальной аппроксимации. А под универсальными аппроксимирующими способностями нечётких систем понимается возможность приближения произвольной функциональной зависимости с любой заданной точностью.

Заключение

Таким образом, внедрение ИТ в ТС приводит к появлению новых видов киберугроз, характеризующихся отсутствием статистики и пост инцидентных данных. Это затрудняет применение вероятностных методов оценивания рисков.

Предложенный метод учитывает различные модели источников угроз. Метод может быть использован для повышения точности и достоверности оценки различных сценариев киберугроз ТС и, следовательно, для снижения уязвимостей и рисков, связанных с угрозами. Метод рекомендован в качестве инструмента для оценки риска киберугроз, при условии, что входные параметры для FIS4 будут изменены в зависимости от требований системы.

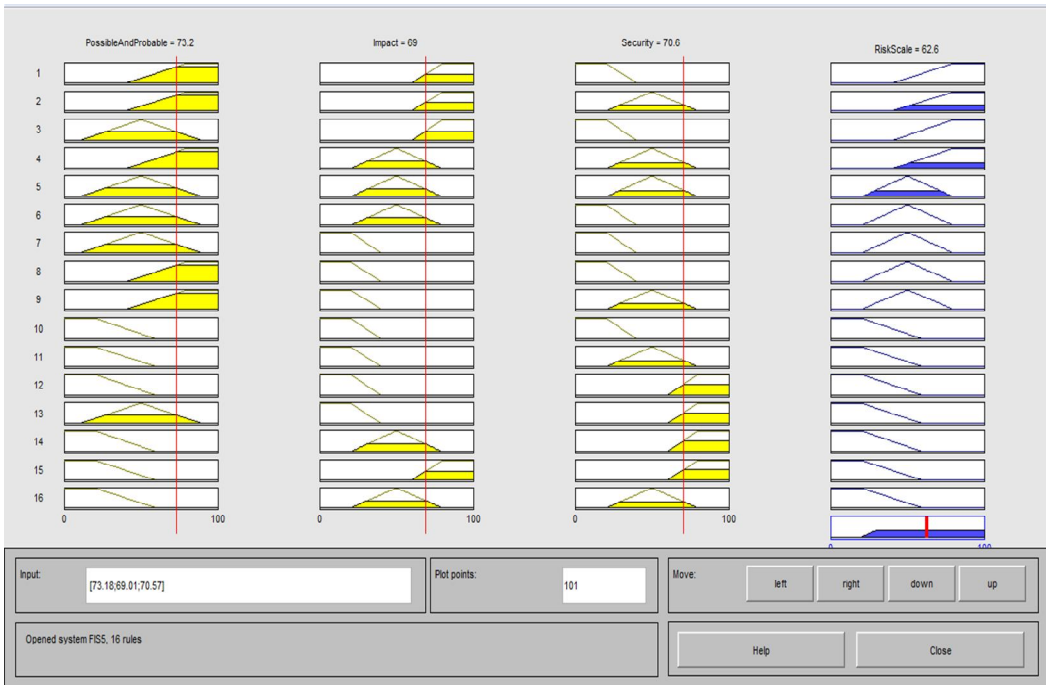

Рис. 11.Графическое представление переменных через правила

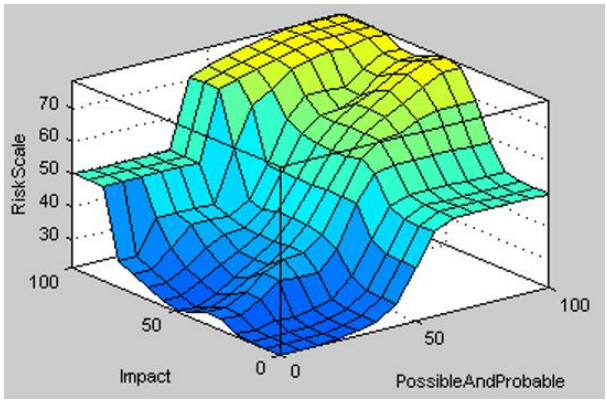

Рис. 12. 3D граф
для (Impact, Possible And Probable, and Risk Scale)

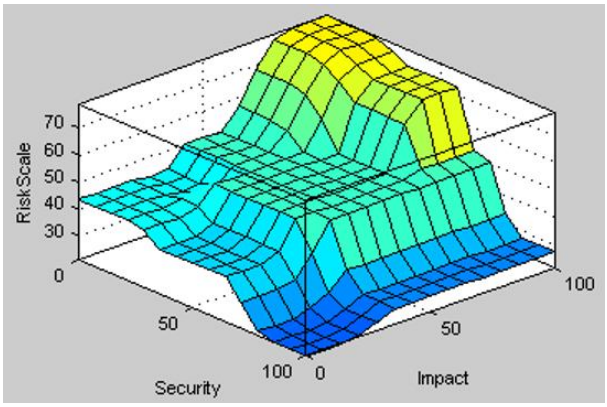

Рис. 14. 3D граф
для (Security, Impact and Risk Scale)

