Годишник Телекомуникации 2019, том 6, с. 63-73

Yearbook Telecommunications 2019, vol. 6, p. 63-73

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.7

АНАЛИЗ И ОЦЕНКА НА РИСКА ОТ РИСКОВИ ТЕХНИЧЕСКИ СИСТЕМИ ПРИ РАЗРАБОТВАНЕТО НА МЕТОДИКА ЗА ОБУЧЕНИЕТО НА СТУДЕНТИ ВЪЗ ОСНОВА НА МЕТОДА ДЪРВО НА СЪБИТИЯТА (EVENT TREE ANALYSIS)

Цветелина Симеонова

ANALYSIS AND RISK ASSESSMENT OF RISK TECHNICAL SYSTEMS TO DEVELOP OF METHODOLOGY FOR TEACHING STUDENTS USING THE METHOD EVENT TREE (EVENT TREE ANALYSIS)

Tsvetelina Simeonova

Резюме: Цел на настоящата работа е да се разработи методика за анализ, оценка и управление на риска чрез използване на метода дърво на събитията.
Показана е примерна последователност от действия за анализ на риска чрез метода дърво на събитията при определяне на вероятността за реализиране на опасно събитие, включваща примерна схема на дърво на събитията съгласно направени приемания и с възможност за изчисления и за определяне на риска при приета стойност на вредите.
Предложена е разработена методика за анализ на риска, базирана на дърво на събитията, приложима за обучение на студенти по анализ и управление на риска.
Ключови думи: дърво на събитията, риск, анализ на риска, оценка на риска, методика за обучение.

Abstract: The aim of this paper is to develop a methodology for risk analysis, assessment and management using the event tree method.
A sample sequence of risk analysis actions is shown with the use the event tree method in determining the probability of realizing a dangerous event including an exemplary event tree pattern according the example under consideration and with the possibility of calculations and for determining the risk at the accepted value of the damage
A methodology for risk analysis is proposed based on the event tree applicable to student training on risk analysis and management.
Keywords: Event Tree, risk, risk analysis, risk assessment, methodology for training**.**

1. ВЪВЕДЕНИЕ

При изследването на риска най-често вероятността за нежеланото събитие при функционирането на системата се описва с помощта на техники за моделиране на надеждността, най-често това са дървото на отказите и дървото на събитията (Event Tree).
При дърво на събитията (метод за качествен и количествен анализ - Event Tree Analysis, ETA) се представят връзките между проявяващите се събития, като обобщените принципи и основни насоки за прилагането на метода са представени в стандарта БДС EN 62502:2010 (IEC 62502:2010) [1]. Методът се състои в построяване на логическа дървовидна схема (структурен метод), показваща развитието на верига от събития, като се започне от началното събитие и се стигне до крайните събития (последствията) [2, 3, 4, 5].
Диаграмата на дървото на събитията моделира всички възможни пътища от началното събитие. Иницииращото събитие започва от лявата страна като хоризонтална линия, която се разклонява вертикално. В края на вертикалния клон се изчертават хоризонтални линии от горната и долната част, представляващи успеха или неуспеха на събитието, като се обозначават с етикет, който описва пътя. Този процес продължава до достигане на

крайното състояние (крайните състояния се класифицират в групи, които могат да бъдат успех/или тежест на последствията). Когато диаграмата на дървото на събитията е достигнала крайното състояние за всички пътеки, се записва уравнението на вероятност за изход.

Общата цел на анализа на дървото на събитията е да се определи вероятността от възможни отрицателни резултати, които могат да причинят вреда в резултат от избраното начално събитие. Необходимо е да се използва подробна информация за системата, за да се разберат междинните събития, сценариите на произшествия и инициирането на събития, за да се изгради диаграмата на дървото на събитията. Дървото на събитията започва с иницииращо събитие (събитие, което започва реакцията), където последствията от това събитие следват по двоичен (успех/неуспех) начин. Всяко събитие създава път, в който ще се случи серия от успехи или неуспехи, когато може да се изчисли общата вероятност за възникване на този път. Вероятностите за откази за междинни събития (междинните събития обикновено са алтернативни - успех/неуспех или да/не, но могат да бъдат разделени на повече от две, докато събитията са взаимно изключващи се, което означава, че не могат да се появят едновременно) могат да бъдат изчислени чрез анализ на дървото на отказите и вероятността за успех може да се изчисли от 1 = вероятност за успех (ps) + вероятност за неуспех (pf).

Например, в уравнението 1 = (ps) + (pf), ако знаем, че pf = 0.1 от анализ на дърво на отказите, тогава можем алгебрично да получим решение за ps, където ps = (1) - (pf), тогава ще имаме ps = (1) - (0.1) и ps = 0.9. Обща вероятност на пътя = (вероятност за събитие 1) X (вероятност за събитие 2) X (вероятност за събитие n ....).

