ВАРНЕНСКИ СВОБОДЕН УНИВЕРСИТЕТ
“ЧЕРНОРИЗЕЦ ХРАБЪР“
ФАКУЛТЕТ„МЕЖДУНАРОДНА ИКОНОМИКА И АДМИНИСТРАЦИЯ”
КАТЕДРА „АДМИНИСТРАЦИЯ, УПРАВЛЕНИЕ И ПОЛИТИЧЕСКИ НАУКИ”

НИКОЛА ТИЛЕВ ИВАНОВ

УПРАВЛЕНИЕ НА РИСКА И НЕПРЕКЪСВАЕМОСТТА НА ИНФОРМАЦИОННО-ТЕХНОЛОГИЧНИ ПРОЦЕСИ В ПУБЛИЧНИЯ СЕКТОР И БИЗНЕСА

А В Т О Р Е Ф Е Р А Т

на дисертационен труд
за придобиване на образователна и научна степен „доктор”
Професионално направление 3.7. „Администрация и управление”,
Докторска програма „Организация и управление извън сферата на материалното производство”

Варна, 2017

ВАРНЕНСКИ СВОБОДЕН УНИВЕРСИТЕТ
“ЧЕРНОРИЗЕЦ ХРАБЪР“
ФАКУЛТЕТ„МЕЖДУНАРОДНА ИКОНОМИКА И АДМИНИСТРАЦИЯ”
КАТЕДРА „АДМИНИСТРАЦИЯ, УПРАВЛЕНИЕ И ПОЛИТИЧЕСКИ НАУКИ”

НИКОЛА ТИЛЕВ ИВАНОВ

УПРАВЛЕНИЕ НА РИСКА И НЕПРЕКЪСВАЕМОСТТА НА ИНФОРМАЦИОННО-ТЕХНОЛОГИЧНИ ПРОЦЕСИ В ПУБЛИЧНИЯ СЕКТОР И БИЗНЕСА

А В Т О Р Е Ф Е Р А Т
на дисертационен труд
за получаване на образователна и научна степен „доктор”
Професионално направление 3.7 „Администрация и управление”,
Докторска програма „Организация и управление извън сферата на материалното производство”

Научен ръководител:

Проф. д-р Павел Георгиев Павлов

Рецензенти:

Проф. д-р Георги Коев Ботев

Проф. д.т.н. Кирил Петров Ангелов

Варна, 2017

Дисертационният труд е с обем 262 страници, стои се от списък на използвани съкращения, списък на използвани термини, увод, 3глави, заключение,използвана литература и 7 приложения.Основния текст съдържа 13 таблици и 13 фигури.

Списъкът на използваните литературни източници наброява 235 заглавия на български, руски и английски език. Цитира 37 нормативни документа.

Дисертационният труд е обсъден в катедра „Администрация, управление и политически науки“ на факултет „Международна икономика и администрация“ и насочен за защита пред научно жури.

Публичната защита ще се проведе на открито заседание на научното жури на 10.10.2017г. от 10,00ч. в Заседателната зала на Ректората на ВСУ “Черноризец Храбър“.

Материалите по защитата са достъпни в кабинет 204 във ВСУ „Черноризец Храбър“ и на сайта www.vfu.bg, раздел „Докторантура“.

I. ОБЩО ОПИСАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност и значимост на изследването.

Актуалността на избраната тема за дисертационно изследване е продиктувана от необходимостта по-добре да се управляват негативните въздействия на рисковете и прекъсванията на информационно-технологични процеси (ИТП) в публичния сектор и бизнеса. Многобройни са тревожните събития, пред които е изправено обществото в прехода към модерност. Желаното подобряване и развитие на ИТП се изправя пред многостранни опасности, заплахи и рискове, провокирани както поради природни бедствия (земетресения, наводнения, свличания, засушавания, внезапни трусове и шокове), така и причинени от обществото катастрофални събития (ядрени инциденти, петролни разливи, климатични промени, водни, почвени и атмосферни замърсявания) и други все по-нови уязвяващи фактори. Не по-малко значими са и разнообразни вътрешни и външни за организациите злоумишлени или непреднамерени вредоносни въздействия. Изследването, селекцията и прилагането на подходящи теоретически обобщения, методически подходи, модели, методи, методики и добри практики за справяне с уязвяващите събития е първостепенна необходимост за рационално решение на възникващите проблеми.

2. Обект и предмет на изследване.

Обект на изследването са рискът и непрекъсваемостта на ИТП в публичния и бизнес сектора. Ефектите от техните нежелани въздействия в двата сектора не се различават съществено. Различна е организационната среда, в която те се проявяват. Все по-често чрез механизмите за аутсорсинг публичните процеси се изпълняват от бизнес структури. Това е основание международната практика да ги разглежда и като бизнес процеси. Към това разбиране се придържа и настоящото изследване, в което под бизнес процеси в определени случаи се включват и тези протичащи в публичната администрация.

Тогава, когато е необходимо подчертаване на различия, те се адресират към отделните сектори.

Предмет на изследване е управлението на риска и непрекъсваемостта (УРН) на публичните и бизнес ИТП. Под рискове най-общо се разбират събития, които биха могли да отклоняват процесите от техните цели и резултати, и биха могли при определени обстоятелства да водят до тяхното нежелано прекъсване. Непрекъсваемостта е способност за запазване на изпълнението на ИТП в условията на разнообразни рискове и реални негативни въздействия. Управлението на тази способност е ключов въпрос на информационната сигурност, в отговор на който изследването се фокусира върхуприлагане на три основни направления на изследване – прилагане на проблемно-ориентиран, интегриран и международно стандартизиран подход; процесен модел и методическа рамка за УРН, насочени за предотвратяване на прекъсвания и възстановяване при възникване на инциденти, извънредни и непредвидени ситуации.

3. Ограничения на изследването.

Диференциацията на ИТП и информационни системи (ИС) в публичния сектор и бизнеса (кадрови, финансови, комуникационни, за разнообразни услуги, управление при кризи и извънредни ситуации, в критичната инфраструктура и пр.) води до голямо разнообразие на развиващи се във времето средства (теории, подходи, модели, методи, методики, техники, процеси, роли, контроли и метрики) за УРН. Изследването приемаследните **ограничения** на обхвата на труда:

- Включва само средствата за УРН на ИТП в публичните организации и бизнеса в страната, които не оперират с класифицирана информация.
- Основава се на анализ на приложението на международно приети и стандартизирани подходи, методи и практики като не включва тясно специализираните инструменти за справяне със специфични видове риск и непрекъсваемост.

- Фокусира се върху стратегическите подходи, организационно-тактическите и оперативно технологични средства, вкл. „back up“/“бекъп“ инструментите за осигуряване на непрекъсваемост.

- Тестването на предложените средства е ограничено в условията на публична банкова дейност и пътно-строителен бизнес в страната.

- Поради динамиката на промените при УРН на ИТП изследването включва тенденциите в кратко и средносрочен периодбез да засяга много по-сложните, дългосрочни и глобални проблеми на развиващото се общество. Извън неговия обхват остават проблемите на свързаната информационна революция, ефектите на т.н. „дезинформирано информационно общество” и идеите за информационна сигурност,водещи до разрушаване на обособеното лично пространство, манипулации и ограничаване на възможностите за рефлексия и критика на действителността.[1]

4. Изследователски проблем.

Основен **проблем** на изследването е неразвитото състояние на практиката за УРН на ИТП в публичния и бизнес сектора в национален план. То приема, че предприеманите усилия не са адекватно насочени и приоритизирани, не са осигурени с необходимите ресурси и не са съобразени с последствията от забавените действия. Те не са подкрепени в достатъчна степен със съвременни иновативни аналитични, проектни, програмни, планови, одитни, и нормативно-контролни механизми и инструменти, с които е възможно справяне с този дефицит. Потвърждения за това са множеството случаи на прекъсване на критични и ключови ИТП, вкл. достъп до електронни мрежи, причиняващи отказ на административни, финансови, здравни и др. услуги, прекъсване на електроснабдяване, водоснабдяване и пр.

С развитието на ИС и процеси нарастват и специфичните и остри проблеми на УРН за ИС в критичната инфраструктура (КИ), засягащи пряко дейността и живота на големи обществени групи в страната. Дигитализацията

[1]Лаш, Ст., Критика на информацията, ИК „Кота”, С., 2004.

