ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – ВАРНА

инж. Петко Генчев Генчев

Заглавие:

Подход за мониторинг на риска в системи за информационна сигурност

А В Т О Р Е Ф Е Р А Т

на дисертация за получаване на образователна и научна степен „доктор“

Варна, 2022г.

Дисертационният труд съдържа 146 страници, включително 19 фигури и 4 таблици, оформени в 4 глави, общи изводи и списък на използваната литература от 113 заглавия, от които 14 на кирилица и 99 на латиница.

Защитата на дисертационния труд ще се състои на ..... г. от ..... ч. в ..... на открито заседание на жури сформирано със заповед на Ректора № ...../..... г.

Материалите по защитата (дисертацията, рецензиите и становищата) са на разположение на интересуващите се в Докторантския център, стая 318 НУК.

I. ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на проблема

В съвременния свят все повече организации разчитат на информационни технологии, за да им помогнат да постигнат своите бизнес цели, като по-бърз отговор на услугата или по-добро качество. Ето защо сигурността на информацията (СИ) е от първостепенно значение за организациите. Необходим е систематичен подход за управление на риска по отношение на сигурността на информацията, който да помогне да се определят изискванията за сигурност на информацията и да се създаде ефективна система за управление.

Тези факти определят актуалността на изследвания в областта на повишаване на ефективността на системите за управление на риска за сигурността на информацията и преодоляване на проблемите, възникващи при изграждане и експлоатация на такива системи.

2. Цели и задачи на изследването

Целта на дисертационния труд е изследване на възможностите за преодоляване на проблемите при реализация на системи за управление на риска за сигурността на информацията (УРСИ). Като резултат от проведени изследвания и анализи, д**а се предложи подход и да се формулира задание за изграждане на информационна система с цел преодоляване на основни проблеми при оценка и мониторинг на риска в системи за информационна сигурност.**

За постигане на поставената цел са изведени следните задачи за изследване:

- Във връзка с постоянно променящата се среда и условия на работа на организацията е необходимо да се направи анализ на вероятностните характеристики на измененията на рисковите фактори. Да се предложи начин за определяне на периодичността на проверките и актуализацията на състоянието на рисковите фактори;
- Да се предложат алгоритми за ефективна организация на следенето на измененията на рисковите фактори и подпомагане на мониторинга на риска за СИ;
- Да се предложи форма на йерархичен контрол на реализацията и ефективността на мониторинга на рисковите фактори;
- На базата на оптимизиране на мониторинга и контрола на риска за СИ и вземайки предвид формулираните по-горе организационни препоръки, да се предложи общ подход за преодоляване на някои основни затруднения и подпомагане на въвеждане и експлоатация на УРСИ;

- При използване на предложения подход да се дефинират функционални изисквания към изграждане на програмна система за реализация на УРСИ.

3. Обект и предмет на изследване

Обект на изследването е изграждането на системи за управление на риска и мониторинга на риска за информационната сигурност.

Предмет на изследването е събиране и обработване на необходимата информация за ефективен мониторинг и управление на риска за сигурността на информацията.

4. Място на изследване

Изследванията са проведени в лабораториите на катедра КНТ на Технически Университет – Варна, България.

5. Методи на изследване

За решаването на поставените задачи, са използвани метода на математическото моделиране на вероятностни процеси, методи и подходи за анализ на риска за сигурността на информацията, методи за оценяване на уязвимостите, методи за оценяване на технически уязвимост, метод на анализ и съпоставка на резултатите от прилагането на различни подходи за решаване на даден проблем.

6. Научна и практическа новост на изследването

В резултат на проведените теоретични и експериментални изследвания в съответствие с целта и задачите на дисертационния труд могат да бъдат дефинирани следните основни приноси:

Приноси с научно-приложен характер:

- Предложен е подход за ефикасно управление на риска за сигурността на информацията, чрез въвеждане, обработване на данни за рисковите фактори и прилагане на динамична система за тяхното регулярно наблюдение;
- Изведени са математически изрази за определяне на периодичността на проверките на рисковите фактори и за определяне на текуща стойност на вероятността за инцидент между две проверки на рисковите фактори;

- Предложен е алгоритъм за оценка на периодичността на проверките за риска на информационен актив;
- Предложен е алгоритъм за йерархична организация на контрола на извършваните проверки за риска на информационен актив.

Приноси с приложен характер:

Предложения подход е илюстриран в примерна реализация на информационна система за обслужване на управление на риска за сигурността на информацията в организация с внедрена СУСИ. Работата на информационната система доказва повишаване на ефективността на управлението на риска.

7. Практическа приложимост

Предложеният подход може да се приложи при разработване на цялостна информационна система за внедряване и поддържане на система за управление на информационната сигурност. Предложените алгоритми и математически изрази ще осигурят ефективен и лесен начин за мониторинг на рисковите фактори и ще предоставят възможности за натрупване на необходимата статистическа информация.

8. Апробация на изследването

Основните теоретични и приложни резултати от дисертационния труд са докладвани в 6 публикации, на следните международни научни конференции:

- International Conference Applied Computer Technologies (ACT) 2019, 19 – 21 September, 2019, in Varna, Bulgaria;
- 2020 International Conference on Biomedical Innovations and Applications (BIA), 24-27 Sept, 2020, in Varna, Bulgaria;
- 56th International Scientific Conference on Information, Communication and Energy Systems and Ttechnologies (ICEST) june 16-18 2021, Sozopol, Bulgaria;
- International Scientific Conference CONFSEC 2021.

Конференциите „Biomedical Innovations and Applications (BIA)" и „56th International Scientific Conference on Information, Communication and Energy Systems and Ttechnologies (ICEST)" са индексирани в международната научна база от данни "SCOPUS".

9. Публикации

Основни постижения и резултати от дисертационния труд са публикувани в 6 научни статии, като 2 от тях са самостоятелни. Научните статии са представени и публикувани в национални, международни и международни реферирани и индексирани издания.

10. Структура и обем на дисертационния труд

Дисертационният труд е в обем от 146 страници, като включва увод, 4 глави за решаване на формулираните основни задачи, списък на основните приноси, списък на публикациите по дисертацията и използвана литература. Цитирани са общо 113 литературни източници, като 99 са на латиница (английски език) и 14 на кирилица. Работата включва общо 19 фигури и 4 таблици. Номерата на фигурите, графиките и таблиците в автореферата съответстват на тези в дисертационния труд.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА 1. Системи за управление на риска и сигурността на информацията

В тази глава е описан преглед на изискванията на стандартите на ISO в сферата на информационната сигурност. Извършен е обзор на основните трудности, които са констатирани при реализация на дейностите по оценка и мониторинг на риска за сигурността на информацията. На базата на направените проучвания е извършен анализ и са набелязани стъпки за преодоляване на проблемите.

1.1 Изисквания на стандартите за изграждане на системи за управление на сигурността на информацията(СУСИ) и системи за управлението на риска за сигурността на информацията(УРСИ)

1.1.1. Системи за управление на сигурността на информацията – същност, стандарти, изисквания за управлението на риска

Стандартът ISO/IEC 27001 дефинира изискванията, на които трябва да отговаря система за управление на сигурността на информацията и се използва за сертифициране на организацията по отношение на информационната сигурност.

В основата на изграждането на СУСИ, стандартът ISO/IEC 27001 поставя управлението на риска за сигурността на информацията.

1.1.2. Управление на риска за сигурността на информацията – същност, стандарти

Помощен стандарт в групата стандарти ISO/IEC 27XXX, свързан с управление на риска за сигурността на информацията е стандартът ISO/IEC 27005. Той не се използва за сертифициране на организации, а е предназначен да подпомогне организирането на управлението на риска за сигурността на информацията. Този стандарт разглежда изискванията за управление на риска, които са описани в стандарти ISO 31000 и EN 31010, в светлината на сигурността на информацията.

Управлението на риска за сигурността на информацията трябва да бъде непрекъснат процес. При това периодично трябва да се установява външния и вътрешния контекст на организацията, да се оценяват рисковете и да се въздейства върху тях, чрез прилагане на план за третиране на риска.

1.1.5. Изводи от прегледът на стандартите за СУСИ и УРСИ

Може да се направи изводът, че оценката и мониторинга на риска за сигурността на информацията е важен елемент в изграждането на СУСИ и определя вида и степента на прилагане на мерки за увеличаване на сигурността на информацията. От изискванията и правилата за управление на риска за СИ е видно, че материята е сложна и разнородна и в много от етапите се налага ползване на експертна помощ.

1.2. Литературен обзор на проблемите при системи за УРСИ

Целта на извършения обзор е да се открият и определят основни проблеми, които затрудняват процесите на управление на риска за сигурността на информацията. За да могат да се формулират ясни мерки за подобряване на ефективността на процесите по оценка и мониторинг на риска, дефинираните проблеми са категоризирани по въздействието им върху етапите и видовете дейности по оценка на риска за информационните активи.