Особеностите на метода се изразяват чрез **предимствата** (позволява оценката на множество, съвместно съществуващи грешки и откази; едновременно разглеждане на събития в случай на неуспех/успех; няма нужда да се предвиждат крайни събития; могат да бъдат идентифицирани и проследени пътища в система, които водят до повреда, за да може да се вземат контрамерки; може да се изпълнява с различни нива на детайлизация; позволява визуализация на причинно-следствената връзка; моделира сложни системи по разбираем начин; комбинирано могат да се описват хардуер, софтуер, среда и човешко взаимодействие и др.) и **недостатъците** (проследява във времето само едно начално събитие; иницииращото събитие и пътищата трябва да бъдат идентифицирани от анализатора, което изисква анализатор с практическо обучение и опит; трудно е да се намерят вероятности за успех или неуспех; може да пренебрегва малките системни разлики; частични успехи/неуспехи не се различават и др.).

Предложена е методика за анализ, оценка и управление на риска от рискови технически системи, чрез използване на метода дърво на събитията, приложима за обучение на студенти по анализ и управление на риска. Процесът на изграждане на методика за моделиране на техническа система, базирана на дърво на събитията, от която определяме риска на една система може да се представи като последователност от отделни задачи и дейности по реализирането им.

2. РАЗРАБОТВАНЕ НА МЕТОДИКА ЗА ОБУЧЕНИЕТО НА СТУДЕНТИ ЗА АНАЛИЗ И ОЦЕНКА НА РИСКА ВЪЗ ОСНОВА НА МЕТОДА ДЪРВО НА СЪБИТИЯТА

Цел на разработката, свързана с обучението на студентите по анализ, оценка и управление на риска, е да се изчисли и анализира рискът за възникване на опасно събитие чрез

Годишник Телекомуникации 2019, том 6, с. 63-73

Yearbook Telecommunications 2019, vol. 6, p. 63-73

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.7

дървото на събитията. Въз основа на задание за студентите трябва да се определи риска чрез метода дърво на събитията, като се изчисли вероятността за поява на опасни събития. Основната цел на всяка система, била тя софтуерна или хардуерна, е да бъде ефективна. Ефективността на системата е една от основните характеристики на всяка система, заедно със сигурността и отказоустойчивостта й.

2.1. Пример за транспортиране на входяща поща.

Ще бъде използван пример за моделиране на типична приложна система за получаване на поща с помощта на ETA. Вероятността от отказ при претоварване и при мейл сървърите се увеличава, което може да компрометира отказоустойчивостта на разглежданата система или по скоро вредата, която може да нанесе на друга система (мейл сървъра).

Повечето оценки на риска започват със следните стъпки, които представляват предварителен анализ (Preliminary Analysis):

- Идентифициране на опасността (Identify the hazard).
- Идентифициране на съответните системи, компоненти и елементи (Identify relevant systems, components, and individuals).
- Ограничаване на анализа (Bound the analysis). Важно е да се знае от самото начало кои събития се разглеждат, кои системи трябва да се анализират и нивото на детайлност.

Пример: Транспортиране на входяща поща (Inbound Mail Transport).

Изискването е задължително входящата поща да не бъде безвъзвратно загубена (организацията е primer.org).

Електронната поща (e-mail) е мрежова услуга, чрез която всеки потребител, свързан към глобална компютърна мрежа, може да обменя съобщения с всички потребители на мрежата [6].

Основните понятия, свързани с електронната поща, са следните:

- Отдалечен подател (Remote sender);
- Отдалечен хост на потребителя (Remote user host);
- Пощенски клиент (Mail Client, Mail User Agent) - програмна система, която изпраща/получава електронни писма към/от пощенския сървър;
- Отдалечен MUA (потребителски агент за поща, например клиентски софтуер) - (Remote MUA - Mail User Agent, e.g., Client Software);
- Пощенски сървър (Mail Server) - представлява програмна система, реализираща основните функции на електронната поща. За всеки домейн от глобалната мрежа е необходим поне един такъв сървър;
- Пощенски транспортен агент (Mail Transport Agent - MTA) - програма, която приема и изпраща електронните писма. При приемане на дадено писмо тя анализира адреса на получателя. Ако получателят има пощенска кутия на сървъра, писмото се записва в нея. В противен случай то се записва в опашката за изходящи писма;
- Отдалечен MTA (агент за транспортиране на поща, например софтуер за пощенски сървър) - Remote MTA (mail transport agent, e.g., mail server software);
- Пощенска кутия (Mail Box) - специализиран файл, съхраняван в определена директория на сървъра. Всеки такъв файл носи името на съответния потребител и е предназначен да съхранява пристигащата за този потребител електронна поща;
- Отдалечена мрежа (Remote network);