навлиза все по-дълбоко в базовите сфери на личния и обществен живот.[2] Управлението на информацията (УИ), включващо натрупване и обработка и пренос на информация (лични досиета, публични регистри, бизнес бази данни, данни от социалните мрежи и други масиви), освен че е уязвимо от естествени и непреднамерени негативни въздействия, създава възможности за несанкциониран достъп със зловредни цели. Такъв достъп е заплаха и проблем за правото за личен живот, обществената и бизнес кибер сигурност. Прекъсването на законово санкционирания достъп до данните и информацията на КИ с различни вредоносни цели е въздействие с особено тежки последици. Понякога такива прекъсвания имат далече по-мащабни и значими негативни ефекти, отколкото традиционните форми на несанкциониран достъп, поради което изискват прилагане на специфични защитни средства.

5. Изследователска теза.

Изследването защитава **тезата**, че подобряването на УРН на публичните и бизнес ИТП, чрез прилагане на проблемно-ориентиран (фокусиран върху прекъсванията на ИТП), интегриран (за риска и непрекъсваемостта)и международно стандартизиран подход, процесен модел и съобразена с тях методическа рамка за анализ и проектиране на защитени от прекъсване ИТПще постави риска за организационната и информационна сигурност в приемливи граници. Структурирането и стандартизирането на процеса на анализ, проектиране, внедряване, мониторинг, одит и документиране на промяната на управлението ще намали вероятността и щетите от прекъсване, ще съкрати времето за възстановяване и повиши качеството и ефективността на използваните ИТП и предлагани услуги.

Никой не е в състояние да предвиди предстоящите драматични събития. Организациите, обаче трябва да бъдат подготвени за тях, като предприемат предварителни одитни действия, изработят визия, приемат политика и стратегия, проектират, програмират и планират своите действия за управление

[2]Солъв, Д., Дигиталната личност, изд. „Планета”, С., 2010.

на организационнияи информационен риск и непрекъсваемостта на ИТП като ключова част на своите цели, организация и практики за изпълнение.

Тази теза е конкретизирана със следните **подтези**:

- Установяването на адекватна на нестабилността на средата и уязвимостта на организациитевизия, политика и стратегия за УРН на ИТП е базов фактор за иновация на организационното управление в бизнеса и публичния сектор.

- Предварителният и последващ промяната одит на дейността по УРН, вкл. събирането на данни, анализа на сигурността и оценкатана съответствието с националните норми и международни стандарти за готовността на ИТП и системи да посрещнат предизвикателствата на заплахите и рисковете е основа за избор на визията, политика и стратегия за противодействие и гаранция за адекватно организационно управление.

- Концептуалното проектиране на системи за УРН (СУРН), програмиране и планиране на възстановяването при инциденти, извънредни ситуации (бедствия и аварии) и неопределеност (непредвидени събития) са решаващи за овладяване на нежелани прекъсвания на ИТП.

- Интегрирането на процесите и операциите по политико-стратегическо насочване, организационно-тактическо осигуряване и оперативно-инструментална защита, вкл. „бекъп“ на данните при УРН е в състояние да снижи разходите и повиши ефективността на прилаганите ИТ.

- Мобилизираните ресурси за УРН трябва да са съобразени и оправдани с потенциалните щети от вредоносни въздействия и ефекти от прекъсвания на ИТП.Ресурсите, които ограничават обхвата на организационните цели и решавани проблеми са определящи за визията, политиката и стратегията за УРН.

6. Цел и задачи на изследване.

Цел на изследването е да се предложат и тестват концептуални насоки, вкл. проблемно-ориентиран, интегриран и международно стандартизиран

подход, процесен модел и методическа рамка за политико-стратегическо насочване, организационно-тактическо осигуряване и оперативно-инструментален контрол за УРН на ИТП. С това то може да подпомогне организациите да оценят реалните заплахи, рискове, разполагаеми ресурси, желани резултати, да определят достигнатата зрялост на УРН и изяснят възможностите за постигане на позитивни ефекти, както за качеството на предоставяните административни услуги за гражданите и информационните активи на публичния сектор, така и за подобряване на ефективността на прилагащите съвременни ИТП бизнес организации.

Поставената цел включва за решаване следните **изследователски задачи**:

- Да се анализират теоретическите и методологически схващания за същността и практиката за УРН на публичните и бизнес ИТП и идентификация на основните проблеми при тяхното прилагане.
- Да се анализират алтернативните насоки и избор на подход, процесен модел и методическа рамка за одит и концептуално проектиране на политико-стратегическо насочване, организационно-тактическо осигуряване и оперативно-инструментален контрол, вкл. програмиране и планиране, включващи набор от средства, методи, техникии инструменти за подобряванена УРН на ИТП.
- Да се тества методическата рамка за УРН, интерпретираща предложения подход и процесен модел в условията на конкретниорганизации от публичния банков сектор и пътно-строителния бизнес.

7. Методология на изследването.

Използваният **изследователски инструментариум** включва проучване на теоретичните основи, методологията, методите, моделите, набор на информация от известните публикации, нормативи и стандарти от електронната мрежа, последващ кабинетен анализ, аргументация на решения и емпирична проверка с пилотни примери от практиката. Включва предложение за набор от прилагани в международната практика подходи и методи за УРН, вкл. на

критерии и метрика за оценка на параметри (MTD/MTO, RPO и RTO)[3] и „бекъп“[4] инструменти за възстановяване на информация и повишаване непрекъсваемостта на ИТП.

8. Основни информационни източници.

Изследването се базира на посочените в литературната справка национални и чужди литературни източници, норми и международни стандартизационни документи. Използваните в него данни се базират на опита на докторанта от участия в одит, анализ,проектиране и експлоатация на публични и бизнес непрекъсваеми ИС.

9. Потребители на резултатите на изследването.

Резултатите от изследването могат да бъдат използвани, както от висшите ръководители, мениджърите и операторите, така и от проектантите на ИС, за които има изисквания за УРН на изпълняваните дейности и ИТП. Те са насочени основно към административни и бизнес лидери, чиято дейност е свързана с управление на мисионно и бизнес ориентирани ключови и критични ИТП, както и за специалистите, които проектират и поддържат съответни ИС. Могат да представлява интерес и за заетите с нормативно регламентиране на изискванията за ИТП, както и за интересуващите се и обучаваните по проблемите на УРН в публичния сектор и бизнеса.

II. ОБЕМ И СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационния труд е с обем 256 стр. Включва списък на използвани съкращения, списък на използвани термини, увод, 3 глави, заключение, използвана литература и 7 приложения. Съдържанието на главите е разделено на отделни параграфи и подраздели. Основния текст съдържа 13 таблици и 13 фигури.

[3]MTD(MTO)/МБО – максимално допустимо време за отказ на достъп; RPO/ЦТВ – Целева точка за възстановяване; RTO/ЦВВ – Целево време за възстановяване.
[4]„бекъп“ –възстановяване на информацията към определен минал момент (RPO/ЦВТ).

Списъкът на използваните литературни източници наброява 235 заглавия на български, руски и английски език. Цитира 37 нормативни документа.

Приложенията включват: 1. Стандарти за управление на информационната сигурност и непрекъсваемост; 2. Организации, на които е проучена практиката за управление на риска; 3. Набор от документи и записи, изисквани при сертификация по ISO 22301 Управление на непрекъсваемостта; 4. Препоръчвани от Корпорация РАНД алтернативни действия за стратегическо, организационно и оперативно УН; 5. Списък на одиторите на банковата система на страната от 2016 г.; 6. Въпросник и данни за идентифициране на проблемите и практиката за УРН на Българска банка за развитие АД (ББР) и „Трейс Груп Холдинг АД“ (ТГХ); 7. Въпросник и данни от одит и оценка на практиката за УНБ, приложение и сертификация по ISO 22301 на ББР/ТГХ.

