УТВЪРЖДАВАМ:

ПРЕДСЕДАТЕЛ НА ДКСИ [redacted]

БОРИС ДИМИТРОВ

ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА
Рег. № ВП-40 / 06. 10. 2020
/дата, месец, година/

С Т Р А Т Е Г И Я

ЗА УПРАВЛЕНИЕ НА РИСКА В ДЪРЖАВНАТА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

СОФИЯ, 2020 Г.

*Заличена информация на основание чл. 5, &1, б. "в" от Регламент (ЕС) 2016/679

СЪДЪРЖАНИЕ:

I. СЪЩНОСТ, ЦЕЛИ И ОБХВАТ

Стратегията за управление на риска в Държавната комисия по сигурността на информацията е разработена на основание чл. 4, ал. 1 от Закона за финансовото управление и контрол в публичния сектор и има за цел да подпомогне ръководството и служителите на Комисията в тяхната дейност, свързана с управлението на риска.

Настоящата стратегия за управление на риска във функционално и организационно отношение цели прилагане на единен подход за управление на риска, включващ идентифициране, оценяване и контролиране на потенциални събития, които могат да повлияят негативно върху постигане на целите на Държавната комисия по сигурността на информацията.

Структурна цел на тази стратегия е да посочи изискванията по отношение на същността и съдържанието на докладването на всеки риск (виж т. 5 към параграф IV).

Стратегията е разработена въз основа на:

- Закона за финансовото управление и контрол в публичния сектор/ЗФУКПС/;
- Закона за защита на класифицираната информация;
- Правилника за прилагане на Закона за защита на класифицираната информация;
- Устройствения правилник на Държавната комисия по сигурността на информацията и нейната администрация;
- Основни приоритети за работа на Държавната комисия по сигурността на информацията;
- Указания за управление на риска в организациите от публичния сектор на Министерство на финансите 2020 (ЗМФ № 184/06.03.2020 г.).

Стратегията обхваща периода 2020 г. - 2023 г., като се актуализира на всеки три години, или при настъпване на съществени промени в рисковата среда.

Тя е насочена към създаване на ефективна организация на процеса по управление на рисковете.

С нея се определя методологията, която следва да се прилага, въвежда се системата за докладване, документиране на състоянието на оценените рискове, предприетите мерки за ограничаване или елиминирането на рисковете на приемливо ниво.

Стратегията за управлението на риска обхваща:

- Дефиниции;
- Роли и отговорности;
- Технология за управление на риска (стъпки).

II. Дефиниции

Управление на риска

Дефиниция за управлението на риска се съдържа в чл. 12, (2) на Закона за финансовото управление и контрол в публичния сектор: „Управлението на риска включва идентифициране, оценяване и контролиране на потенциални събития или ситуации, които могат да повлияят негативно върху постигане целите на организацията, и е предназначено да даде разумна увереност, че целите ще бъдат постигнати.", като се доразвива в Методическите насоки по елементите на финансовото управление и контрол: „Управлението на риска включва идентифициране, оценяване и контролиране на потенциални събития или ситуации, които могат да повлияят негативно върху постигане целите на организацията, и е предназначено да даде разумна увереност, че целите ще бъдат постигнати.".

Управлението на риска в ДКСИ е динамичен процес, който следва да осигурява добро разбиране на потенциалните заплахи, действия или събития, които могат положително или отрицателно да повлияят на способността на администрацията да постигне своите цели, както и навременното им идентифициране, предприемане на подходящи действия за управление, наблюдение и докладване.

Риск

Дефиницията за Риск, приета в ДКСИ се съдържа в § 1, т. 5 на Допълнителните разпоредби на Закона за финансово управление и контрол в публичния сектор: „Риск" е събитие, което ще повлияе върху постигане на целите на организацията. Рискът се измерва с неговия ефект и с вероятността от настъпването му.

Вероятност – представлява възможността дадено събитие да се случи;

Ефект (влияние) – представлява описание и оценка последствията/ въздействието от настъпило събитие. Ефектът може да бъде както отрицателен, така и положителен;

Оценка на риска – процес, състоящ се от определяне на степен на вероятност от сбъдването на идентифицирания риск и определяне на степен на влияние (ефект) върху целите на организацията при неговото настъпване;

Риск-апетит – нивото на риска, което организацията е склонна да приеме при изпълнение на своята мисия, без да бъде застрашено постигането на целите.