- Системата за имена на домейни - DNS (The Domain Name System);
- Интернет (Internet);
- Прехвърлящ хост (Relay Host) - програма, която управлява маршрутизирането и изпращането на електронните писма в рамките на глобалната мрежа. Тя обработва в последователен ред писмата, съхранявани в опашката за изходящи писма на сървъра. За изпращане на маршрутизираното писмо се използва пощенски транспортен агент;
- Шлюз (gateway) - програмна система, която управлява обмена на електронна поща между различни видове комуникационни мрежи;
- Интернет доставчик (primer.org's ISP - Internet Service Provider);
- Локална мрежа (Local network);
- Местни MTA (Local MTAs);
- Местен потребителски хост (Local user host);
- Местен MUA (Local MUA);
- Местен получател (Local recipient).

Основни функции на протоколите и програмите, реализиращи електронна поща [7].
За обмен на данни чрез електронна поща се използват множество протоколи, например:
• SMTP (Simple Mail Transfer Protocol) - осигурява обмен на писмата между програмите, предназначени за изпращане и получаване на електронна поща.
• POP (Post Office Protocol) - предназначен за прехвърляне съдържанието на пощенската кутия на потребителя от пощенския сървър към персоналния компютър на потребителя.
• IMAP (Internet Message Access Protocol) - осигурява връзка между пощенския сървър и потребителските персонални компютри чрез динамичен достъп до пощенските кутии на сървъра. Разликата с протокола POP е, че прочетените писма остават на съхранение в пощенския сървър, а не се прехвърлят в локалната система. Това позволява на потребителя да има достъп до пощенската си кутия от различни клиентски компютри. Освен това в пощенската кутия на сървъра се поддържа йерархична система от директории, част от които могат да бъдат обявени и като публични. Възможно е търсене на писмо по някакъв признак и преглеждане само на заглавните части на писмата без да бъдат изтегляни изцяло на клиентския компютър.
• UUCP (Unix to Unix CoPy) - опростен протокол за обмен на електронни съобщения между компютърни системи, работещи с UNIX операционна система.
• X. 400 - протокол е приет от ITU (International Telecommunicaton Union) и ISO (International Standardization Organization) и стандартизиран като ISO 10021. В днешно време е по-малко разпространен, за сметка на SMTP.

Разширявайки обхвата, може достатъчно обосновано да се разгледа и следното,:

- Пренос и разпределителна мрежа (Power transmission and distribution network);
- Местна околна среда (температура, влажност и др.) - On-site environment (temperature, humidity, etc.);
- Външна околна среда (вероятност от пожар, наводнение, ледена буря, земетресение и др.) - Off-site environment (likelihood of fire, flood, ice storm, earthquake, etc.);
- Човешка дейност (неспособна или злонамерена) - Human activity (inept or malicious);
- Извънземна активност (слънчеви изригвания, магнитни бури и др.) - Extraterrestrial activity (solar flares, magnetic storms, etc.);

Годишник Телекомуникации 2019, том 6, с. 63-73

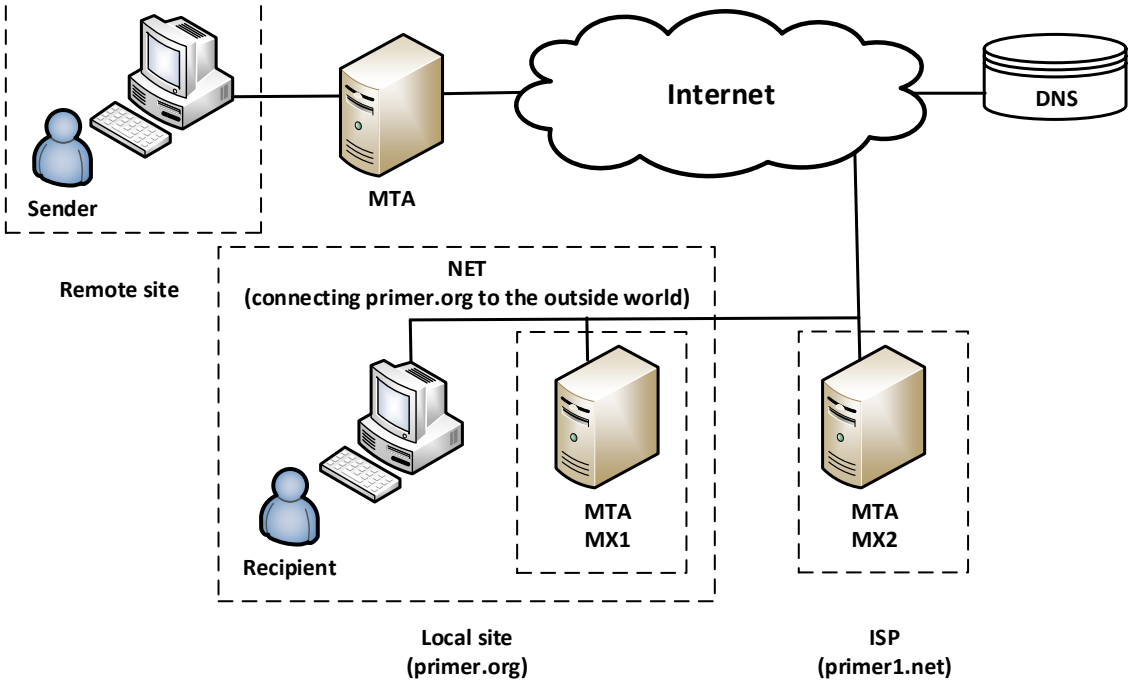
Yearbook Telecommunications 2019, vol. 6, p. 63-73