СЪДЪРЖАНИЕ:

ЗАКЛЮЧЕНИЕ
ИЗПОЛЗВАНА ЛИТЕРАТУРА
ПРИЛОЖЕНИЯ

III. КРАТКО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

В УВОДА на изследването се подчертава, че съвремието предлага непрекъсната промяна на ролята на информационните технологии (ИТ) във всички области на съвременния живот. Представят се разнообразни идеи, които осмислят тази промяна. Отбелязва се, че все повече между тях надделява виждането за доминиращото значение на ИТ за ефективността на вземаните решения при справяне с възникващите негативни явления и процеси в обществения живот. Аргументира се необходимостта от изследване на УРН на ИТП в публичния сектор и бизнеса.

Обосновава се актуалността и значимостта на изследваната тема. Определя се обекта и предмета на изследване. Очертават се ограниченията на изследването. Идентифицират се изследователските проблеми. Лансира се изследователската теза. Дефинира се целта, подцелите и задачите на изследването. Представя се приложената методология и информационната база, с която е основано изследването. Посочват се потенциалните потребители на постигнатите резултати.

В Първа глава „Теоретични аспекти, състояние и проблеми на УРН на ИТП в публичния сектор и бизнеса“ се представат теоретичните схващания и състоянието на основните аспекти при УРН в международен и национален план., идентифицират се основните проблеми на националната практика.

В Параграф 1.1. се представят теоретичните схващания за информационна сигурност, риска и непрекъсваемостта на ИТП. Очертава се корелацията на развитието на ИТП с възникването и развитието на теоретическите идеи за информационна сигурност, Отбелязва се въздействието на мрежовата комуникация върху информационните характеристики. Въвеждат

се приетите в международната практика дефиниции за надеждност и непрекъсваемост на ИТП в контекста на Теорията надеждността на техническите системи в инженерното дело. Подчертават се съществуващите различия на подхода към надеждността на ИС и ИТП в западната и източна практика. Обръща се внимание на развитието на новите идеи за информационно пространство и ескалацията на кибер рисковете в епохата на глобална дигитализация. Извеждат се основните ориентири за информационна сигурност и необходимостта от прилагане на устойчива политика за УРН на ИТП. Аргументира се приемането на схващане за информационна сигурност включваща зона на традиционни рискове и зона на киберсигурността. Очертава се обхвата, принципите и елементите на политиката за управление на непрекъсваемостта (УН).

В Параграф 1.2. се въвежда темата за УРН на ИТП в публичния сектор и бизнеса, която характеризира нарастващия интерес към управлението на риска (УР) като средство за гарантиране на организационна и информационна сигурност. Представят се основните въпроси при изследване на риска, неговата същност, видове и основни характеристики. Представя се националната нормативна уредба за управление на организационния риск (УОР) и включените в нея процеси и организация.

Разширява се нормативната рамка с проблематиката за управление на информационния риск (УИР) и УН на ИТП в контекста на кибер сигурността на организациите в публичния сектор и бизнеса. Дефинират се елементите на кибер сигурността (конфиденциалност, интегритет и разполагаемост/достъп) на информацията. Аргументира се необходимостта от преход към интегрално третиране на организационния риск (ОР) и информационния риск (ИР) в публичния сектор и бизнеса. Представят се основни схващания и дефиниции за непрекъсваемостта на ИТП, както и приложимите стандарти за нейното управление. Подчертава се необходимостта от изграждане на операционна гъвкавост на процесите и способност за отговор на прекъсванията, както и

ролята на предварителното планиране и подготовката за прекъсвания. Излагат се аргументи за приемане на международно стандартизирано и интегрирано УРН в публичния сектор и бизнеса в страната.

В Параграф 1.3. се идентифицират проблемите на УРН в глобален и национален план. Представят се изводите от проведени анкетни проучвания като прави обобщен извод за изоставане на националната практика от глобалните тенденции. Показва се, че голяма част от организациите в света и Европа (над 60%) осъзнават, че са изправени пред комплексни и нарастващи рискови проблеми, но само половината от тях (35%) прилагат формално УР. Ограничено проучване на 50 организации в страната показва, че почти всички организации от публичния сектор (около 3500) и използващи публични ресурси и ограничен брой големи бизнес компании са приели политика и изградили формално управление на риска. Изградените системи са съобразени с нормативните изисквания на Закона за финансово управление и контрол. Само 4% от проучените организации докладват за внедряване на международни системи за УР.

Приведените ориентировъчни данни позволяват да се направи обобщен извод за изоставане на националната практика за управление на ОР в сравнение със световната рамка, в която около 35% от бизнес организациите посочват наличие на системи за УР. Въпреки често отбелязваното добро състояние на внедряване на ИТ, направеното проучване не показва и активно развитие на практиките за УИР и непрекъсваемостта на ИТП в страната. Напротив, то показва наличие на пречки, проблеми и изоставане на практиката за управление.

В параграфа се представя по-детайлна идентификация на следните основни проблемни области на националната практика – визия, регулаторна среда, политика и стратегията, планирането и програмирането на противодействието за УРН. Конкретизират се възникващите проблеми по отношение на визията, политиката, целевото насочване и стратегията,

програмирането, планирането и противодействието на рискапри УРН. Отделя се внимание на проблематиката на УРН в организациите от КИ в страната.

Изводи от Първа глава:

1. Прогресът на ИТ ускорява развитието на материалната и духовна сфера на обществения живот, но поставя редица сложни проблеми на сигурността на информацията в публичния сектор и бизнеса.

2. Към традиционните рискове (от природни бедствия и други обществени катастрофални събития) се добавят киберрисковете с мрежов характер съсзначително въздействие и нарастваща вероятност за прекъсване на изпълняваните ИТП и ограничаване на достъпа до информационните активи.

3. Потенциални кибер атаки, съчетани с вероятни бедствия и аварии изискват систематично управление на информационна сигурност, поддържане на достъпа, работоспособността и непрекъсваемостта на действие, планиране и оперативен контрол на възстановяването на КИ и на останалите публични обекти и уязвимите бизнес структури.

4. Прекъсването на ИТП, вкл. и на достъпа до ИС е нарастващо актуален проблем на информационната сигурност. Непрекъсваемостта е качество на ИС, технологии, процеси, операции и продукти, което характеризира степента на постигнати специфични изисквания за достъпност и възстановяване на информационните активи при възникнало прекъсване на достъпа. Политиката за непрекъсваемост е само една от необходимите политики, които целят гарантиране на информационната сигурност в публичния сектор и бизнеса.

5. Ключов организационен проблем е изоставането на практиката за УРН на ИТП в публичния и бизнес сектора на страната в сравнение с водещите страни в ЕС и света. Тя е изправена предмножество пречки, ограничения и нерешени въпроси, коитозасягат идентификацията на контекста, визията за сигурност, политиката и регулаторна среда, целевото насочване и стратегията, планирането, програмирането и проектирането на СУРН.

6. Организациите от публичния сектор и бизнеса са изправени пред трудно изброими и идентифицируемирискове. Нараства частта от тях, която развиват своите ИС и са изправени пред усложняващи се ОР, ИР и прекъсване на критични ИТП. Те разполагат с ограничени ресурси и трябва да намерят решения за сигурността на използваната информация, които гарантират най-добра възвръщаемост на инвестициите и текущите разходи.

7. Нормативната уредба за УРН на ИТП в страната е в начална фаза на развитие, както в бизнеса, така и в публичния сектор. Последователното и ускорено внедряване на национални норми и международни стандарти за ефикасно управление на организационния и ИР в публичния сектор и бизнеса в страната е наложителна предпоставка за успешен преход към интегрирано УРН на ИТП.

8. Предприеманите действия от организациите в страната не са адекватно насочени и приоритизирани, не са осигурени с необходимите ресурси и не са съобразени с последствията от забавените действия. Те не са подкрепени от иновативен проблемно-ориентиран, интегриран и стандартизиран подход,процесен модел и методическа рамка за предварителен анализ на подготвеността, концептуално проектиране, програмиране, планиране и текущ мониторинг и одит на съответствието на добрите практики за УРН. Не се използват международните стандарти за описание на изградените и оперираща СУРН. Разработката, нормативното регламентиране, внедряването и непрекъснатото подобряване на тези инструменти е приоритетна насока за справяне с очертания дефицит.

Втора глава „Алтернативни практики, подходи, модел и рамка за УРН на ИТП“ включва обобщение на прилаганите национални практики, аргументира приемането на проблемно-ориентиран, интегриран и международно стандартизиран подход, процесен модел и методическа рамка за УРН на ИТП.