1.2.1. Проблеми, свързани със събиране и обработване на данни:

- Липсва информация за конкретни реализации на УРСИ;
- Липсват или са трудно достъпни изчерпателни, обществено достъпни и достоверни данни за възникнали събития, въздействия и техните вероятности;

- Статистическите данни за инциденти и заплахи за информационната сигурност не са толкова достъпни, колкото други данни;
- Поради невъзможността да проследят всички изменения на рисковите фактори, много организации изпускат важни данни, свързани с риска;
- Решенията често се вземат без необходимата информация и често се основават на предположения на ръководството;
- Съществува проблем с тестване и потвърждаване на данни за резултатите от управлението на риска.

1.2.2. Проблеми с методите за оценка на риска:

- Ползват се много методи за оценка на риска и изборът на подходящ метод е труден;
- Липсва съгласуван метод за измерване на рисковете за информационната сигурност;
- Липсва утвърждаване и проверка за ефективност на съществуващите методи;

1.2.3. Проблеми свързани със субективен фактор:

- Наблюдава се безотговорно отношение и поведение на служителите към сигурността на информацията;
- Подборът на методи за оценка на риска се основава на експертно мнение и субективна преценка;
- Хората като цяло извършват лоша оценка на риска;
- Нежеланието за докладване на инциденти води до недостатъчно отчитане и липса на знания за ефективността на системата;
- Субективен мениджмънт.

1.2.4. Проблеми с ефективността:

- Важно е да се прави анализ на ефективността на оценката на риска в организациите;
- Невъзможността да се докаже, че УРСИ работи може да е по-лошо от това да няма внедрена система;
- Липсата на достатъчно бюджет за сигурност често е пречка за постигане на желаното ниво на защита на сигурността на информацията;
- Не е достатъчно да се приложат мерките за сигурност, те трябва да се управляват правилно, за да бъдат ефективни;

- Несигурността влияе на ефективността.

1.2.5. Пропуснати или недооценени източници на риск:

- Сигурността трябва да се разглежда като процес, а не като продукт;
- Подценява се защитата на надеждността и сигурността на бизнес процесите в организацията;
- Не се взема предвид съвместното възникване на рискове;
- Пропускат се нематериални активи;
- Пренебрегване на рисковете, свързани с човешките действия, за сметка на технологичните аспекти.

1.2.7. Организационни проблеми:

- Кампанийност - няма точни правила за периодичността на оценката на риска на информацията в организациите;
- Тъй като сложността се увеличава успоредно с разнообразието на драстично нарастващите информационни системи, адаптирането на конкретен модел става все по-сложно.

1.3. Анализ на проблемите и предложения за набелязване на мерки за намаляване на влиянието на проблемите върху ефективността на системата

След направения литературен обзор на констатираните проблемите при изграждане и експлоатация на системи за УРСИ, беше извършен анализ и бяха изведени организационни предложения за намаляване на влиянието на някои от проблемите.

1.4. Изводи от направените обзор и анализи на проблемите

За да се увеличи ефективността на СУСИ, е необходимо да се изгради система от организационни мерки, която да позволи преодоляване на голяма част от проблемите и да доведе до по-ефективно управление на процесите по управление на риска за СИ. Необходимо да се въведат мерки, които да дисциплинират персонала и да въведат по-строги отговорности на всички нива на управление.

Може да се направи изводът, че значителна част от проблемите са свързани с нуждата от въвеждане на единен програмен продукт за събиране и обработване на необходимата информация и адаптацията на системата към бързо променящата се среда.

На базата на направените проучвания, и посочените изводи може да бъде формулирана следната цел на научните изследвания в дисертационния труд:

Цел на дисертационния труд

Да се предложи подход и да се формулира задание за изграждане на информационна система с цел преодоляване на основни проблеми при оценка и мониторинг на риска в системи за информационна сигурност.

Задачи на изследването

- Във връзка с постоянно променящата се среда и условия на работа на организацията е необходимо да се направи анализ на вероятностните характеристики на измененията на рисковите фактори. Да се предложи начин за определяне на периодичността на проверките и актуализацията на състоянието на рисковите фактори;
- Да се предложат алгоритми за ефективна организация на следенето на измененията на рисковите фактори и подпомагане на мониторинга на риска за СИ;
- Да се предложи форма на йерархичен контрол на реализацията и ефективността на мониторинга на рисковите фактори;
- На базата на оптимизиране на мониторинга и контрола на риска за СИ и вземайки предвид формулираните по-горе организационни препоръки, да се предложи общ подход за преодоляване на някои основни затруднения и подпомагане на въвеждане и експлоатация на УРСИ;
- При използване на предложения подход да се дефинират функционални изисквания към изграждане на програмна система за реализация на УРСИ.

ГЛАВА 2 Модел за определяне на периодичността на проверките на рисковите фактори

Една от най-важните мерки, които могат да се предприемат за намаляване на влиянията на проблемите при изграждане и експлоатация на система за УРСИ е осигуряване на ефективен мониторинг на рисковите фактори. За тази цел е необходимо да се определят елементите, подлежащи на мониторинг и периодичността на извършваните проверки. В тази глава, е направен анализ на вероятностните характеристики на измененията на рисковите фактори. На базата на този анализа, е изведен математически израз, за изчисляване на времето до следваща

необходима проверка, за да се отчетат промените и новите стойности на риска за СИ.

2.1. Изследване на измененията на рисковите фактори

2.1.1. Обосновка на необходимостта от изследване на измененията на рисковите фактори и определяне на периода за тяхната проверка

При извършване на оценка на риска за определяне на нивото на риска се използват вероятността за всеки сценарии и въздействието на инцидентите. Това представлява моментна снимка на риска за актива, защото оценката е направена при определени условия за актива. Във времето условията за актива се променят и следователно е възможно да се променят и вероятността за инцидент и въздействието от инцидента. Промяната на условията за реализация на сценарии за инцидент и за определяне на нивото на риска е случайна величина, която трябва да бъде проследявана.

Правилното и навременно провеждане на инспекциите на рисковите фактори гарантира точно и актуално определяне на нивата на риска за всички активи и адекватно прилагане на политиките за управление на СИ.

Поради тези причини има необходимост от анализ на измененията на рисковите фактори и определяне на параметрите, които влияят на това.

2.1.2. Дефиниране на рисковите фактори

Стандартът ISO/IEC 27005 дефинира някои от рисковите фактори като стойност на активите, въздействия, заплахи, уязвимости, вероятност за поява. Определено е, че те трябва да бъдат наблюдавани и преглеждани, за да се идентифицират всякакви промени в контекста на организацията на ранен етап и да има актуален поглед върху цялостната картина на риска.

2.1.4. Подходи за определяне на периодичността на проверките

В стандартите за управление на риска има дадени изисквания за извънредни проверки на рисковите фактори и повторна оценка на риска за даден актив при значителни промени в предмета на дейност на организацията, подобрения, които са направени в организацията, проблеми, произтичащи от задачата, инциденти или пропуски.

При различните активи промяната на условията на работа има различно въздействие върху нивото на риска. По тези причини **в стандартите няма ясни и категорични правила за определяне на периодичността на проверките** на условията на експлоатация и променените рискови фактори.

При изграждане на системи за управление на информационната сигурност в повечето случаи **периодите за проверка се препоръчват от експерти** възоснова на статистически данни от застрахователни компании и държавни статистически организации.

При направения литературен обзор не бяха намерени данни за анализ и методи за определяне на периоди за проверка на рисковите фактори за различни активи.

2.1.6. Постановка на задачата

При въвеждане на система за управление на сигурността на информацията на една организация е установен контекста за управление на риска, методиката, която ще се използва за оценка на риска, приемливите и допустимите нива на риска, въведените контроли за управление на нивата на риска. Идентифицирани са всички рискове и са определени собствениците на рисковете, оценен и преценен е риска, определени и утвърдени са методите за третиране на риска.

На базата на тези налични данни, трябва да се определи кога да се проведе следващата инспекция на рисковите фактори и евентуално преизчисляване на нивото на риска за дадения актив. За целта трябва да се определи кои са динамично променящите се фактори при изчисляване на риска и да се определи минималното време между две проверки, което осигурява минимално изменение на риска, поради изменение на средата.

Промяната на условията за реализация на сценарии за инцидент е случайна величина, която се променя във времето и тази промяна следва да доведе до промяна на нивото на риска. Освен това този елемент от нивото на риска се изменя най-динамично. От тази гледна точка е важно да се изследва скоростта на изменение и нивата на промените в нивото на вероятността за реализация на инцидент.