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.7

- Политически климат (граждански вълнения, война) - Political climate (civil unrest, war).

За да се опрости анализа, ще се моделират само части от локалния сайт на primer.org, техния ISP (пощенски сървъри, DNS) и интернет (връзката от primer.org към primer1.net, нейния ISP) - фиг. 1.
Пощенските сървъри са изброени в DNS (db.primer.org) в низходящ приоритетен ред, както следва:
1D B MX 10 shaft.mx.primer.org.
1D IN MX 20 dolomite.mx.primer.org.
1D IN MX 30 mta00.primer1.net.
Това показва два вътрешни пощенски сървъра (първичен с приоритет 10 и вторичен с приоритет 20) и външен резервен пощенски сървър (mta00.); mta00 е третичен с приоритет 30.



Фиг. 1. Пример: транспортиране на поща.

Анализ по дървото на събитията
Дървото на събитията е диаграма на всички събития, които могат да се появят в една система, т.е. е графична форма на таблица на истинността. Анализът на дървото на събитията е индуктивен подход, тъй като следва подхода "Какво става, ако се случи събитие X ?"
Започва се с инициращо събитие (от лявата страна на диаграмата), като се преминава през поредица от точки на разклонение, които представляват вероятната поява и съответно големината (стойността) на определени събития. Всеки от клоновете има свързана вероятност, като крайните състояния представляват комбинацията от събития, водещи до конкретна последица. Резултатът е дървовидна структура, която ясно показва събитията, водещи до конкретни последствия, и позволява лесно да бъде получено количествено измерване на риска.

Начин на структуриране на дървото на събитията

Най-напред се определят последствията представляващи интерес, като се разглеждат системи или функции, свързани с тази последица.

В примера дефинираме последствията като "загуба на входяща поща" и избираме системите да бъдат:

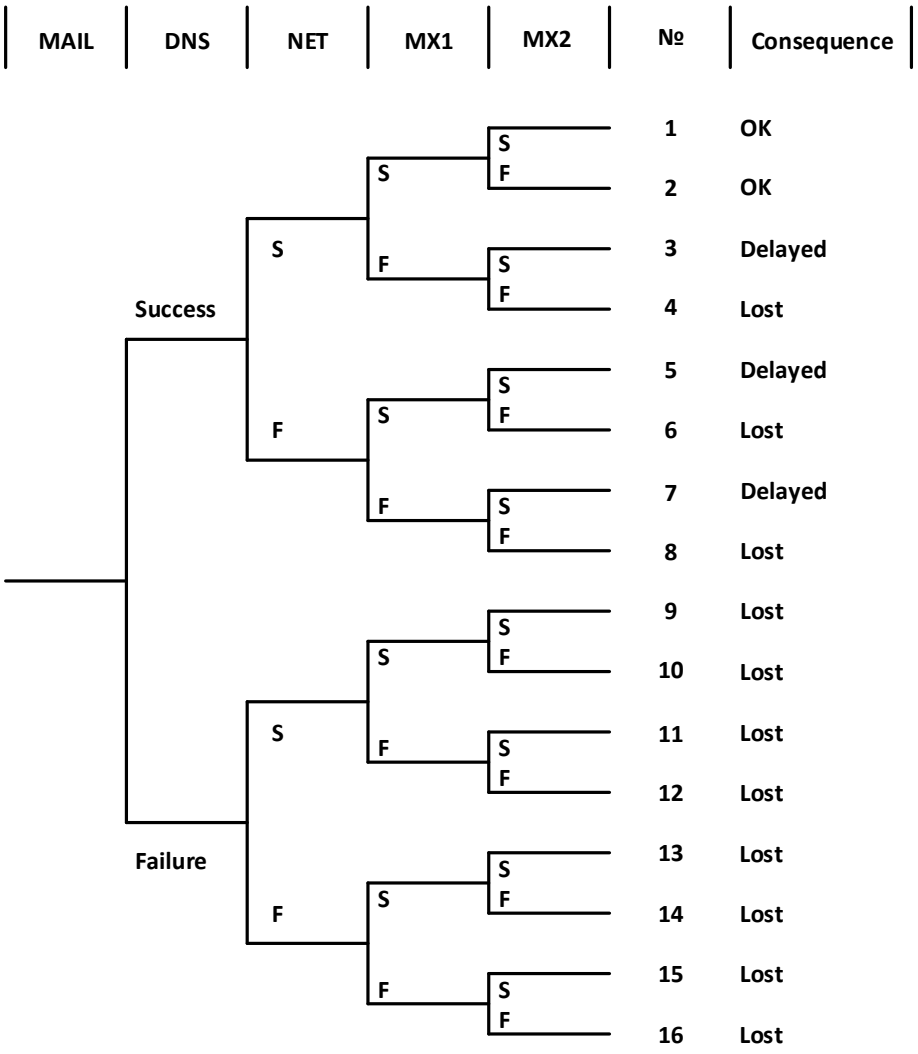
• DNS: може ли системата за имена на домейни да разреши подходящата дестинация за входящата поща (по-специално MX записите, съдържащи пощенските сървъри в домейна)?

• NET: може ли отдалечените хостове да достигат до локални пощенски сървъри? Могат ли местните потребители да достигнат до локални пощенски сървъри?

• MX1: местните (първични) пощенски сървъри приемат ли поща?

• MX2: дали отдалечените (вторични) пощенски сървъри приемат поща?

Нашето инициращо събитие е "поща, изпратена на primer.org." Това е събитие с висока вероятност за всички, освен за най-малките домейни. Комбинирайки тези събития, ние изграждаме основно дърво на събития (фиг. 2), което съдържа всички възможни разклонения.



Фиг. 2. Основно дърво на събитията.

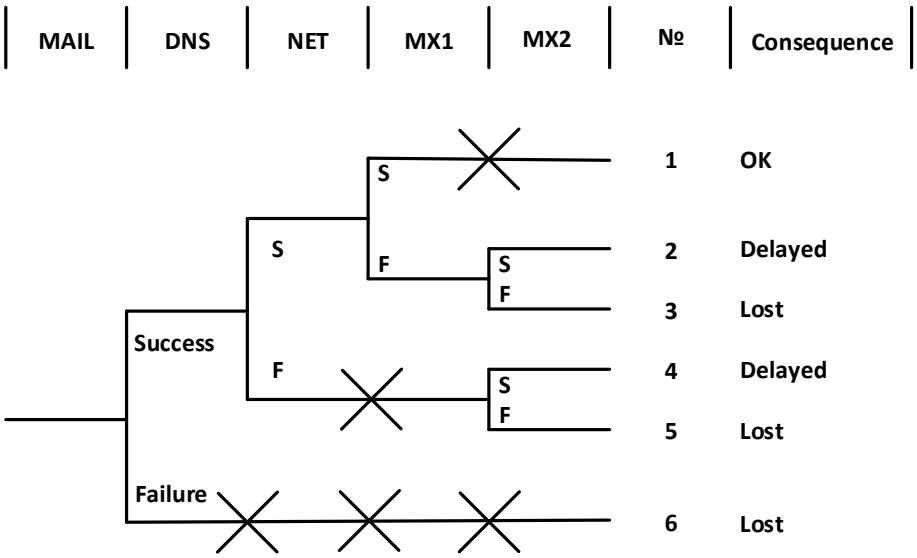
Годишник Телекомуникации 2019, том 6, с. 63-73

Yearbook Telecommunications 2019, vol. 6, p. 63-73

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.7

Някои състояния нямат смисъл и могат да бъдат елиминирани, което води до редуцирано дърво на събития - фиг. 3.
Например, ако DNS не може да актуализира адреса на получаващия MTA (MX1 или MX2), състоянията на локалната мрежа и първичните и вторичните пощенски сървъри са без значение.
Ако са налични DNS, NET и MX1, състоянието на MX2 е без значение, тъй като пощата ще бъде доставена до MX1 и няма да има търсене за MX2.
И накрая, ако локалната мрежа (NET) не е достъпна, състоянието на MX1 е без значение; след като опитът за свързване към MX1 се провали, изпращането на MTA ще опита MX2.
Намаленото дърво на събитията ясно обяснява доста сложна система.