В Параграф 2.1. се обобщават националните организационни практики за УРН. Разграничават се четири групи организации, опита на които свързва с

достигнатото равнище на зрялост на тяхната организационна култура. Установява се, че за първата група е присъща култура с ниско равнище на зрялост, обикновено определяна като "начална" или „анархична".[5] Характерна за нея е слаба приспособеност и зависимост от промените на външния контекст, както и ограничени способности за вътрешна промяна. Тя не създава стабилен вътрешен контекст за устойчивост на процесите. Успехът при нея зависи основно от компетентността и усилията на персонала, а не от прилагането на изпитани процеси. Естествен изход от това може да бъде приемлив резултат, но ипонижена административна и конкурентна способност,както и предстояща проблемна дилема за бъдещ крах или промяна под въздействие на външния контекст. Подходът на тези организации може да се определи като „ирационално пренебрегване на УР".

Втората група изгражда ИС за подкрепа на вземаните решения. Тези организации са на второ, „управляемо" или „фолклорно" равнище на зрялост. При тях се прилага процес на планиране и управление, в съответствие с установена политика. Използват компетентен персонал, осигурен с необходимите ресурси. Фокусирани са върху проблемите на риска и оцеляването. Те имат различна стартова позиция и прибягват до внедряване на достъпни рамки и стандарти за подобряване на управленската практика. Алтернативи за това са практиките на ITIL, LEAN, SixSigma, COBIT, CMMI, Prince 2, PIMBOK (последните две за проектно управление), ISO 9000 и стандартите от серията ISO/IEC 20000.[6]Тази, все по-голяма, част от организациите изпитва и приема промените на средата, и предприема ограничен кръг от мерки за УР. Тези организации предприемат действия за управление на ОР и приемат култура на промяната. Организационната култура за тях се характеризира с ново съчетание от духовни и материални ценности, съответстващи на реалността на публичния, бизнес, частен, личен или друг

[5]Chrissis, M. B., M. Konrad, S. Shrum, CMMI, Guidelaines for Process Integration and Product Improvement, Second Edition, Addison-Wesley, Upper Saddle River, 2007, p. 52.
[6] ITIL, Best management Practice, Service Strategy, 2011 edition, www.best-management-practice.com.

аспект на живота.[7] Достигнатата културна зрялост е ограничаваща рамка за вземаните ключови решения, вкл. по отношение на защитата на приетите ценности и цели от вътрешни и външни въздействия и атаки. Тя започва да влияе на визията, политиката, целите, стратегиите, организационната структура и оперирането. Обогатява стила на управление, който моделира отговора на различните комбинации от външни и вътрешни уязвяващи обстоятелства. Създаваните информационни услуги и продукти са видими и контролирани от мениджмънта в определени критични точки. На практика тези организации не управляват непрекъсваемостта на процесите, но в ограничена степен се придържат към принципите, правилата и стандартите за УОР, като предпоставка за УИР. Причина за това е все още ограниченото прилагане на ИТ в управлението. Подходът на тези организации може да бъде определен като „ограничено управление на ОР".

Третата група притежава организационна култура на следващото, наричано „дефинирано" или „стандартизирано" равнище на зрялост. Те приемат и развиватвъв времето своите политики, процедури, инструменти и методи в съответствие с международните стандарти за УИР и сигурност. Разликата на тези организации от тези на предходното равнище на зрялост е в обхвата на стандартите, процесните описания и процедурите. Различията в тях за отделните фази от процесите и процедурите се избягват чрез съобразяване и придържане към общи и интегрирани процеси за организацията. Това означава преход към интеграция на всички информационни процеси.Тези организации изграждат и поддържат Системи за управление на информационната сигурност - СУИС (InformationSecurityManagementSystem – ISMS). Базовият стандарт за тези системи съдържа рамка и операционен модел за процес на управление. Включва семейство от стандарти, които очертават различни аспекти на системата за управление, приложими за защита на информацията. Базов аспект на

[7]Ivanov, T, Cyber Security Culture – Personnel Domain, MA "G.S. Rakovsky", 2015.

организационната политика е управление на риска за информационната сигурност.[8]

Четвъртата група организации, притежаващи зрялост на равнище „количествено управление“, установяват количествени цели за процесните характеристики, които използват като критерии за интегрирано управление. Задължително включват натрупване на статистическа информация за процесите от жизнения цикъл. С нея те установяват специфичните причини за отклонения от целите и отчитат интересите на заинтересованите страни от управлението. С това постигат количествена предвидимост на процесите, което е и разликата от предходното ниво на зрялост с качествена предвидимост.Организациите на това ниво на зрялост фокусират своето внимание към надеждността и предотвратяване на откази и достъпдо предоставяните информационни услуги и свързаните ИТП. Най-често тези организации предприемат и по-специализирани мерки за УР в контекста на непрекъсваемост на изпълняваните процеси.[9] Характерно за тях е, че не са защитени от специфични информационни (вкл. кибер) рискове, които водят до критично прекъсване на протичащите процеси. При тях управлението на ИР е базова рамка за вграждане на превенция на щетите за организационната дейност и преследваните цели. Тази рамка е основа за изграждане на ефективна система за УН на ИТП, а с това и на свързаните управленски и технологични операции.

Разграничаването на изброените групи организации позволява по-детайлен анализ на еволюцията на практиките и адресиране на добри стандартни практики за УРН към всяка от тях. Параграфътпредставя характеристиките на стандартите от фамилиите на ISO 27000 и ISO 22000 и възможностите за тяхното приложение.Подчертава универсалното значение на метода „Планиране-Правене-Контрол-Действие“при УРН.

[8]ISO/IEC 27005, Information security risk management.
[9]ISO 22 301:2012Societal Security – Business continuity management system – Requirements.

В Параграф 2.2. се представя предлаган от изследването подход и модел за УРН в публичния сектор и бизнеса. След съпоставяне на приложимите подходи, техните предимства и недостатъци се предлага набор от следните принципи на предлагания подход:

- Интегрирано управление на организационните, информационни и свързани с непрекъсваемостта на ИТП рискове.
- Национално нормативно и международно стандартизирано УРН на ИТП.
- Комплексно за публични и бизнес организации холистично УРН.
- Структурирано и систематизирано процесно УРН.
- Преминаване от функционално към програмно, проектно и ситуационно УРН.
- Съвместно одитиране и планиране на УРН при инциденти, извънредни ситуации, неопределеност на контекста и възстановяване на дейността.
- Количествено определяне на риска и критерии за оценка достигането на целите за непрекъсваемостта на ИТП.
- Съобразяване на промяната на УРН с конкретната организационна култура, вкл. водещо лидерство и персонален интегритет.
- Проактивно и превенционно, обектно-ориентирано УРН.
- Съобразено с последствията за качеството на информационните услуги УРН.