2.1.7. Предлаган математически модел за изследване на промените на вероятността за инцидент

Възможността за реализация на сценарии за инцидент представлява вероятност в определен начален момент I_0 и зависи от промяната на условията във времето. Промяната на условията ще доведе до променена стойност на вероятността за инцидент в края на периода. В одобрената от организацията методиката за оценка на риска за СИ е определена приемлива стойност на нивото на вероятността. Тази стойност може да се използва за гранична величина I_{limit}, до която може да нараства нивото на вероятността при изменения на условията. Разликата между допустимото и началното ниво на вероятността $I_{limit} - I_0$, ще определи размера на изменение на

вероятността в зависимост от промените на условията през времето между две проверки.

Ще разгледаме следната постановка. За срок примерно от една година се приема, че за даден актив има дефинирани n сценария за инцидент. Приема се също, че динамиката на поява на нови сценарии е по-малка от динамиката на промените в описаните сценарии и няма да влияе на целите на провеждания анализ.

В рамките на една година изменения на вероятностните характеристики може да възникнат по нито един сценарии, по един или по няколко от сценариите. В зависимост от случая този брой би бил един или друг и следователно трябва да се разглежда като случайна величина K с някакво разпределение на вероятностите. Съществуват различни хипотези за вероятностното разпределение на подобна случайна величина. Една от тях може да се синтезира по следния начин. Да означим с q вероятността за настъпване на изменение на условията за отделния сценарии и да предположим, че тя е една и съща за всички сценарии. Предполага се независимост на настъпване на изменения на условията за всички сценарий, т.е. при това положение броят K на измененията през годината представлява случайна величина с биномно разпределение:

Известно е, че биномното разпределение с малка величина на вероятността q е доста близко до разпределение на Поасон с параметър $\lambda=nq$. Така, че друга възможност за разпределението на броя K на измененията през годината е това на Поасон с математическо очакване λ и дисперсия също λ.

Използването на разпределението на Поасон позволява и улеснява преодоляването на някои технически затруднения и затова при по-нататъшните разглеждания ще го ползваме като пример за разпределение на случайната величина K.

Вследствие на настъпилите промени в условията за реализация на сценариите, се формира добавка към вероятността за инцидент при даден сценарий. Големината на добавката, а оттук и на риска за актива, варират от случай към случай и е логично да се разглеждат като непрекъсната случайна величина X. Често се възприема хипотезата, че тази случайна величина има експоненциално разпределение с интензитет ξ . При това положение среднят размер на добавките към вероятността за инцидент при отделните сценарии е $\frac{1}{\xi}$, а дисперсията е $\frac{1}{\xi^2}$.

Сборът на добавките (измененията на вероятностите) през годината представлява случайна величина и актива може да се окаже застрашен, ако тази величина надхвърли определено критично равнище. Следователно изучаването на разпределението на годишния размер на добавките (измененията на вероятностите)

би могло да допринесе и за изясняване на политиката за управление на риска за актива.

2.1.8. Анализ на измененията на вероятността за инцидент

Нека да разгледаме ситуация при която проверки на рисковите фактори се правят през период ***t***. Ако няма изменения на рисковите фактори за актив, няма да има и формирана добавка към вероятността за инциденти с актива. Появата на изменения на рисковите фактори ще доведе до формиране на добавка (величина с която ще се промени вероятността) в края на периода.

Да предположим, че броят на добавките за период от ***0*** до ***t*** като средна величина се акумулира с постоянна скорост ***E(K(t)) = λt***. В такъв случай математическото очакване на годишния размер на добавките би било ***λμ***, като за общата стойност на вероятността за инцидент като математическо очакване ще важи:

$$E(I_t) = I_0 + \lambda\mu t \qquad (2.12)$$

Където:

E(I$_t$) –сумарно ниво на вероятността за инцидент с актива, което е натрупано за време ***t***

I$_0$ е първоначалното ниво на вероятността за инцидент с актива;

λ е брой изменения за единица време – скорост на изменение;

λt е брой изменения за време ***t*** – средна скорост на натрупване;

μ е математическо очакване на експоненциално разпределение – има смисъл на големината на добавките към вероятността за инцидент. Това показва с колко средно се изменя вероятността за инцидент

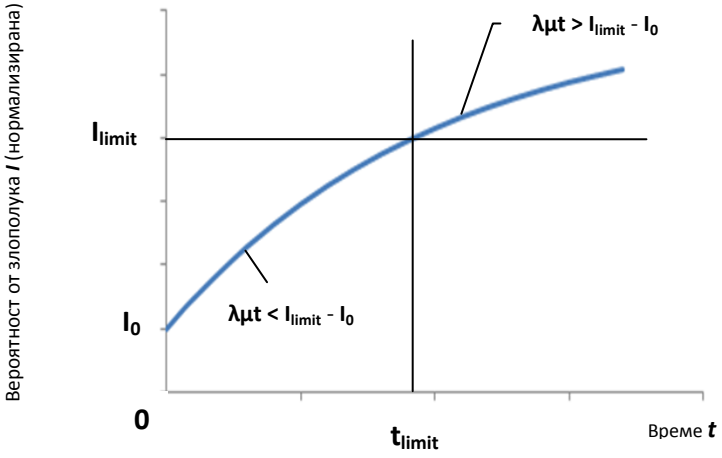
Тогава средният прираст на добавките (вероятността за инцидент) за време ***t*** е ***λμt.*** Можем да разгледаме следните случаи:

При ***λμt < 0*** имаме ситуация при която с времето вероятността, за случване на инцидент със сценарий, намалява. Това е положителна тенденция за намаляване на риска за актива. Тази тенденция би трябвало да окаже малко влияние на процеса на следене на рисковите фактори, защото не води до намаляване на периода на проверки.

Ако ***λμt > 0*** имаме случай на нарастване на вероятността за инциденти. Това е ситуацията, която трябва да окаже основно влияние при определяне на периода за проверки. Необходимо е да се разгледат следните случаи:

- При ***I$_0$ ≥ I$_{limit}$*** имаме изчислена вероятност за инцидент, която е равна или

по-голяма от приемливото ниво на вероятност за този актив. Това допускане е малко вероятно, защото в такава ситуация се предприемат мерки за въздействие върху риска (въвеждане на нови методи за контрол), които имат за цел намаляване на риска под допустимото ниво.



Фиг. 2.3. Изменение на вероятността за инцидент

- При $(I_0 + \lambda\mu t) \geq I_{limit}$ има много висок темп на нарастване на вероятността за инцидент, който за време t довежда до увеличаване на вероятността за инцидент над определената приемлива стойност на нивото на вероятността. В този случай периода за проверка на рисковите фактори трябва да бъде намален до стойности, при които не се достига приемливото ниво на вероятността. На фиг. 2.3. тази ситуация е илюстрирана със стойности над стойността на I_{limit}.
- При $(I_0 + \lambda\mu t) < I_{limit}$ имаме ситуация на нормален темп на нарастване на нивото на вероятността за инцидент вследствие на изменения на рисковите фактори. В този случай може да се приеме, че е определен приемлив период на проверки. В илюстрацията на фиг. 2.3., това е периода в границите от 0 до t_{limit}.

2.2. Определяне на периодичността на проверките на рисковите фактори и оценката на риска

Изведеният по-горе математически израз (2.12) за сумарното ниво на вероятността за инцидент с актива, натрупано за време t може да се разтълкува, като обща стойност на вероятността за инцидент в края на периода между две проверки

на рисковите фактори. За горна граница на нарастването на вероятността за инцидент I_{limit}, можем да използваме одобрената от организацията приемлива стойност на нивото на вероятността. Тогава:

$$E(I_t) = I_0 + \lambda\mu t = I_{limit} \quad (2.13)$$

В такъв случай параметъра t представлява време до следваща проверка, до която ще достигнем ниво на вероятността I_{limit}. Това време ще означим с t_c.

Ако приемем, че от статистиката е известно средното време за реализация на заплаха за даден актив и означим това време с t_{stat}, то можем да включим този параметър в по-нататъшните изчисления.

След преобразувания получаваме:

$$t_c = t_{stat}\sqrt{\frac{I_{limit} - I_0}{n}} \quad (2.22)$$

Това всъщност е време за което вследствие на изменения на рисковите фактори, вероятността за инцидент, ще достигне граничното, приемливо ниво I_{limit}.