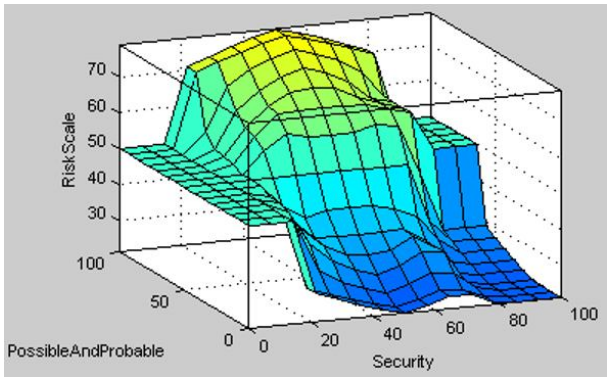

Рис. 13. 3D граф
для (Possible And Probable, Security and Risk Scale)

Литература

1. Колодочкин, М. Взлом без лома: легко ли вскрыть машину со смартфона? [Электронный ресурс] / М. Колодочкин. – Режим доступа: http://www.zr.ru/content/articles/783458-vzlom-bez-loma-legko-li-vskryt-mashinu-so-smartfona. –08.10.2016.

2. Miller, C. A Survey of Remote Automotive Attack Surfaces [Text] / C. Miller, C. Valasek // In Black-Hat USA. – 2014. – 94 p.

3. Ebert, C. Webinar: Automotive Cyber Security [Text] / Christoph Ebert // Vector Cyber Security Symposium. – Stuttgart : Vector Consulting Services GmbH, 2016. – 52 p.

4. Onishi, H. Paradigm Change of Vehicle Cyber Security [Text] / Hiro Onishi. – New-York, NATO CCD COE, 2012. – P. 381–391.

5. Onishi, H. Guidelines for Vehicle Cyber Security [Electronic resource] / Hiro Onishi // Alpine Electronics, Inc. – 2013. – Access mode: http://s3.amazonaws.com/sdieee/1737Hiro+SDIEEE+PACE+20140429_CyberSecurity_K_legal.pdf. – 08.10.2016.

6. Ruddle, A. Security risk analysis approach for on-board vehicle networks [Text] / Alastair Ruddle // The Fully Networked Car. – Geneva : Geneva International Motor Show, 2011. – 25 p.

7. Hank, P. Automotive Ethernet, a holistic approach for a next-generation in-vehicle networking standard [Electronic resource] / P. Hank, T. Suermann, S. Müller // NXP Semiconductors Germany. – 2012. – Access mode: http://itersnews.com/?p=10541. – 08.10.2016.

8. Automotive Security Best Practices [Text] / D. Clare, G. Cooper, H. Handschuh and etc. – Santa Clara : McAfee. Part of Intel Security, 2015. – 19 p.

9. Comprehensive Experimental Analyses of Automotive Attack Surfaces [Text] / S. Checkoway, K. Koscher, A. Czeskis and etc. – Washington : USENIX Security, 2011. – 16 p.

10. Van Roermund, T. Secure connected cars for a smarter world [Text] / Timo van Roermund // Security Architect, BU Automotive. – Eindhoven: NXP Semiconductors, 2015. – 30 p.

11. Sallam, H. Cyber Security Risk Assessment Using Multi Fuzzy Inference System [Text] / Hany Sallam. // International Journal of Engineering and Innovative Technology (IJEIT). – 2015. – № 8. – P.13–19.

12. Глушенко, С. Применение системы MATLAB для оценки рисков информационной безопасности организации [Текст] / Сергей Глушенко. // Бизнес-Информатика. – 2013. – № 4 (26). – С. 35–42.

13. Кукса, П. Методы обучения нечетких систем [Электронный ресурс] / Павел Кукса // BMSTU Press. – 2004. – Режим доступа: http://pkuksa.org/~pkuksa/Publications.htm. – 08.10.2016.

References

1. Kolodochkin, M. *Vzlom bez loma: legko li vskryt' mashinu so smartfona?* [Hacking without scrap: is it easy to open a car from a smartphone?]. Access mode: http://www.zr.ru/content/articles/783458-vzlom-bez-loma-legko-li-vskryt-mashinu-so-smartfona. (Accessed 08.10.2016).

2. Miller, C., Valasek, C. A Survey of Remote Automotive Attack Surfaces. *In BlackHat USA*, 2014. 94 p.

3. Ebert, C. Webinar: Automotive Cyber Security, *Vector Cyber Security Symposium*, Stuttgart, Vector Consulting Services GmbH, 2016. 52 p.