Фиг. 3. Редуцирано дърво на събитията.

Следващата задача е да се извлекат числени стойности за всяка от тези вероятности за отказ. Може да се оценят вероятностите или да използват статистически данни, но в по-сложни модели тези стойности се получават чрез анализ на дървото на отказите.

2.1. Пример за построяване и анализ на дърво на събитията в среда на Ексел чрез разработване на шаблон.

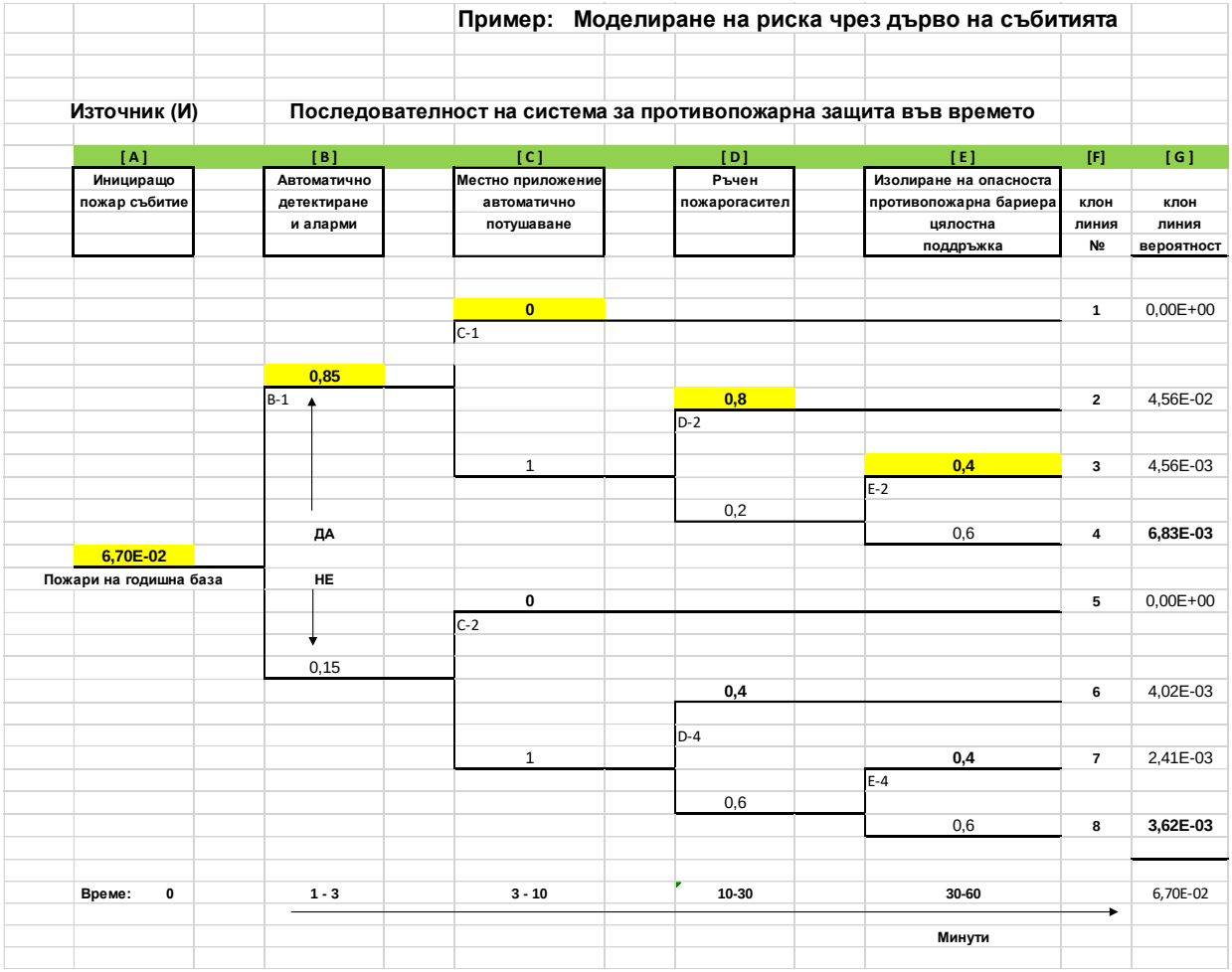
Като вариант на изпълнение може да се използва среда на Excel (шаблон) за да се построи дърво на събитията и да се попълнят приетите събития и вероятности - фиг. 4 [8].
В случай, че рискът е неприемлив (на база на качествена и/или количествена оценка), трябва да се въведат допълнителни мерки (допълнително събитие), чрез което да се намали вероятността за реализиране на голяма вреда и рискът да се преизчисли.