Трябва да се вземе под внимание, че в изчисляването на периода между проверките с изведения математически израз (2.22) участват вероятностни параметри, които са изчислени или потвърдени при предна проверка. Тези вероятностни параметри са пресметнати, като се отчитат характерните особености на работа на конкретната организация. **Това означава, че изчисления период е във функция както на статистически параметър за актива, така и от контекста и условията на експлоатация на актива в конкретната организация.**

2.3. Определяне на текуща стойност на вероятността за инцидент между две проверки на рисковите фактори

За да се изчисли промяната на риска във всеки момент от времето след последната проверка е необходимо да се преработим израза (2.22), като функция на времето от последната проверка. При това ако вместо времето до проверката t_c, се зададе текущо време t_{curent}, а стойността на вероятността за инцидент в момента t_{curent}, обозначим с I_{curent}, то ще се получи:

$$I_{curent} = n\frac{t_{curent}^2}{t_{stat}^2} + I_0 \quad (2.25)$$

В това уравнение t_{curent} има смисъл на времето от последната проверка на рисковите фактори, където е определена вероятността I_0, до текущия момент, в който ще се определи I_{curent}.

След като се знае вероятността за инцидент и въздействието, което оказва инцидента, можем да се определи и текущата стойност на риска за актива. Беше определено, че въздействието е дефинирано при последното пресмятане на риска и може да се счита, че в изследвания период от време то не се е променило.

Математическият израз (2.25) може да се използва за автоматизиране на процесите по обслужване на мониторинга на риска за даден актив. Така на базата на последните проверени рискови фактори за актива и ползвайки данни от статистиката за интензивността заплахите, може да се изчисли текуща стойност на риска за актива.

2.4. Изводи

След направения анализ на измененията на рисковите фактори, е изведен математически израз за изчисляване на периода до следваща проверка на рисковите фактори. Този период гарантира измененията на риска за периода да не надвишават дефинираните, допустими нива на риска за организацията. Предимство на изведеният израз (2.22) е, че той използва параметри, които са изчислени за организацията и отразяват характерните особености на организацията. От друга страна в уравнението се използват статистически данни, които са осреднени и носят информация за вероятностните процеси в други организации и случаи.

Използването на израз (2.22) позволява по-точно определяне на времето до следващата проверка. Това ще доведе до по-висока ефективност на мониторинга на риска за даден актив:

- **Ще се избегне излишно честа проверка на риска за актива, което е свързано с разход на време и пари;**
- **Ще се избегне проверка през много голям период от време, което предполага опасност от изтърване на промени в рисковите фактори, които могат да доведат до недопустимо увеличение на риска и до предизвикване на инцидент със СИ.**

Изведената зависимост (2.25) позволява да се пресмята моментната стойност на вероятността за инцидент, а от там и пресмятане на текуща стойност на риска за информационната сигурност на даден актив. Тези пресмятания могат да се извършват само след извършена оценка на риска, но имат съществено значение при мониторинга на риска.

В дисертацията е обоснован извода, че направените анализи и изведените формули могат да се използват и за нуждите на мониторинг на риска и в други системи за управление на риска.

ГЛАВА 3 Формулиране на подход за подпомагане на управлението на риска за сигурността на информацията

Целта на тази глава е да се формулира подход за преодоляване на някои проблеми, свързани със събиране и обработка на информация, необходима за оценка и мониторинг на риска при системи за управление на риска за сигурността на информацията.

3.1. Обосновка и дефиниране на задачите и елементите на подхода

3.1.2. Предложения за решаване на някои проблеми при оценка и управление на риска за сигурността на информацията

Основният извод от направените проучвания и анализ на проблемите за изграждане на система за УРСИ е, че за подпомагане на разработването и поддържането на системата е необходимо да се изгради програмен продукт (информационна система) за събиране и обработка на данни, свързани с риска от информационна сигурност на организация.

Преструктурирането на проблемите в светлината на изисквания за възможностите , които трябва да има програмната реализация, води до откроването на няколко основни задачи, които продукта трябва да може да реши. Например той трябва да е в състояние да предостави инструменти за ефективно събиране, систематизиране и обработване на големи обеми информация, подпомагане на регулярното следене на изменения на рисковите фактори, подпомагане на отчетността, подходящо оформяне и поднасяне на информация към управленските структури на организацията и др..

3.2. Динамична система за регулярно наблюдение на рисковите фактори и нивото на риска

Във връзка с променящите се условия на експлоатация на информационните активи, възниква идеята да се изгради система за наблюдение на рисковите фактори, която да позволи **оценка** на влиянието на изменените рискови фактори, върху нивото на риска за актива. Можем да наречем такава система **динамична**, защото ще позволи да се формира постоянно променяща се стойност на

нивото на риска в зависимост от условията на експлоатация и качеството на следене на тези изменения.

3.2.3. Предложение за оценка и контрол на мониторинга на информационните активи

Най-важна роля в проследяване на промените на рисковите фактори играе собственика на актива. Следователно неговото отношение към коректността на проверките на рисковите фактори, пряко влияе на нивото на риска за актива и това трябва да се отчита.

Предлага се да се изгради и развие алгоритъм за проследяване и оценка на изпълнение на задълженията на собственик на информационен актив. За тази цел е важно да се определи как ще повлияе нивото на риска от поведението на собственика на актива върху общото ниво на риска за актива.

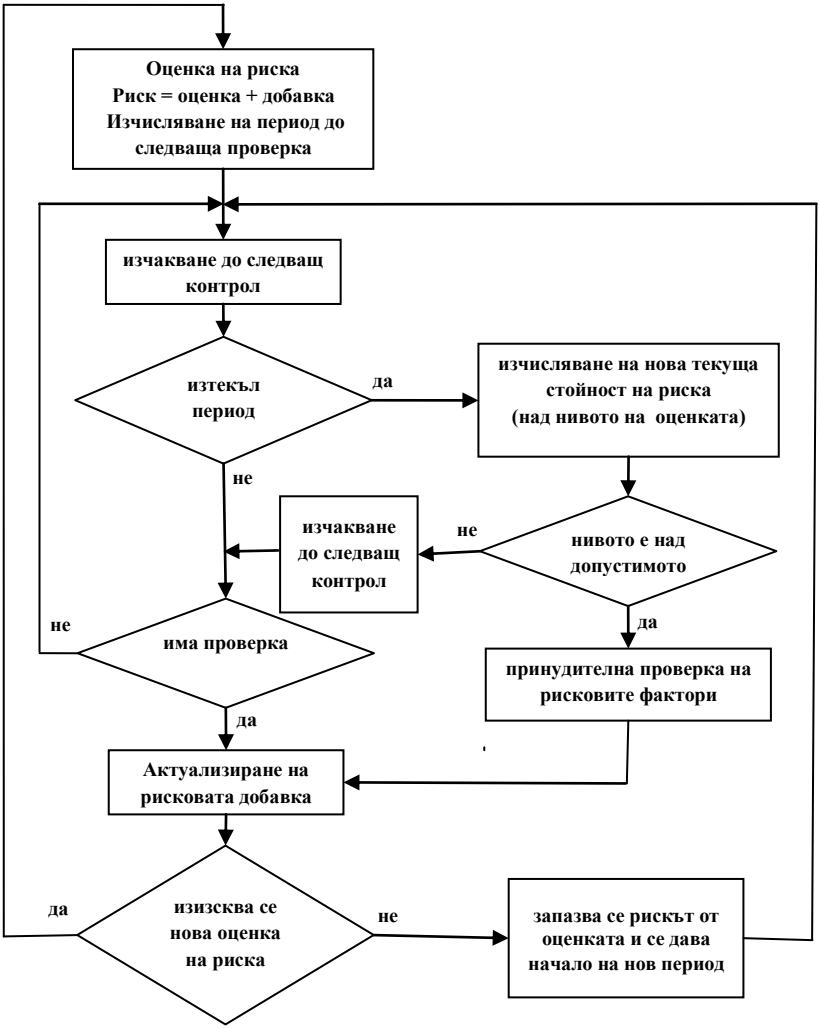
3.2.3.1 Схема за провеждането на регулярните периодични оценки на риска

Може да се определи, че процеса на мониторинг представлява цикличен процес на провеждане оценки на нивото на риска, като времето между оценките зависи от промените на условията в които работи актива.