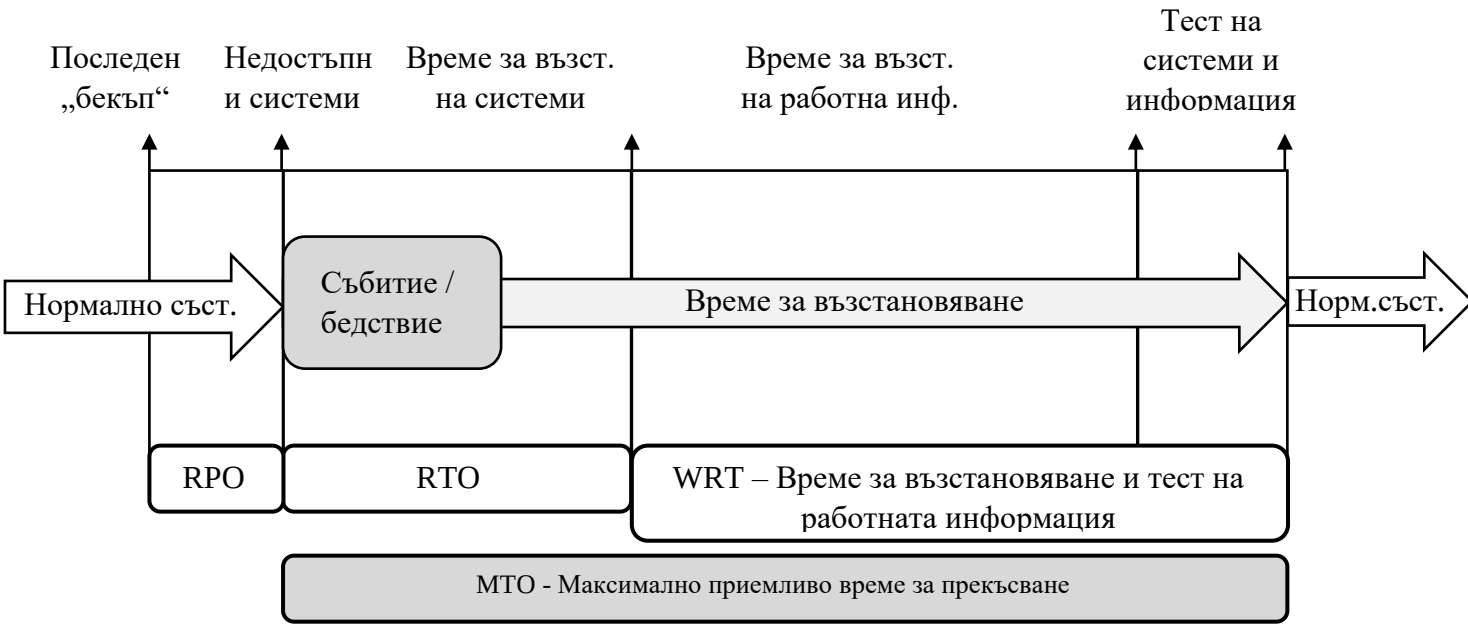
Анализът на бизнес въздействието на прилагания подход позволява дефиниране на ясни критерии и скали за оценка на ефектите от УРН за информационната сигурност на ИТП. Такива критерии са:

- Максимално допустимо време на отказ на достъп (МДО)/MaximumTolerableDowntime (MTD). Определянето на този критерии е предпоставка за определяне на приемлив метод за възстановяване, както и на

изискванията за развитие на обхвата и съдържанието на процедурите за възстановяване.

- Целево време за възстановяване (ЦВВ)/RecoveryTimeObjective (RTO). Този критерии е необходим за избор на приемлива технология за възстановяване, съобразена с МДО/MTD.
- Целева точка за възстановяване (ЦТВ)/RecoveryPointObjective (RPO).Този критерии не е съобразен с МДО/MTD, а отразява приемливото количество на загубени данни по време на възстановителния процес.

Тези критерии са показани на следващата Фиг. 1.



Фиг. 1. Целева точка за възстановяване (RPO) и максимално приемливо време за прекъсване (MTO).

Критериите позволяват да се даде предпочитание и приеме проблемно-ориентиран, интегриран за съвместно УОР, УИР иУН, и международно стандартизиран подход при УРН на ИТП в публичния сектор и бизнеса. Този подход не е само фокусиран върху риска. В него на преден план излизат и са водещи проблемите за непрекъсваемостта на ключовите и критични процеси, които причиняват рисковите въздействия. Идентификацията и въздействието на

риска е предпоставка за дефиниране и опит за предотвратяване на потенциални проблеми за организационната, информационна сигурност и непрекъсваемостта. Изследването на връзката и въздействието на риска върху функционирането на ИС е средство за решаване на проблемите, които произтичат от въздействието върху критериите за непрекъсваемост на ИТП. Одитът, концептуалното проектиране на ИС, планирането на мерките по непрекъсваемостта и прилагането на адекватни инструменти за УРН, вкл. визия, политика, стратегия, организация и опериране е по същество очертаване на проблемно решение на непрекъсваемостта на ИС.

Представеният подход включва приложение на процесен (цикличен) модел за УРН включващ етапи за:

1. *Идентификация на проблем, избор на цел и формулиране на стратегически насоки за нейното постигане.*
2. *Установяване на критерии и построяване на функция и мрежа за оценка на достигането на целта.*
3. *Събиране на информация за средата и възможните алтернативи за решение (събиране на знания, опит, практики).*
4. *Обработка на данни и ограничаване на възможните алтернативи за решение, чрез редуциране до няколко приемливи.*
5. *Оценяване на характеристиките и сравняване на алтернативите с приетата критериална функция и нейната мрежа.*
6. *Избор на предпочитана алтернатива, отговаряща на характеристиката на предпочитанията на вземащите решение.*
7. *Внедряване на решението с помощта на изграден организационен механизъм и оперативни средства за действие.*
8. *Измерване на резултата и при необходимост непрекъснато подобряване чрез коригиране на целта и избраната алтернатива за действие (стратегическите насоки,организационно-тактическия механизъм или конкретните оперативно-технологични инструменти).*

Прилагането на процесния модел позволява подобряване на УРН чрез контрол на стратегическото насочване към целта. Осигурява статистическа информация за преход към култура на оптимизирано УРН.

В Параграф 2.3. се предлага методическа рамка за УРН на ИТП в организациите от публичния сектор и бизнеса. Тази рамка е съобразена с изискванията на Стандарт SL за описание на системи за управление (СУ), реализира аргументирания подход и модел за УРН, и включва: *Обхват на управление; Нормативни препоръки; Термини и определения; Организационен контекст; Лидерство; Програмиране и планиране; Поддръжка; Оперирање; Оценка на работните характеристики и Подобряване.* Тези компоненти са представени синтетично поради техния извънредно голям обем.

1) Обхват на управление – Тази първа клауза от рамката съдържа на първо място описание на обекта на управление и обхвата на приложение. Тя дефинира какъв е преследвания (целеви), а не очаквания изход от прилагане на СУ. Включва определяне на критерия или критериите, с който може да се оценяват резултатите от управлението. В случая на УРН трябва да се определят рисковете, които засягат непрекъсваемостта и времената и точката за възстановяване след прекъсване на дейността (MTD/MTO, RTO, RPO).

2) Нормативни препоръки – Тази клауза определя нормативните изисквания, които следва да се прилагат при управлението. Тези изисквания, могат да произтичат от национални, секторни или международни източници.

3) Термини и определения – Клаузата съдържа използваните термини и определения, които са използвани при описанието на СУРН.

4) *Организационен контекст* – Тази клауза съдържа идентификация на организационния контекст. Включва следните четири стъпки: *4.1) Разбиране на организацията и нейния контекст; 4.2) Разбиране на потребностите и очакванията на заинтересованите страни; 4.3) Определяне на обхвата на СУ; 4.4) Дефиниране на СУ.* Дефинирането наконтекста може да бъде направено преди внедряване на стандартизирана СУ. Основава се на организационната

мисия. Включва определяне на адекватните вътрешни и външни проблеми, които влияят на преследвания резултат (ефект). Дефинира заинтересованите страни, техните изисквания и виждания за обхват на цели и включени задачи. Очертава визия за изграждане, оперирane и подобряване на СУ. Идентифицираният контекст е основа за планирането на дейността, поради което включва идентификацията на риска (ОР и ИР) и техните въздействия върху непрекъсваемостта – последствията от определени събития и свързаната вероятност, с която те се случват. Най-съществен момент е уточняване на стегнат списък на целите – действия (насоките) и преследваните резултати. Това дава вътрешна светлина и яснота за дейността на организацията.

5) *Лидерство* – Клаузата включва три стадия: *5.1) Лидерство и ангажимент; 5.2) Политика; 5.3) Организационни роли, отговорности и пълномощия.* Тази клауза изяснява лидерския аспект на СУРН. Подчертава въвличането на висшия мениджмънт. Гарантира интегриране на изискванията към СУ по отношение на организационните процеси. Дейностите и ключовите процеси са основание за съществуване на организацията. Висшият мениджмънт следва да покаже своя ангажимент за постигане на преследваните резултати, да гарантира адекватни ресурси и да информира всички, че СУ има значение и, че всеки трябва да участва в нейното ефикасно внедряване и подобряване. Въвличането на висшия мениджмънт в СУ е значимо и трябва безусловно да бъде декларирано. Този раздел трябва да подсили и организационната политика, която да включи ангажименти за посрещане на приложими изисквания и непрекъснато подобряване на СУ. Да бъде комуникирана, както в организацията, така и със заинтересованите страни. Трябва да включи подчертаване на стратегическите насоки на организацията, вкл. всичко, което те съдържат.