4. Onishi, H. *Paradigm Change of Vehicle Cyber Security*, New York, NATO CCD COE, 2012, pp. 381–391.

5. Onishi, H. *Guidelines for Vehicle Cyber Security*, Alpine Electronics, Inc., 2013, Access mode: http://s3.amazonaws.com/sdieee/1737-Hiro+SDIEEE+PACE+20140429_CyberSecurity_K_legal.pdf (Accessed 08.10.2016).

6. Ruddle, A. Security risk analysis approach for on-board vehicle networks. *The Fully Networked Car*, Geneva, Geneva International Motor Show Publ., 2011. 25 p.

7. Hank, P., Suermann, T., Müller, S. *Automotive Ethernet, a holistic approach for a next-generation in-vehicle networking standard*, NXP Semiconductors Germany, 2012, Access mode: http://itersnews.com/?p=10541 (Accessed 08.10.2016).

8. Clare, D., Cooper, G., Handschuh, H., and etc. *Automotive Security Best Practices*, Santa Clara, McAfee. Part of Intel Security Publ., 2015. 19 p.

9. Checkoway, S., Koscher, K., Czeskis, A., and etc. *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, Washington, USENIX Security Publ., 2011. 16 p.

10. Van Roermund, T. Secure connected cars for a smarter world. *Security Architect, BU Automotive*, Eindhoven, NXP Semiconductors, 2015. 30 p.

11. Sallam, H. Cyber Security Risk Assessment Using Multi Fuzzy Inference System. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2015, no. 8, pp. 13–19.

12. Glushenko, S. Primenenie sistemy MATLAB dlja ocenki riskov informacionnoj bezopasnosti organizacii [Application of MATLAB to evaluate the risks of the organization of information security]. *Biznes-Informatika*, 2013, no. 4 (26), pp. 35–42.

13. Kuksa, P. *Metody obuchenija nechetkih system* [Methods of teaching fuzzy systems], BMSTU Press, 2004. Access mode: http://pkuksa.org/~pkuksa/Publications.htm. (Accessed 08.10.2016).

Поступила в редакцию 14.01.2017, рассмотрена на редколлегии 16.02.2017

РОЗРОБКА МЕТОДУ ОЦІНКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТРАНСПОРТНИХ ЗАСОБІВ

Є. В. Брежнєв, В. В. Бородавка, Р. В. Салахов

Пропонується метод оцінювання ризиків кібербезпеки транспортних засобів (ТЗ), який засновано на використанні багаторівневого нечіткого виведення (Multi Fuzzy Inference System - MFIS), що дозволяє знизити вимоги до повноти статистичних даних, що характеризують окремі елементи моделі (загрози, ризики, активи, пр.), а також отримати нечіткі оцінки ризиків кібербезпеки ТЗ, прогнозувати наслідки взаємовпливу компонентів системи, а також сформувати безліч контрзаходів, спрямованих на підвищення кібербезпеки. Метод засновано на моделі загроз і ризиків, що враховує взаємовплив між ризиками активів і контрзаходами, а також між вузлами ТС і ризик-факторами.

Ключеві слова: кібербезпека, транспортний засіб, ризик-аналіз, загрози.

THE DEVELOPMENT METHOD OF ASSESSMENT OF CYBERSECURITY VEHICLES

E. V. Brezhnev, V. V. Borodavka, R. V. Salakhov

Proposed cyber security risk assessment method for vehicles, which is based on the use of multi-level fuzzy output (Multi Fuzzy Inference System - MFIS), which allows to reduce the requirements to the completeness of statistical data characterizing the individual elements of the model (threats, risks, assets, etc.) and get fuzzy evaluation cyber security risks of vehicles, to predict the effects of the mutual influence of the system components, as well as to form a plurality of countermeasures aimed at increasing cyber security. The method is based on the model of threats and risks, taking into account the interaction between risk assets and countermeasures, as well as between the vehicle nodes and risk factors.

Key words: cyber security, vehicle, risk analysis, threat.

Брежнев Евгений Витальевич – канд. техн. наук, доцент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: milestone@list.ru.

Бородавка Владислав Вячеславович – студент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: v.v.borodavka@hotmail.com.

Салахов Ренат Витальевич – студент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: renat.salakhow@gmail.com.

Brezhnev Evgenii Vitalyevich – Candidate of Technical Science, Assistant Professor of Dept. Of Computer Systems and Networks, National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine, email: milestone@list.ru.

Borodavka Vladyslav Vyacheslavovych – Student of Department of Computer Systems and Networks, National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine, e-mail: v.v.borodavka@hotmail.com.

Salakhov Renat Vitalievich – Student of Department of Computer Systems and Networks, National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine, e-mail: renat.salakhow@gmail.com.