Предлага се да се въведат изменения и допълнения в етапите на цикличната последователност за мониторинга на риска за даден актив. Тези промени целят ясно дефиниране на периодите на проверка, отчитане на нарушенията на периодите и отчитане на повишеното ниво на риска за актива при просрочен период на проверките. Процесите в предложения периодичен процес на мониторинг на риска за информационен актив могат да се опишат по следния начин:

- Периодите за провеждане на проверки и евентуално нова оценка на риска за актива се изчисляват с използване на математическия израз (2.22);
- За времето на изчисления период за ниво на риска за актива се счита нивото от последно проведената оценка;
- Собственикът на актива има грижа да спази изчисления срок и да проведе анализ на рисковите фактори преди изтичането на срока;
- Проследяване за спазване на изчислените периоди между проверките се извършва автоматично от системата за мониторинг;
- При просрочване на изчисления период имаме ситуация, която се характеризира с достигнато и надхвърлено приемливо ниво на риска;
- До провеждане на нова, извънредна оценка на риска за ниво на риска се

счита изчислената към текущия момент стойност на риска за актива, при използване на математически израз (2.25). Тази стойност постоянно расте във времето до провеждане нова оценка на риска;



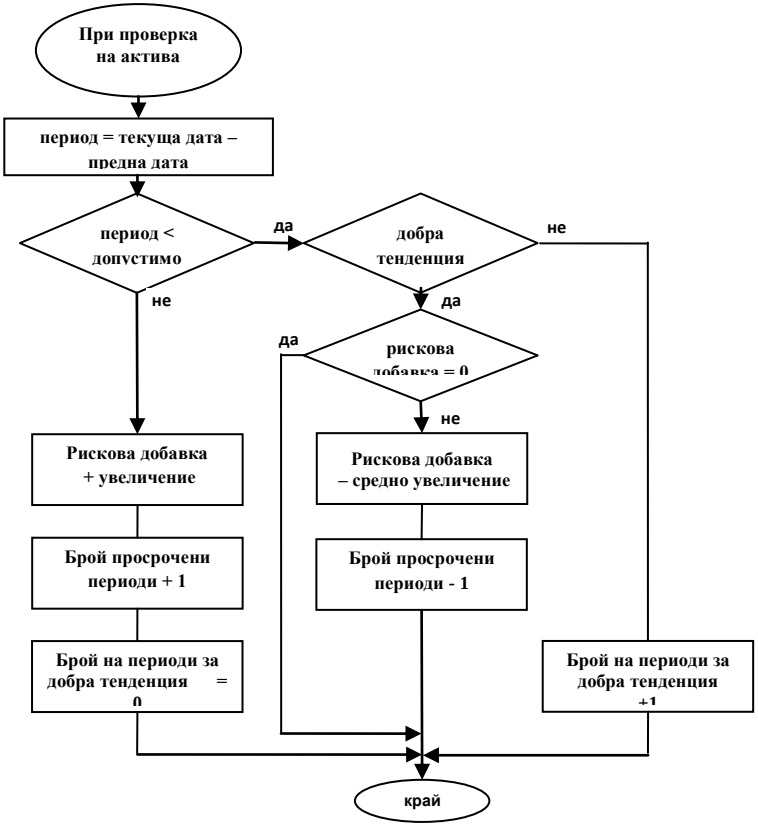
Фиг. 3.1. Схема на предложената циклична последователност на мониторинга и формиране на риск за актива

- След провеждане на нова оценка на риска, за ниво на риска за актива се

приема нивото от оценката. При провеждане на оценката се извършва и ново изчисляване на периода до следваща проверка на риска.

Този подход позволява осигуряване на актуална информация за риска за активите, както и определяне на собствениците на информационни активи, които не са спазили зададения срок. На фиг. 3.1. е показана схема на предложената циклична последователност на мониторинга и формиране на риск за актива. В тази схема при изчисляване на риска е използвана наказателната рискова добавка свързана с коректността на извършване на проверка на рисковите фактори от собственика на актива, която ще бъде дефинирана и описана по-долу.

3.2.3.4 Алгоритъм за формиране на наказателна рискова добавка



Фиг. 3.2. Изменение на стойността на рисковата добавка от поведението на собственика на актива

Предлага се формиране на допълнителна рискова стойност за актива, която се нарича рискова добавка. Тази наказателна рискова добавка може да се нарече риск от поведението на собственика и се добавя към утвърдена стойност на риска след проведена оценка на риска.

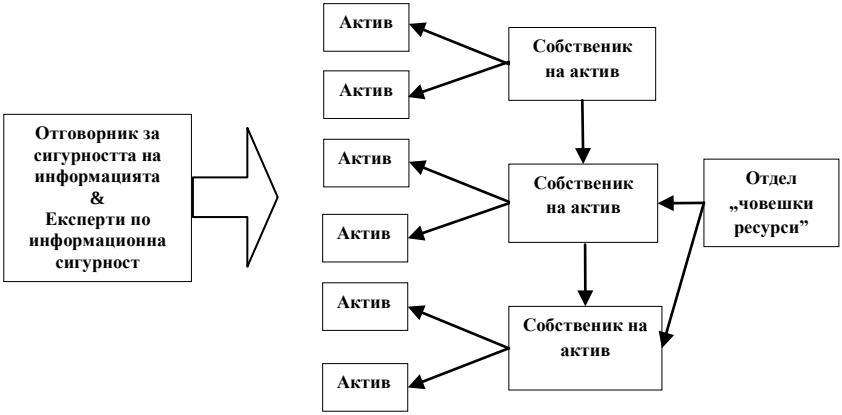
Нарастването на рисковата добавка става при всяко просрочване на проверките, а намаляването се извършва бавно при установяване на положителна тенденция за редовно провеждане на проверките на рисковите фактори. Изменението на рисковата добавка е показано в блоковата схема от фиг. 3.2.

Предложения алгоритъм може да се прилага след всяка, извършена от собственика, проверка на рисковите фактори за актива, при автоматична процедура за проверка на активността на собствениците на активи, или при извършване на контрол от ръководството на организацията.

3.3. Йерархия на нивата на достъп, въвеждане и контрол

Основният обект при оценката на риска е активът, който представлява лице, машина, документ, инфраструктура, програма, данни или каквото и да е, което има информационна стойност за организацията или има отношение към информация, ценна за организацията. За всеки актив трябва да е определен собственик на актива, като така се осигурява отговорност и отчетност за актива.

От гледна точка на дефиницията на актив, собственикът на актив е актив на един от лидерите на по-високото ниво на йерархията в организацията. Правилното разпределение на ролите и активите, за които отговарят собствениците на активите, всъщност е пряка връзка между структурата на организацията и УРСИ.



Фиг. 3.3. Йерархия на контрола на активите

Предложение в тази посока може да бъде формулирано като предоставяне на възможност за съхраняване на информация и проследяване на проведените проверки от по-високи нива в административната йерархия на организацията.

Правилното разпределение на активите между собствениците ще доведе до йерархия на проследяване на риска, което е повторение на административната йерархия в организацията.

Такава нивова информационна структура е показано на фиг. 3.3.. Тя показва собствениците и информационните активи, за които те трябва да проследяват промяната на рисковите фактори и нивото на риска.

В тази схема, на най-ниското ниво има собственици, които са свързани с материални и информационни активи, но не и със служители, които имат отговорности за СИ. В средата на структурата ще има информационни активи, които по същността си са служители, свързани със СИ. В горната част на информационната структура ще бъдат информационни активи, които нямат собственик и представляват административни ръководители от най-високо ниво, които не са пряко подчинени на друг ръководител. Такава нивова организация ще позволи контрол на събирането и обработването на информация за активите, което съответства на административния контрол за изпълнение на целите на организацията.

Към тази структура трябва да се добави и отдел „човешки ресурси", който е собственик на риска за всички собственици на информационни активи, без най-високото административно ниво.

В тази организационна структура от собствениците на информационни активи е необходимо да се предостави възможност за отчитане и архивиране на информация за контрола върху собствениците.

Пирамидалната информационна структура трябва да е обвързана и със системата за определяне на правата за достъп до различните нива на информация.

3.4. Други елементи на подхода

Основни елементи в предлагания подход са оценъчната система за регулярни проверки на рисковите фактори и йерархичната система за контрол на извършените проверки. На базата на анализираните проблеми при мониторинга на риска за сигурността на информация настоящия подход може да бъде допълнен с още няколко не маловажни организационни предложения. Те са насочени към повишаване на ефективността на събиране и използване на информация за управлението на риска.

3.4.1. Въвеждане на автоматизирани средства за поддръжка на документацията на СУСИ

Констатирано беше, че при изграждане на система за управление на сигурността на информацията се изисква оформяне, съхраняване и ползване на голям обем документи. Налага се изводът, че обработването на информацията за СУСИ на средно голяма или голяма организация, наложително трябва да се извършва със специализирана, компютърна, информационна система. Използването на такава система, ще даде възможност за лесно разширение и надграждане чрез добавяне на нови автоматизирани инструменти за обработка.

Предлагания подход препоръчва акценти и решения за изграждане на автоматизирани средства за подпомагане на мониторинга и управлението на риска за информационната сигурност.

3.4.2. Осигуряване на възможности за въвеждане и извеждане на статистическа информация за СУСИ

Важен елемент от функционалностите на системата е възможността за филтриране на чувствителната информация, която се събира и натрупва по време на изграждането на УРСИ за една организация. Такава функционалност, ще предостави възможност за пренос на основни данни, свързани с оценката на риска, за изграждане на УРСИ за друга организация, без да се нарушава конфиденциалността на организацията. Възможността за обмен на статистическа информация за процесите по управление на риска, между различни СУСИ ще осигури много облекчения при оценката на риска.