6) Програмиране и планиране – Включва: *6.1) Действията, насочени към риска и съобразени с възможностите; 6.2) Целите-действия и планиране на тяхното постигане.* Тази клауза прави риска явен. Адресира

противодействията и ги включва в организационната програма или план. Изяснява как да бъдат предотвратени или намалени нежеланите ефекти. Проектира как да бъдат достигнати преследваните резултати (изходи) и постигнато непрекъснато подобрение на СУ чрез програмиране, планиране и координиране на действията. Програмата или планът определя какво, кой, как и кога да бъде направено. Този проактивен подход и предотвратяващи действия намалява необходимостта от поправки и последващи коригиращи мерки. Изисква детайлизирани цели-действия. Те трябва да бъдат съвместими с политиката, измерими (осъществими), наблюдаеми, комуникирани и обновявани като приемливи. Да бъдат адресирани към съответните нива и конкретизирани със задачи. Трябва да изяснят как да се избегнат, елиминират, минимизират или смекчат идентифицираните рискове. При това трябва да се отчита позитивния ефект на възможностите и тяхното подобряване и дори оптимизиране. Съчетанието на рискове и възможности ще води до адекватни политики, стратегии и цели-действия. Програмирането на действията трябва да отчете ефективността на предвидените мерки и да подбере набор от такива, които се включват в разполагаемите ресурси и гарантират постигането на целевите критерии. Без да си поставя такива високи изисквания планирането трябва да очертае ясен път от проблемите и изискванията през риска и възможностите към политиките, стратегиите и целите-действия.

7) Поддръжка – Съдържа:*7.1) Ресурси; 7.2) Компетентности; 7.3) Осведоменост; 7.4) Комуникация; 7.5) Документирана информация (обща, създаване и актуализация, контрол на документираната информация).* Основна задача на клаузата е да осигури поддръжка на постигането на организационните цели. Осведомеността означава всички да знаят последствията от несъответствието на системните изисквания. Комуникацията включва изясняване какво, кога и с кого да се обменя информация във и извън организацията. Изискванията за управление на документацията засягат терминология, документи и записи. Те трябва да отговорят на потребностите на

всеки зает в организацията от работни инструкции, независимо от разполагаемия опита.

8) Оперирane – Включва операционно планиране и контрол на вътрешната и външно възложена (с аутсорсинг) дейност. Контролът изисква уточнени процесни критерии и съпоставяне на процеса с тях. Клаузата съдържа специфичните изисквания за непрекъсваемост и определя конкретния модел на изгражданата СУ и нейните операции.

9) Оценка на характеристиките – Съдържа: *9.1) Мониторинг; Измерване, анализ и оценка; 9.2) Вътрешен одит; 9.3) Преглед на управлението.*Включва проверка на характеристиките. Определя какво, как и кога те да бъдат наблюдавани, измервани, анализирани и оценявани. Съдържа вътрешен одит и преглед на управлението за постигане на очакваните резултати. Показва дали СУ съответства на изискванията и дали стандартът е ефикасно внедрен и поддържан. Прегледът на управлението отговаря на въпроса дали СУ е подходяща, адекватна и ефективна. Одитът установява ползите от изискванията за проверяваните резултати, в съответствие с плана. Това предполага множество от обективни доказателства, които могат да бъдат идентифицирани и потвърдени като измерители, времева рамка, оценки, несъответствия, коригиращи действия, мониторинг и измерване на резултати, одит и изводи от прегледа на управлението.

10) Подобряване – Съдържа: *10.1) Несъответствия и коригиращи мерки* и *10.2) Непрекъснато подобряване.* Клаузата включва установяване на нежелани отклонения и предписване на възстановяващи и коригиращи мерки. Непрекъснатото подобряване отразява отклоненията и подобрява плана за действие.

Тази методическа рамка включва три основни йерархични равнища (контури) на управление.

На стратегическо равнище (основа на управлението) са включени дейностите по определяне на: обхват на управление; нормативни препоръки; термини и определения; организационен контекст и стратегическо лидерство.

На организационно-тактическо равнище (определяне на отговорности) са: организационното лидерство; програмирането и планирането, и поддръжката на системата.

На операционно-инструментално равнище (процеси и операции) са дейностите по: опериране; оценка на работните характеристики, мониторинг, преглед и непрекъснато подобряването.

Съчетаването на тези дейности е основа за конструиране и прилагане на представения модел иметодическа рамка за проектиране на проблемно-ориентирано, интегрирано и стандартизирано УРН, включваща посочените три основни контура за управление.

Изводи от Втора глава:

1. Практиката за УРН на ИТП в организациите от публичния сектор и бизнеса силно варира в зависимост от условията на средата, прилагания подход, модел идостигнатата организационна култура.

2. В зависимост от организационната култура и практика за УРНе възможно да се разграничатчетири вида организации. Първата група, са тези организации, които неглижират УР. При негативна промяна на контекста тези организации са изправени пред провал. Втората, все по-голяма част от организациите приемат динамиката на средата, а с това и ограничен кръг от мерки за УР. Тези организации предприемат действия за УОР и приемат култура на промяната, но рядко УИР и непрекъсваемостта на ИТП. Третата група организации приемат и настройват своята култура и политика в съответствие с международните стандарти за УИР и сигурност, и непрекъсваемостта на ИТП. Те са изправени пред специфични информационни, вкл. киберрискове, които водят до критично прекъсване на протичащите процеси, което налага приемане и поддържане на съответствието на

управлението с международните стандарти за УРН. Четвъртата група приемат съвременните стандарти за количествено дефинирано УРН. Установяват количествени цели и ясни критерии за достигане. Използват статистическа информация за подобряване на политиката и стратегията за УРН.

3. Организациите които пренебрегват и не прилагат съвременно управление на ОР като интегриран процес от принципи, техники и практики за комуникация и консултация, идентификация на контекста, идентификация на риска, анализ, оценка и третиране, както и мониторинг (наблюдение) и преглед на риска следва да променят своята визия, политика и стратегия за да осигурят приемливи граници на риска за достигане на организационните цели.

4. Организациите с по-голям мащаб от втората и третата група, които са застрашени от прекъсване на критични ИТПе препоръчително да възприемат и прилагат проблемно-ориентиран, интегриран и международно стандартизиран подход и процесен моделза УРН на ИТП.

5. Тези организации е необходимо да се придържат към обхвата и съдържанието на предложената адаптирана методическа рамка на Annex SL за одит, концептуално проектиране и описание на основните елементи, компоненти и управленски контури на СУРН.

6. Тези организации следва да одитират своята практика и оценят готовността си за прилагане на стандартите от семействата ISO 27000 и ISO 22000 (ISO 22301) техните развития и стимулират процеса на акредитация по тях. Препоръчително е да прилагат представените методи за УРН и съобразяват отделяните ресурси с очакваните ефекти за непрекъсваемостта на ИТП.

7. Организациите с малък и среден мащаб, които се включват или имат обекти с висока публична значимостотКИ на страната, следва за извършат подготвителна работа като препоръчително използват предложената рамка, включваща контури за стратегическо насочване, организационно-тактическо и оперативно-инструментално управление, като инструмент за вътрешен одит за приложение на ISO 22399.

Трета глава „Апробация на методическата рамка за УРН на ИТП“ включва набор на данни за ИС на организации за публично банкиране и пътно строителство, анализ и интерпретация на резултатите и изводи и предложения за подобряване на рамкатаза одит и концептуално проектиране на СУРН.

В Параграф 3.1. е представен набор на данни за УРН при публично банкиране и пътно строителство, с което се определят условията и задачите на пилотната апробация. Ограничава се изследването на рамката в два казуса, включващи организация за публично банкиране (ББР) и пътно-строителна компания (ТГХ). Представя се контекста, уточняват се организационните цели и критерии за УН, определят се конкретните задачи за предварителен одит и концептуално проектиране на СУРН. Предлагат се одитни анкетни инструменти, съобразени с международната практика. Представят се данни за практиката за УРН на ИТП, получени от анкетно проучване на ограничен кръг експерти.