Методиката включва следните приемания:
1. Вероятностите (параметрите) на всички елементи за разглеждания пример от фиг. 2 и фиг. 3 се задават и нанасят по подобие на примера от фиг. 4.
2. Вредата (тежест на очакваната вреда) в измерителни единици (например левове загуба, дни на неработоспособност, левове за възстановяване) е с условни стойности за разглежданите случаи, които се задават.

На фиг. 4 показаният пример предвижда недопустим риск и трябва да се въведе предвижданото допълнително събитие (съгласно фиг. 4) със зададена вероятност и да се преизчисли риска.

2.3. Последователност за извършване на анализ чрез дърво на събитията:

Анализът чрез дървото на събитията се използва при оценка на риска за определяне на вероятността, която се използва за определяне на риска, като се умножи по вредата от събитието. Анализът на дървото на събитията е метод, който онагледява пътя създаващ най-голямата вероятност за нежелано (крайно) събитие за определена система.



Фиг. 4. Примерна структура на дърво на събитията в среда на Ексел.

Като пример да се построи дърво на събитията от фиг. 2 в среда на Excel като се разработи шаблон при следните стъпки (първите 5 стъпки са включени във фиг. 2 - фиг. 4):

1. Определяне на системата: какво трябва да бъде включено и къде да са границите.
2. Идентификация на сценариите на произшествията: оценка на системата, за да се открият рискове (или сценарии на произшествия в рамките на проектирането на системата).
3. Определяне на началните събития: анализ на риска, за да се дефинират началните събития.
4. Идентификация на междинните събития: Идентификация на мерките за противодействие, свързани със специфичния сценарий.
5. Създаване на диаграма на дървото на събитията.

Годишник Телекомуникации 2019, том 6, с. 63-73

Yearbook Telecommunications 2019, vol. 6, p. 63-73

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.7

- Въвеждат се в горната част събитията описателно или с номер и легенда: Източник (инициращо събитие), Последователност, Цели (риск).
- Въвежда се в долната част "ос на времето (времева линия)".
- Започвайки от инициращото събитие, съобразно времевата линия, се проследява описаната последователност от събития (в нашия случай събитията са дуални) как се развива във времето.
- Присвояват се стойности на вероятността (да възникне или не; поради дуалността сумата е =1) на всяко от събитията.

6. Изчисляване на вероятност за крайно събитие: Присвояване на уравнение (на крайните събития - КС), описващо всеки клон (линия) чрез последователно умножаване на вероятностите на събитията, които са разположени по съответния клон.
7. Изчисляване на риска за крайното събитие: Изчисляване на общата вероятност на пътя на събитието и определяне на риска от него.
В този контекст се налага рискът да се анализира с цел да се определи вероятността да се сбъдне и евентуалните последици. Като възможност е необходимо системите да може да се модифицират, откъдето следва, че е необходимо рисковете да може да бъдат приоритизирани. Също така е необходимо да се вземе предвид, че конкретният момент на настъпване на риска има значение върху последиците, които ще окаже. Използвайки тези два показателя се въвежда т.нар. матрица за оценка на степента на риска [9], съобразно стандарта БДС ISO 31000 [10].
Рискът се дефинира в контекста на оценката на ефективността на технико-икономическите системи като произведение на вероятността за претърпяване на вреда и тежестта на вредата, отнесено към определена времева единица [11], т.е. изчисляването на риска се извършва чрез степента на риска, която се определя като математическо очакване на вредата от нежеланото събитие, а именно:
$R = P.W$,
където: P – вероятност за поява на събитието (например отказ на техническа система), W – вреда, нежелани последствия.

8. Оценяване на риска (R) от крайното събитие (КС): Оценяване на риска на всеки път и определяне на неговата приемливост.
9. При получен неприемлив риск се извършва управление на риска, т.е. въвеждат се коригиращи действия (допълнително събитие и др., които да променят риска) и се извършва преизчисляване за да се определи риска.

За случая, когато полученият риск е неприемлив, за всеки от двата случая се попълва табл. 1, където:

1: изчислен риск без допълнителни мерки;
2: изчислен риск след допълнителни мерки.

Табл. 1. Изчисляване на риска от дърво на събитията.

№	R от КС 1	R от КС 2	R от КС 3	…	R от КС N
1					
2					

10. Преглед на документирания процес на диаграмите на дървото на събитията (ETA) и актуализиране в случай на поява на нова информация.