Процесът на пренос на информация между системи за УРСИ на различни организации изисква създаване на възможности за въвеждане и извеждане на различни таблици с информация за отделните типове рискови фактори.

3.4.4. Възможност за съхранение на информация за влияния на рисковите фактори между активите

За по-точното отчитане на нивата за риска е необходимо да се въведе отчитане на влиянието на рисковете между активите. Това отчитане трябва да е съпроводено с допълнителна информация, която гарантира проследимост. Необходима е методология за измерване на въздействието.

3.4.5. Съхраняване на информация за ефективността на приложените методи за контрол

За отчитане на ефективността от прилагане на различните методи за

контрол, е необходимо да се предостави възможност за съхраняване на информация за приложените методи за контрол, целта за прилагане и нивото на риска за актива преди и след прилагане на метода за контрол. Необходимо е натрупване на информация за нивото на риска след прилагане на контролата при няколко последователни оценки на риска за актива.

3.4.6. Генериране на добре структурирани справки за работата на системата и измененията на риска

За доброто ефикасно управление на СУСИ важна роля играе качеството на справките, които системата генерира за ръководството на организацията и експертите по информационна сигурност. Справките трябва да обхващат информация за измененията в условията на работа на актива, изменения в контекста на организацията, които косвено влияят на риска за актива, изменения на нивата на риска, сведения за инциденти и предприети мерки, справки за доказателства за ефективно управление на риска, справки с информация, необходима за сертифицираните СУСИ.

3.5. Обща структурна схема на предложения подход

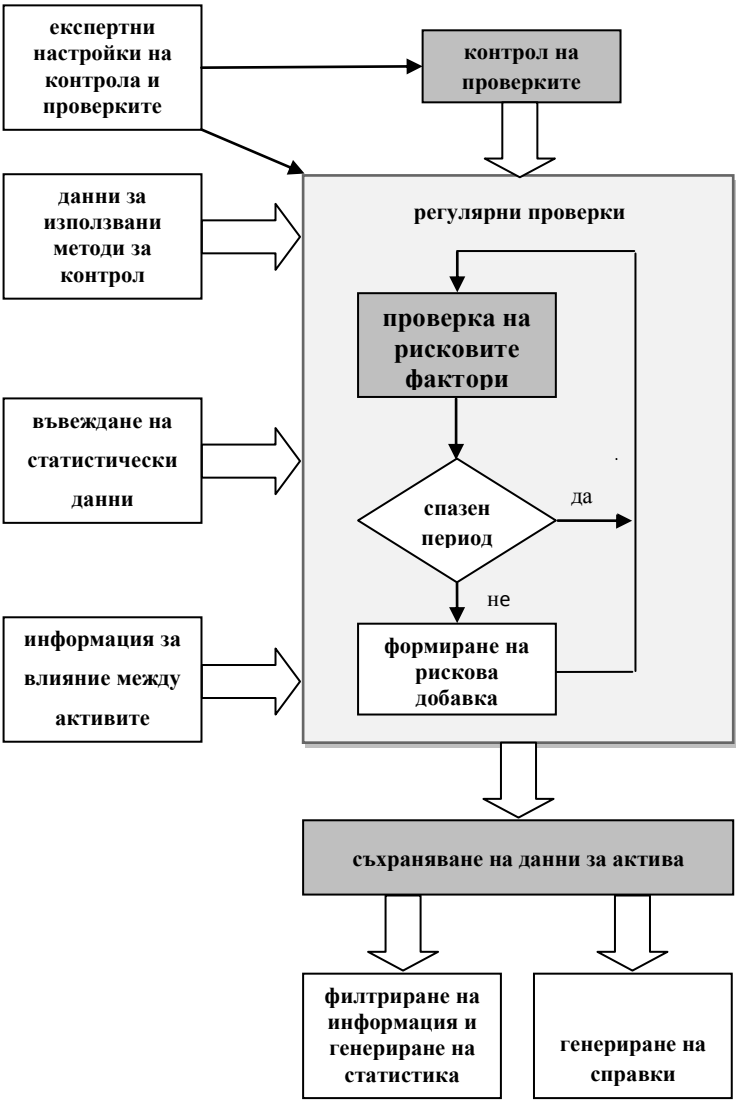
Целта на предложения подхода е да преодолее някои по-съществени затруднения при управлението на риска за СИ. На Фиг. 3.4. е илюстрирана структурна схема на елементите на описания подход.

Основен елемент в подхода е организация на оценка и проследяване на регулярността на проверка и анализ на измененията на рисковите фактори, които влияят на нивото на риска за информационен актив. Системата за оценка на извършваните проверки е допълнена с препоръки за йерархична организация на контрола на работата на собственика на актива.

Съчетаването на тези два основни организационни подхода с акцентиране на важни препоръки за структуриране на информацията и предложени функционални инструменти за нейното обработване, формират цялостния вид на предлагания подход за мониторинг на риска в системи за информационна сигурност.

3.6. Структурни изисквания за реализация на предложения подход

Вземайки предвид препоръките на предложения подход и в съответствие с изискванията на стандартите за сигурност на информацията са формулирани изискванията за реализиране на информационна система с прилагане на описания подход.



Фиг. 3.4. Структурна схема на елементите на подхода за облекчаване на управлението на риска за информационен актив

3.7. Изводи

В тази глава е обоснован и формулиран подход за организиране на по-ефективна реализация на процеса за мониторинг и оценка на риска за

информационната сигурност.

Основните елементи на предложения подход са свързани с организация на провеждането и контрола на мониторинга на рисковите фактори за информационните активи. Към тях са добавени препоръки и идеи за осигуряване на структуриране и съхраняване на основната и помощната информация за цялостния процес на УРСИ.

Подходът предлага оценка на измененията на рисковите фактори, влияещи на нивото на риска за информационните активи. Тази оценка, съчетана с подходящ дисциплинарен процес може да доведе до повишаване на ефективността на УРСИ.

ГЛАВА 4 Изследване на възможностите на предложения подход чрез изграждане на програмна система за оценка и мониторинг на риска за сигурността на информацията

В тази глава се описва примерна реализация на информационна система за обслужване на оценката и мониторинга на риска за сигурността на информацията в една организация с внедрена СУСИ. Целта на реализираната ИС е да се провери възможността за прилагане на препоръките от подхода и да се направи анализ на предимствата от приложените препоръки.

В главата е направен и анализ за въздействие на предложения подхода върху част от проблемите при оценка и мониторинг на риска за сигурността на информацията. Извършена е оценка на прилагането на изведените изрази (2.22) и (2.25) и са изследвани ефектите от прилагане на предложения подход при изграждане на информационна система за УРСИ. В края на главата са направени изводи за получените резултати.

4.2. Описание на някои възможности на реализираната информационна система

4.2.1. Общо описание, потребители, нива(права) на достъп

Създадена е информационна система в която са реализирани повечето от предписанията на описания подход. Системата за управление на бази данни е реализирана на SQL сървър и съдържа 21 таблици и 39 съхранени процедури за управление на данните.

При реализацията на информационната система са спазени дефинираните структурни изисквания за реализация на предложения подход.

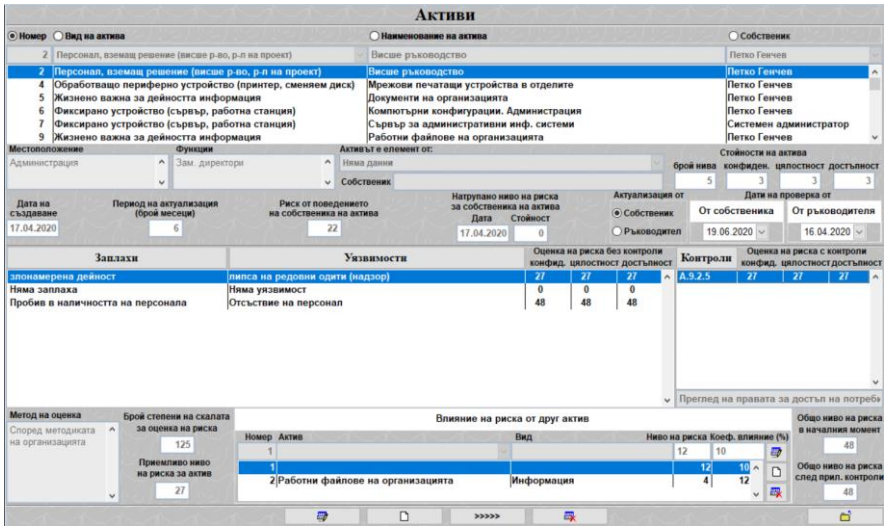
Основен обект в информационната система е информационния актив.