В Параграф 3.2. се включва анализ и интерпретация на данните за УРН за двете организации. Предлагат се основни констатации за състоянието и концептуално проектиране на трите контура на СУРН. Правят се изводи и конкретни предложения за изпълнение на изисквания към текущата дейност. Идентифицират се портфейли от проекти за развитие на ИС и СУРН за двата казуса. Отделя се специално внимание на решенията за „бекъп“ и архив на използваните данни и тяхното възстановяване за гарантиране на целевата непрекъсваемост на изпълняваните ИТП и предлагани услуги. Параграфа съдържа изводи и препоръки от тестване на рамката за одит и концептуално проектиране на СУРН на ИТП в пилотните организации.

В Параграф 3.3. включва следните изводи и предложения:

Ефективността и ефикасността на администрацията зависят във все по-голяма степен от информационната сигурност на публичния сектор и бизнеса. Промените на националния, институционален и бизнес контекст водят до непрекъснато разширяване на обхвата на традиционните и нови заплахи за сигурността. Все по-често кибер базираните намеси и атаки (WannaCry, Petya,

Sacula и др.) върху ИТП и системи стават не само по-многобройни и разнообразни, но и по уязвяващи и разрушаващи.[10] Това, както и традиционните организационни и ИР са основание за подобряване на практиката за защита на ИТС чрез прилагане на най-добрите практики и международни стандарти за УРН на ИТП.

Прилагането на водещите практики е в състояние да гарантира достигането на организационните цели в публичния сектор и бизнеса и да намали негативните ефекти от нежеланите намеси. Още по-значими ще бъдат тези ефекти в институциите, които зависят силно от ИТС (вкл. от публичния банков сектор и други, които осигуряват КИ на страната) и бизнес организациите, които използват съвременни системи. Отказът или забавянето при използване на стандартизираните практики при прогресиращи рискове ще засегне тези организации по различни вредоносни начини, вкл.:

- Компютърните ресурси могат да бъдат използвани за неоторизирани цели и предприемане на атаки към други компютърни системи.
- Класифицирана информация, например свързана с персонала, интелектуалната собственост, поверителна бизнес информация може да бъде разкрита, прочетена или копирана за престъпни, криминални цели.
- Ключови операции като например тези за поддръжка на КИ, отбраната, вътрешния ред, правораздаването, управление на извънредни ситуации могат да бъдат провалени.
- Съхраняваните конфиденциални данни могат да бъдат допълвани, модифицирани или изтриване с преднамерени, разрушителни и престъпни цели.

Прогресиращите киберзаплахи за информационната сигурност могат да бъдат непреднамерени и преднамерени. Първите включват откази на съоръженията, средата, софтуера, предизвикани от остаряване, изчерпване на ресурси или други обстоятелства, които надвишават очакваните операционни

[10]Information Security, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greeter Adoption of its National Cybersecurity protection System, USGAO, Report to Congressional Committees, GAO Highlights, January 2016, GAO-16-294, INFORMATION SECURITY.

параметри. Те включват още природни бедствия и пропадане на КИ, които са извън контрола на организациите.

Преднамерените или враждебни заплахи могат да бъдат дело на индивидуални, групови, правни и национални субекти, които целят увеличаване на организационната зависимост от киберресурсите (информацията в електронен вид, ИКТ и комуникациите, и способностите за обслужване на данни, осигурявани от тези технологии). Източници на заплаха могат да бъдат корумпирани служители, криминални групи и дори терористи. Тези заплахи зависят от способностите, волята за действие и мотивите, които могат да включват: парична изгода, икономически, политически или военни предимства.

Класификацията на непреднамерените и преднамерени действия сама по себе си е сложна задача, която зависи от конкретните условия на въздействие. Киберзаплахите могат да включват различни стратегии, тактики, техники и практики за въздействие върху хардуера, софтуера, мрежите, да прехващат, крадат или манипулират чувствителна информация.

Редица са примерите за подобни въздействия в публичния и бизнес сектора. Все по-чести и с все по-големи ефекти са тези случаи в банковия и бизнес сектор в страната.

Началното развитие на нормативната уредба със Закона за изменение и допълнение и на консолидирания Закон за електронното управление[11], в частта на глава четвърта, раздел трети за мрежовата и информационна сигурност, включваща само два члена, не е в състояние да даде задоволително решение на възникващите проблеми. Чл. 54 определя, че „административните органи осигуряват мрежова и информационна сигурност”. Следващият раздел за Стандарти и мерки за информационна сигурност, ичл. 55, постановяват, че „Изискванията и стандартите за сигурност, на които трябва да отговарят

[11]Закон за електронното управление, Обн., ДВ, бр.46 от 12.06.2007 г., посл. изм. от 01.07.2014..

информационните системи за въвеждане, изпращане, обработка, достъп, обмен, съхраняване и архивиране на данни, както и общите мерки за сигурност, които трябва да се приемат от административните органи, се определят с наредбата по чл. 43, ал.2. Тази наредба е в проект, както и практическото приложение на приетата национална Стратегия за киберсигурност. Това състояние е основание да се очаква ускорено развитие на нормативната база за раздел сигурност, която по-късно може да бъде развита в самостоятелен закон за информационна сигурност.

Законовата уредба за процедиране с ОР по ЗФУК в публичния сектор изостава от международната практика за подобно управление. Отсъства най-съществената част от интегрирания процес на организационно управление – финансовото планиране. Надграждането на финансовото планиране над управлението и контрола е класическа международна практика. Осъвременяването на тази уредба за променените икономически условия, стартирало през 1996 за контрол, надградено през 2006 за финансово управление е логично да бъде развито с област за финансово планиране. Това надграждане ще даде възможност за развитие на инструментариума за УОР и неговото свързване със спецификата за УИР и УН на ИТП.

Настоящото състояние на нормативната уредба не осигурява ефикасна рамка за гарантиране на ефективността на контрола на ИР и непрекъсваемост в публичния сектор. Ограничената стандартизация в сектора за УОР,ИР и непрекъсваемостта на бизнеса също не допринасят достатъчно за решаване на възникващите проблеми. Това на практика води до развитие на ведомствени инициативи за децентрализирано изграждане, функциониране и развитие на центрове за киберсигурност (МО, МВР, ДАНС), обслужващи секторните политики за сигурност. Несъмнена е необходимостта от изграждане и развитие на Национален интегриран център за управление, мониторинг, отговор на инциденти и фокусна точка за интеграция на усилията срещу кибер и комуникационни инциденти.

Интегрираният център следва да стане основа на национална система за защита на киберсигурността. Тази система трябва да осигури необходимия обхват от способности, вкл. установяване и превенция на намеси, аналитична дейност и предоставяне на информация. Тя следва да разполага с необходимия персонал, базова инфраструктура и съвременна технология за планиране на дейността и опериране, а това означава и с необходимия програмен бюджет. Възможно е тези функции да се делегират на Държавна агенция „Електронно управление“ с последващо развитие на Закон за електронно управление, тъй като в момента агенцията не е предвидено да изпълнява необходимите защитни функции. Още по-перспективно е изграждане в бъдеще на динамична мрежова структура за противодействие.

На практика изградените структури имат ограничени способности да установяват намеси в мрежовия трафик, което предполага в бъдеще възникване на подобни на тази от последните избори атаказа блокиране на сървъра на Централната изборна комисия от типа „отказ на услуга/Denialof Service“. В това отношение Националният институт за стандарти и технологии (NIST) препоръчва използване на комбинация от три методологии за установяване на намеси: „базирани на подпис”, „базирани на аномалии” и „анализ на пълнотата на целта”. Подобно ограничени са и способностите за превенция на намеси при множество от типове мрежови график.

Необходимо е и подобряване на аналитичните способности за: обединяване и корелиране на одитни записи на различни хранилища за по-добра ситуационна ориентация; координиране на информация от нетехнически източници; анализиране на характеристиките на вредоносни кодове и използване на автоматизирани инструменти за анализ в реално време.

Подобряването на обмена на информация е също важно направление за поддръжка на ефективността на информационната системна сигурност. Това може да бъде постигнато с нормативна уредба на операционните процедури при мониторинга, докладването и общия преглед на контролната дейност.