ЗАКЛЮЧЕНИЕ

Описан е метода дърво на събитията, като са посочени неговите предимства и недостатъци с цел последващото му прилагане за анализ, оценка и управление на риска.
Показани са примери (в случай на получаване на входяща електронна поща, както и вариант с използване на шаблон и отчитане на особеностите на програмата Ексел) за анализ на риска с използване на дърво на събитията, съгласно предложена разработена методика, приложим за обучение на студенти по анализ и управление на риска, включващ примерни структури, както и възможни изчисления по тях.
Оценява се рискът и се отбелязват събитията, които оказват най-съществено влияние върху неговата стойност, като на тази база са възможни варианти за намаляване на риска, в случай, че първоначално получената му стойност е неприемлива.

ЛИТЕРАТУРА

1. БДС EN 62502:2010 Методи за анализ на надеждността. Анализ чрез дървото на събитията (IEC 62502:2010). BDS EN 62502:2010 Metodi za analiz na nadezhdnostta. Analiz chrez darvoto na sabitiyata (IEC 62502:2010)
2. Clemens, P.L.; Rodney J. Simmons (March 1998). "System Safety and Risk Management". NIOSH Instructional Module, A guide for Engineering Educators. Cincinnati, OH: National Institute for Occupational Safety and Health: IX-3–IX-7.
3. Hong, Eun-Soo; In-Mo Lee; Hee-Soon Shin; Seok-Woo Nam; Jung-Sik Kong (2009). "Quantitative risk evaluation based on event tree analysis technique: Application to the design of shield TBM". Tunneling and Underground Space Technology. 24 (3): 269–277.
4. EVENT TREE ANALYSIS [Accessed on: 15 Nov. 2018]. Viewed in: https://www.sciencedirect.com/topics/engineering/event-tree
5. P. L. Clemens EVENT TREE ANALYSIS June 1990 [Accessed on: 16 Nov. 2018]. Viewed in: http://kspt.icc.spbstu.ru/media/files/2011/course/depend/01_EventTree.pdf
6. Robert Apthorpe - Excite@Home, Inc. A Probabilistic Approach to Estimating Computer System Reliability [Accessed on: 25 Nov. 2018]. Viewed in: https://www.usenix.org/legacy/events/lisa2001/tech/apthorpe/apthorpe_html/
7. Ларс Кландер. Защита от хакери. София, СофтПрес. ISBN 954-685-055-1, 1999. (българско издание). Lars Klander, Hacker Proof: The Ultimate Guide to Network Security, Jamsa Press, 1999, (английско издание)
8. Шаблон на Excel за построяване на дърво на събитията и анализ на риска. [Accessed on: 12 Dec. 2018]. Viewed in: http://www.google.bg/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiCu4iilJ3gAhVBUlAKHeZHBEcQFjAAegQICBAC&url=http%3A%2F%2Fwww.cfaa.ca%2FFiles%2Fflash%2FEDUC%2FTECHNICAL%2520SPREADSHEETS%2FFire%2520Risk%2520Event%2520Tree%2520Model%2520(RiskTOOLS%2520ETA%252001%2520Sept%252027%25202003%2520%2520F2).xls&usg=AOvVaw1j6cHy1C3ZQiSYsyO2gJsK. SHablon na Excel za postroyavane na darvo na sabitiyata i analiz na riska.
9. Управление на риска. Уикипедия. [Accessed on: 11 Nov. 2018]. Viewed in: [https://bg.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BD%D0%B0_%D1%80%D0%B8%D1%81%D0%BA%D0%B0]. Upravlenie na riska. Uikipediya.
10. ISO 31000:2018, Risk management – Guidelines; БДС ISO 31000:2018 - Управление на риска. Принципи и указания.
11. Юридическият термин „риск“ в националната сигурност на Република България. [Accessed on: 11 Nov. 2018]. Viewed in: http://conf.uni-ruse.bg/bg/docs/cp15/7/7-24.pdf. YUridicheskiyat termin „risk“ v natsionalnata sigurnost na Republika Balgariya

Информация за автора:
Ас. д-р инж. Цветелина Богданова Симеонова, София 1574, ул. Гео Милев 158, ВТУ „Т. Каблешков”, Тел.: 02 9709296, e-mail: ts.b.simeonova@abv.bg

Годишник Телекомуникации 2019, том 6, с. 63-73

Yearbook Telecommunications 2019, vol. 6, p. 63-73

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.7

Contacts:
Assist. professor Tsvetelina Simeonova PhD, T.Kableshkov University of Transport, 158 Geo Milev St., Sofia, office phone: +359 2 9709296, e-mail: ts.b.simeonova@abv.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 05.01.2019.
Дата на приемане за публикуване (Date of adoption for publication): 05.03.2019.