Активите се категоризират по вид съобразно изискванията на стандартите. В системата е предоставена **възможност за въвеждане и допълване на таблици** за заплахите, уязвимостите и за връзки между заплахи и уязвимости. Тези таблици се градят на основата на примерните таблици в стандарта ISO/IEC 27005 и могат да бъдат надграждани чрез добавяне на информация от други СУСИ. Таблиците не съдържат чувствителна информация и могат да се експортират за използване от друга СУСИ.

В съответствие с предложената в използвания подход йерархична структура на въвеждане и контрол на рисковите фактори е реализирана схема на **права за достъп** до данните за активите и реализираните справки.

4.2.2. Основна информация за информационния актив

На фиг. 4.1. е представена снимка на екрана с общата информация за актива. От този екран се отива към екрани за въвеждане на рисковите фактори за актива.



Фиг.4.1. Изглед на екрана за избор на актив и обща информация за избрания актив

Въвеждането на нов актив се осъществява на базата на вид актив и име на актива. Вида на актива се избира от таблица с предварително въведени вид и подвид на актива, които съответстват на препоръчаните от ISO/IEC 27005 видове.

Предвидена е възможност, информацията за всеки актив, да може да се

въвежда и на базата на вече въведен актив с възможност за модификация.

4.2.3. Въвеждане и използване на рисковите фактори в системата

4.2.3.1. Въвеждане на данни за въздействието

Системата позволява съхранение и обработка на три обобщени стойности за стойността на актива за трите критерия – поверителност, цялостност и наличност.

4.2.3.2. Въвеждане на данни за заплахите

Заплахите за разглеждания актив се характеризират с вид на заплахата и описание. Вида на заплахите се въвежда чрез избор от предложения в таблица. Съхранява се помощна информация за произхода на заплахата и това дали тя е предизвикана от външен или от вътрешен източник. За всяка заплаха се въвежда и използва информация за нивото на заплахата.

4.2.3.3. Въвеждане на данни за уязвимости

Името на уязвимостта е в пряка връзка с вида на актива, като на потребителя се предлага избор на вече въведени уязвимости за този вид актив, или въвеждане на ново наименование на уязвимост.

Връзката между уязвимост и заплаха се установява при въвеждане на всяка уязвимост, чрез избор на някоя от въведените заплахи за този актив. Възможен е изборът на опцията „няма заплаха“. Такава уязвимост не участва в анализа на риска, но информацията за всички възможни уязвимости води до подпомагане на оценката на риска.

Предоставена е възможност за въвеждане и използване на три нива на уязвимост преди прилагане на методи за контрол.

4.2.3.4. Въвеждане на данни за използвани механизми за контрол

В продукта е предвидено да се въведе информация за механизмите за контрол, които се използват за защита на активите чрез намаляване на тяхната уязвимост и въздействието от инцидент. В системата се въвежда и информация за типа защита, която осигурява този механизъм.

Съхранява се и информация за нивата на въздействие и нивата на уязвимост след прилагане на мерките за контрол. Предвидени са по три стойности, свързани с неблагоприятните последствия от загуба на поверителност, цялостност и наличност.

4.2.3.5. Актуализиране на данните за нивата на риска

Реализирано е автоматично изчисляване на нивата на риска, на базата на нивата на въздействие, нивата на заплахи и нивата на уязвимост. Визуализирани са нивата на риска преди и след прилагане на механизмите за контрол за всяка валидна двойка заплаха - уязвимост. Освен това има възможност за въвеждане или пресмятане на две интегрални величина на нивата на риска за този актив, преди и след прилагане на мерките за контрол.

В системата се обработват и данни за нивото на риска от некоректен собственик. Формираната рискова добавка се използва при изчисляване на текущата стойност на риска за актива.

4.2.4. Извеждане на справки

Реализираната информационна система предоставя разширени възможности за генериране на структурирани справки и генериране на документи, които се изискват за работата на СУСИ. Предвидени са и справки за натрупваната информация, която може да мигрира към система за УРСИ на друга организация.

4.3. Анализ за въздействие на предложения подход върху част от проблемите

Елементи на подхода / проблеми:	регулярни проверки + рискова добавка	контрол на проверките	вход и изход на статистика	инф. За влия-ния между акти-ви	инф. за прило-жени конт-роли	ефек-тивни справки	информация за използвани методи
събиране и обраб. на данни	влияе	влияе	влияе		частично	влияе	частично
субекти-вен фактор	влияе	влияе	влияе	частично	частично	влияе	частично
ефектив-ност	влияе	влияе	влияе	частично	влияе	влияе	частично

Таблица 4.2. Въздействие на елементите на подхода върху групи проблеми

За да се определят ползите от предложения подход е важно да се отговори на въпроса за влиянието му върху проблемите при прилагане на УРСИ. За целта беше направена съпоставка на реализираните елементи на предложения подход и

групите проблеми, които бяха дефинирани на базата на литературния обзор. Обща представа за това влияние може да се получи от приложената по-долу Таблица 4.2.

След анализ е направен изводът, че предложения подход подпомага решаването на голяма група проблеми, свързани субективния фактор, ефективността и организационните затруднения.

4.4. Оценка на прилагане на подхода за динамична оценка на риска при мониторинг на системи за УРСИ

Извършена е оценка на прилагането на алгоритъма за динамичното формиране на риск за актива и изчисляването на стойността на рисковата добавка от поведението на собственика на актива. За тази цел е реализирана примерна схема на изчисляване на рисковата добавка, в зависимост от провежданите проверки на рисковите фактори от собственика на актив.

Про-верка №	Има про-сроч-ване	Увели-чение към добавката	Брой про-срочени проверки	Средно увеличение	Брой периоди за добра тенденция	Рискова добавка
1	Не	0	0	0	0 +1 = 1	
2	Да	0,03 * R	1	0,03 * R	0	0,03 R
3	Да	0,06 * R	2	0,09 * R /2 = 0,045 * R	0	0,09 R
4	Да	0,03 * R	3	0,12 * R /3 = 0,04 * R	0	0,12 R
5	Не	0	3	0,04 * R	0 +1 = 1	0,12 R
6	Не	0	3	0,04 * R	1 +1 = 2	0,12 R
7	Не	0	2	0,04 * R	0	0,08 R
8	Не	0	2	0,04 * R	0 +1 = 1	0,08 R
9	Не	0	2	0,04 * R	1 +1 = 2	0,08 R
10	Не	0	1	0,04 * R	0	0,04 R
11	Не	0	1	0,04 * R	0 +1 = 1	0,04 R
12	Не	0	1	0,04 * R	1 +1 = 2	0,04 R
13	Не	0	0	0	0	0
14	Не	0	0	0	0	0
15	Не	0	0	0	0	0

Таблица 4.3. Примерно изчисляване на рисковата добавка, зависеща от собственика на актива

При използване на зададени начални данни, резултатите от прилагането на алгоритъма за няколко последователни проверки на рисковите фактори от собственика на актива са отразени в Таблица 4.3.

Изводът е, че предложеният алгоритъм постига подчертаване на отрицателния ефект от недобросъвестното отношение на собственика на актива.

За да се отчетат и ползите от използване на математическия израз (2.22) за определяне на периода между извършваните проверки на рисковите фактори е извършено сравнение на използване на предложения математически израз, спрямо практикувания подход с твърдо зададен период между проверките.

Може да се отчете, че използването на изведените математически изрази (2.22) и (2.25) дава възможност за обективна оценка с цифрови стойности на динамиката на промените на рисковите фактори. Това води до значителни улеснения при оценки и вземане на решения по УРСИ.

4.5. Констатации по прилагане на предложения подход при изграждане на информационна система за УРСИ

При оценка на предложения подход бяха срещнати следните затруднения:

- Прилагането на подхода при оценката и мониторинга на риска на реална УРСИ е труден и бавен процес, свързан с внедряване на информационната система;
- Затруднено е сравняване на възможностите на информационната система с работата на други подобни продукти, защото те са платени и за техните възможности може да се съди единствено по рекламните материали за тях.

Оценка на възможностите на реализираната ИС, е извършена **чрез сравняване** на резултатите от нейната работата с документацията на „ръчно" изградена и сертифицирана СУСИ. За целта в информационната система са въведени част от данните от реализираната СУСИ и са генерирани част от документите, които стандартите изискват за изграждане на СУСИ.

В резултат на направеното сравнение могат да се открояят следните констатации:

- Използване на предложения от подхода структуриран начин за въвеждане на информация в информационната система позволява лесно отделяне на конфиденциалната за организацията информация и извеждане на статистическа информация. Използването на предварително подготвени таблици с информация за различни видове активи позволява избягване на неточни формулировки, въвеждане на излишна и ненужна информация и носи облекчения при съпоставяне на данни за различни информационни активи;
- Генерирането и поддържането на документите за използваните контроли, без използване на информационна система е трудоемък процес,

съпроводен с много грешки и допълнения.;

- Чрез прилагането на създадения алгоритъм за мониторинга на рисковите фактори се постига аргументиране и дисциплиниране на дейностите на собствениците на информационни активи;
- Прилагането на изведените математически изрази позволява оптимално планиране на проверките на рисковите фактори за активите;
- При прилагане на проверките на работата и оценките на собствениците на активите може да се постигне многостепенна оценка на измененията и по точен анализ на предприетите мерки за намаляване на риска. По този начин ще се намали субективността на мониторинга.