По-сложен и също нерешен въпрос е състоянието на инструментите за измерване (метриката) на ИТ сигурност. Този въпрос засяга, както представянето на изискванията, така и измерването на ИТ характеристики на сигурността. Използването на RTO и RPO може да послужи за база за развитие на индикатори на системната способност за постигане на организационните цели. За такива се препоръчват времеви лимити за установяване на нежелана намеса, за осигуряване на автоматизирано уведомяване, за агрегиране и координиране на намеса след уведомяване.

За ИС и ИТП в публичния сектор и бизнеса е препоръчително утвърждаване на нормативни целеви способности за установяване, превенция, информиране и обмен на информация при вредоносни въздействия.

Особено внимание заслужава и проблематиката за УРН в контекста на защитата на КИ.[12] Изследваните аспекти на този актуален проблем в цитирания източник дават аналитична основа за редица важни изводи и препоръки към защитата на КИ. Предложеният инструментариум за оценка на риска и ефективността на мерките за защита поставят въпроса за интегрирано планиране и оперативно УНна организационната дейност (в публичния и бизнес сектора) в условията на риск при инциденти, извънредни ситуации и неопределеност (кризисно и конфликтно възстановяване).

Мащабен проблем на информационната сигурност на бизнес сектора е съществуващото състояние на организационната култура за вграждане на УР в дейността. Първостепенна задача в това отношение е приемането на принципите и насоките на ИСО БДС 31000:2011, съдържащи внедряване на стандартизирана рамка и процес на УОР. Рамката за УР е ефикасен инструмент за вграждане на риск-базираното управление в организационната култура. Предложеният със стандарта процес на управление включва последователност от процедури за УОР, необходими за последващ преход към УИР и УН на ИТП.

[12]Ботев, Г., Защита на критичната инфраструктура, Академия на МВР, РИО, С., 2013.

В заключението на изследването се подчертава, че настоящата епоха на глобализация и цифровизация на обществения живот дава нови възможности за развитие. Нарастващият капацитет, сложност и уязвимост на електронизираните ИС улесняват администрацията и бизнеса, но създава условия за уязвимост от естествени, непреднамерени и преднамерени зловредни въздействия върху ИТП. Предизвикват се специфични и остри проблеми, засягащи пряко КИ и дейността и живота наголеми обществени групи в страната.

Свързаната с УРН дейност е ключов фактор за гарантиране на надеждност и ефективност на ИТП в публичния сектор и бизнеса,значимостта и актуалността на който нараства със степента на внедряване на съвременни ИТ и ескалация на риска и неопределеността на естествената и киберсреда.

Към момента на настоящото изследване тази дейност не е получила необходимото внимание и предизвиква проблемен дисбаланс и дефицит на средства за ефикасно УРН на ИТП в страната. Тя се развива ограничено в контекста на правителствените инициативи за електронно управление, вкл. при гласуване при избори, както и в рамката на дейността на защитата на КИ и защита на класифицирана информация.

Въпреки установеното изоставане и пречки пред внедряването на СУРН в организациите направените общо и пилотно проучване показват нарастващо осъзнаване на проблема, готовност и предприети начални стъпки в редица от тях за подобряване на УР, информационната сигурност и непрекъсваемост на изпълняваните ИТП.

За да се постигнат организационните цели ръководителите в публичния сектор и бизнеса в страната, които използват ИТС и процеси, особено в КИ следва да предприемат ускорено прилагане на проблемно-ориентиран, интегриран за риска и непрекъсваемостта и международно-стандартизиран подход за УРН. Препоръчително е да се придържат към процесен модел на управление и прилагат предложената методическа рамка за анализ,

концептуално проектиране и представяне на СУРН. Те трябва да се подготвят за ускорена промяна, одит и сертифициране на своята практика за съответствие с международните стандарти от фамилиите за УОР (БДС ISO 31000), УИР (ISO 2700) и УН на ИТП (ISO 22000/22301).

Убедителни основания за това са: тенденцията за нарастване на вероятността от киберрискове; изоставането на развитието на националната политика за информационна сигурност и непрекъсваемост на ИТП; неразвитата нормативна рамка за УР; недостатъчна подготовка на персонала; остаряваща и несвоевременно осъвременявана ИТ база и редица по-частни причини.

Уязвимите организации от публичния сектор и бизнеса следва да изградят визия и приемат политики и стратегии за изграждане на системи за УРН, които обхващат набор от клаузи, препоръчвани от Annex SL включващи: обхват; препоръки; термини и дефиниции; организационен контекст; лидерство; планиране; поддръжка; опериране; оценка на изпълнението и подобряване. Тези организации следва да развият дейности по програмиране и планиране, които обхващат както непрекъсваемостта при експлоатационната дейност, така и при извънредни (бедствия и аварии) и непредвидени катастрофални ситуации.

Особено актуална ще бъде потребността за осъвременяване и международно стандартизиране на политиката за УРН в банковия и ключови бизнес сектори, особено от КИ, при които прекъсването на услугите води до значими щети не само за отделните клиенти, но и за националната икономика.

Опериращите в страната публични и частни банки и бизнес организации следва да създадат надеждно УРН на ИТП и дейността си, за да гарантират опериране при всякакви условия на контекста. Това ще ограничи оперативните, финансовите, правните, за репутацията и други негативни последици, възникващи при прекъсване на дейността.

Изискванията за съвременно стандартизирано УРН на ИТП има още по-съществено значение за организациите от КИ в страната. Голямата уязвимост

на мрежовите подсистеми на КИ е в състояние да парализира националното стопанство и предизвика катастрофални последствия за обществото.

Преходът към нова политика и стратегия за УРН ще протича в условията на силно ограничени ресурси, което налага прилагането на съвременните принципи на одитен анализ на ефектите, програмиране и проектиране на дейностите, съобразено с критериите за ефективност на вземаните решения за непрекъсваемост и възстановяване на данни.

Тези аргументи са основание за разширяване и задълбочаване на изследванията за теорията, методологията, моделите, методите и практиката за УРН на ИТ процесите в публичния сектор и бизнеса в страната. Те дават и убеденост, че активизирането на изследванията на свързаните проблеми е актуално и ако е успешно ще допринесе реално за икономическото и културно благосъстояние на обществото.

IV. ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

1. На базата на ретроспективен анализ, вкл. терминологията, са обобщени основните насоки и подходи за развитие на надеждността и непрекъсваемостта на ИТП и УРН в условията на мрежова комуникация, и нарастваща цифровизация на дейността в публичния сектор и бизнеса.

2. Идентифицирани са основните проблеми на визията, политиката, целевото насочване и стратегията, програмирането, планирането и проектирането на противодействието и приложението в КИ при УРН.

3. Разработена е методология, включващаобосновка за приложение на проблемно-ориентиран, интегриран и международно стандартизиран подход, процесен модел и методическа рамказа одит и концептуално проектиране на СУРН на ИТП.

4. Направено е пилотно емпирично потвърждение на приложимостта на методическата рамка за УРН в условия на публично банкиране и пътно-строителен бизнес.

5. Синтезирани са изводи и са предложени мерки за подобряване на националната практика за УРН на ИТП.

V. ПУБЛИКАЦИИ НА АВТОРА, СВЪРЗАНИ С ДИСЕРТАЦИОННИЯ ТРУД

1. Иванов, Т. К., Н. Т. Иванов, Непрекъсваемост на информационно технологични процеси в обекти от критичната инфраструктура, Академия на МВР, Факултет „Пожарна безопасност и защита на населението “, Седма конференция с международно участие „Гражданска безопасност 2017“, 6 и 7 април 2017.

2.Иванов, Н. Т., Организационни практики за управление на риска в публичния сектор и бизнеса, Институт по металознание, съоръжения и технологичен център по хидро- и аеродинамика „Акад. А. Балевски“ – БАН, Шеста национална конференция с международно участие „Металознание, хидро- и аеродинамика, национална сигурност‘2017“, 29-30 май 2017.

3.Иванов, Н. Т., Планиране при управление на риска и непрекъсваемостта на информационно-технологични процеси, НБУ, Департамент „Национална и международна сигурност“, Международна научна конференция на тема „Европа: Глобални заплахи и интегрирана сигурност. Сигурност в Черноморския регион“, 19 май 2017.

4.Иванов, Н. Т., Кибер рискове и непрекъсваемост на информационно технологични процеси, Военен журнал, бр. 3, 2017 г (в печат).