Справка на активи с повишен риск към 17.05.2022									
вид актив / подвид	**име на актива**	**собственик**	**период на проверка (дни)**	**дата на следваща проверка**	**просрочване (дни)**	**рискови добавки**	**оценен риск**	**допустимо ниво**	**изчислен текущ риск**
Хардуер / периферно устройство	**Мрежови печатащи устройства в отделите**	мрежов администратор	30	**15.3.2022**	**61**	**1.92; 2.4**	8	15	**24.26 + 2.4**
Мрежа / Носител и поддръжка	**Връзка към Интернет**	мрежов администратор	30	31.5.2022	0	0.96; 0.48	12	15	12 + 0.48
Персонал / вземащ решение	**системен администратор**	ръководителна ИТ отдел	30	**30.4.2022**	**17**	**0; 0.54**	18	20	**28.2 + 0.54**
Информация / Жизнено важна	**Документи на организацията**	отдел деловодство	90	**14.4.2022**	**30**	**0.27; 0.81**	9	27	12 + 0.81
Информация / Жизнено важна	**Работни файлове на организацията**	системен администратор	5	20.5.2022			18	27	
Хардуер / сървър, работна станция	**Компютърни конфигурации. Администрация**	техник от ИТ отдел	7	20.5.2022			8	20	

Фиг. 4.10. Справка за просрочени проверки на рисковите фактори

Като илюстрация на положителните страни на предложения подход за мониторинг на риска, на Фиг. 4.10. е показана справка за активите с повишени нива на риска за информационния актив вследствие на ненавременно провежданите проверки от собствениците на активите. Тази справка дава възможност лесно да се следят всички активи, които са изложени на допълнителен риск вследствие на

просрочване на проверките на рисковите фактори.

От справката се вижда, че при просрочване на проверките, нивото на риска се изчислява чрез израза (2.25) и това е ниво, което надхвърля допустимото ниво на риска за актива. Неспазването на изчислените периоди за проверка е довело до формиране на рискови добавки, които се добавят към нивата на риска от последната оценка риска за актива, или към изчислената стойност на риска според израз (2.25).

4.6. Изводи

От направения анализ на ефекта от прилагането на предложения подход при изграждането на информационна система за УРСИ, може да се заключи, че предложеният подход подпомага решаването на голяма група проблеми. Влиянието на подхода е ясно изразено за проблемите със субективния фактор, ефективността и организационните затруднения.

ЗАКЛЮЧЕНИЕ

Целта на дисертационния труд е да се предложи подход за организиране на по-ефективен начин на въвеждане, обработване и мониторинг на информация, която е необходима за система за управление на риска за сигурността на информацията в една организация.

В изпълнение на поставената цел и на базата на извършените анализи на проблемите и измененията на рисковите фактори е формулиран е общ подход за мониторинг на риска за информационните активи.

Реализирана е информационна система за подпомагане на дейностите по оценка и мониторинг на риска за информационната сигурност в една организация. В нея са приложени основните елементи на дефинирания подход. Направени са изводи за ползите от прилагането на предложения подход за повишаване на ефективността на управлението на риска и документалното поддържане на системи за управление на сигурността на информацията в една организация.

ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

Приноси с научно-приложен характер:

- Предложен е подход за ефикасно управление на риска за сигурността на информацията, чрез подходящо въвеждане и обработване на данни за рисковите фактори и прилагане на динамична система за тяхното регулярно наблюдение;
- Изведени са математически изрази за определяне на периодичността на проверките на рисковите фактори и за определяне на текуща стойност на вероятността за инцидент между две проверки на рисковите фактори;
- Предложен е алгоритъм за оценка на периодичността на проверките за риска на информационен актив;
- Предложен е алгоритъм за йерархична организация на контрола на извършваните проверки за риска на информационен актив;

Приноси с приложен характер:

Предложения подход е илюстриран в примерна реализация на информационна система за обслужване на управление на риска за сигурността на информацията в организация с внедрена СУСИ. Работата на информационната система доказва повишаване на ефективността на управлението на риска.

Списък на публикации по дисертационния труд

1. Генчев П., М. Карова, “Оценка на риска в системи за управление на сигурността на информацията – същност и насоки.”, Компютърни науки и технологии, ТУ-Варна, 2018, бр. 2, с. 96-104, ISSN: 1312-3335
2. Genchev P., M. Karova, “Analysis of some issues in risk assessment for information security.”, Computer Science and Technologies, TU-Varna, 2019, Vol. 1, p.p. 62-70, ISSN: 1312-3335
3. Genchev P., “An approach to support information security risk assessment.”, Published in: 2020 International Conference on Biomedical Innovations and Applications (BIA), 24-27 Sept, 2020, in Varna, Bulgaria, Electronic ISBN:978-1-7281-7073-2, Print on Demand(PoD) ISBN:978-1-7281-7074-9, 2020, Page(s): 125 – 128, Indexed in SCOPUS.
4. Генчев П., Н. Николов, “Програмна система за оценка на риска за информационната сигурност.”, Компютърни науки и технологии, ТУ-Варна, 2020, бр.1, с. 101-110, ISSN: 1312-3335
5. Genchev P, “Analysis of changes in the probability of an incident with information security.”, Published in: 56th International Scientific Conference on Information, Communication and Energy Systems and Ttechnologies (ICEST) june 16-18 2021, Sozopol, Bulgaria, DOI: 10.1109/ICEST52640.2021, 16-18 June 2021, Publication Year: 2021,Page(s):119 – 122, Indexed in SCOPUS.
6. Genchev P., M. Mileva-Karova, “Determining the period for information security risk checks.”, Proceedings International Scientific Conference CONFSEC 2021 ISSN 2603-2945 (Print), ISSN 2603-2953 (Web).

Списък на участия в проекти

1. ФНИ НП9 ТУ-Варна (2019), „Изследване на криптографски алгоритми и методи от машинно обучение за създаване на интелигентни системи“ с ръководител доц. д-р Ивайло Пенев;
2. ФНИ ПД5 ТУ-Варна (2019), „Изследване на методи за оценка на риска за информационни активи“ с ръководител доц. д-р Милена Карова;
3. ФНИ НП5 ТУ-Варна (2020), „Изследване на възможностите за интегриране на машинно обучение и блокчейн технологии за Internet of Things“ с ръководител доц. д-р Жейно Жейнов;

Специални благодарности на:
Доц. д-р инж. Милена Карова, доц. д-р инж. Ивайло Пенев, доц. д-р инж. Христо Вълчанов, на моето семейство и на всички колеги, които са били съпричастни към моята дисертационна работа и са ми помогнали със съвети и подкрепа.

An approach to risk monitoring in information security systems

PhD Thesis Abstract

Petko Genchev Genchev

In today's world, information security is of paramount importance to organizations. A systematic approach to information security risk management is required. These facts determine the relevance of research in the field of increasing the effectiveness of risk management systems for information security and overcoming problems arising in the construction and operation of such systems.

The aim of the dissertation work is to investigate the possibilities of overcoming some of the problems in the implementation of information security risk management systems. As a result of conducted research and analysis, to propose an approach to overcome basic problems in risk assessment and monitoring in information security systems.

The disertation work consists of 4 chapters:

Chapter 1 describes an overview of the requirements of ISO standards in the field of information security. An overview of the main difficulties found during the implementation of information security risk assessment and monitoring activities was carried out. Based on the studies, an analysis was carried out and steps to overcome the problems were marked, and the goals and objectives of the dissertation work were identified.

In the 2nd chapter, an analysis of the probabilistic characteristics of changes in risk factors is made. Based on this analysis, a mathematical expression is derived to calculate the time until the next necessary check to account for changes and new information security risk values. A mathematical expression for calculating the current value of the risk after a risk assessment has been carried out is also derived.

Chapter 3 is dedicated to formulating an approach to overcome some problems in assessing and monitoring information security risk. The main elements of the proposed approach are related to the organization of conducting and controlling the monitoring of risk factors for information assets.

The 4th chapter describes an exemplary implementation of an information system for the evaluation and monitoring of information security risk in an organization with an implemented information security management system. The proposed approach is implemented in the realized information system.

Conducted research and analysis confirm the thesis that the application of the proposed approach helps to solve a large group of problems related to the subjective factor, efficiency and organizational difficulties.