III. РОЛИ И ОТГОВОРНОСТИ В ПРОЦЕСА ПО УПРАВЛЕНИЕ НА РИСКА

Управлението на риска е интегриран процес в дейността на ДКСИ, в който вземат участие ръководството и всички служители в комисията.

Съгласно чл. 3 ал. 1 и 2 от ЗФУКПС: „(1) Ръководителите на публичните организации отговарят за осъществяване на финансовото управление и контрол във всички ръководени от тях структури, програми, дейности и процеси при спазване на принципите за законосъобразност, добро финансово управление и прозрачност. (2) Ръководителите на всяко ниво в публичните организации отговарят и се отчитат

пред горестоящия ръководител за своята дейност по отношение на финансовото управление и контрол в структурите и звената, които ръководят."

Председател на Комисията - отговорен за управление на риска по смисъла на чл. 2, *чл.7, ал.1, т.2 и ал. 2, чл.10, ал. 1, т.2 и чл. 12* от ЗФУКПС. В тази си дейност той се подпомага от всички членове на комисията, от работната и експертната група, определени със Заповед № 3-292/11.09.2020 г. на Председателя на ДКСИ, както и от служителите на ръководни длъжности.

Председателят ДКСИ отговаря за определяне на мисията, визията и стратегическите цели на организацията. Те трябва да създадат условия за формулиране на ясни, конкретни и измерими цели, осигурени с конкретни по размер и източник ресурси, в съответствие със съществуващите нормативни изисквания и добри практики. Предвид значението на правилното целеполагане за ефективността на Системите за Финансово управление и контрол в този документ се използва понятието Система за Вътрешен контрол (СВК) и в частност – на управлението на риска (описано подробно в Методическите насоки по елементите на финансовото управление и контрол), тези отговорности на Председателя на ДКСИ са ключови за реалното функциониране на управлението на риска;

Председателят на ДКСИ утвърждава Стратегия за управление на риска, която се актуализира периодично (на всеки три години), както и при настъпване на съществени промени в рисковата среда;

Председателят на ДКСИ определя Риск-мениджмънт, както и разпределя отговорностите по управление на риска в средното ниво на ръководството на организацията и служителите;

Отговорност на Председателя на ДКСИ е да одобри риск апетита на организацията, да одобри и да осигури прилагането на реакциите на риска, определени в резултат от управлението на риска, за да се намали влиянието и вероятността от настъпването на тези рискове (реакция на риска) до приемливо ниво (т.е. остатъчния риск);

Отговорност на Председателя на ДКСИ е да осигури предприемане на коригиращи действия на база на информацията от мониторинга на риска.

Заместник-председател, членове на Комисията и главен секретар - отговорни за управлението на риска, в рамките на правомощията си като при необходимост докладват за възникнали случаи на критични рискове.

Звено/лице, отговорно за управлението на риска (риск-мениджмънт)

Ръководителят на организацията определя Риск-мениджмънт (звено/комитет за управление на риска, Риск-ръководител/мениджър или служител по управление на риска). За да разполага с нужната позиция за изпълнение на функциите си, Риск-ръководителят следва да бъде ръководител на високо ниво в организацията и да познава добре структурата и дейността на организацията, нейните стратегически и годишни цели, както и да има познания за същността на процеса по управление на риска.

Риск-мениджмънтът има отговорности по:

1. Създаване на организация за разработване на Стратегията за управление на риска, съответно нейната актуализация;

2. Координиране, организиране и информационно обезпечаване на дейностите по идентифициране и оценка на риска и определяне на реакции на риска;

3. Осигуряване отразяването на рисковете, тяхната оценка и мониторинг, на резултатите от извършените по управление на риска действия, сроковете, в които действията ще бъдат предприети и отговорните лица, в специален документ – риск-регистър, както и да се подсигури неговото редовно актуализиране;

4. Подпомагане ръководството на организацията при определяне на риск-апетита и даване на указания относно приемливите нива на риск;

5. Методологически функции по управление на риска – подпомагане и консултиране „собствениците на риска“ при прилагането на методите и техниките на идентифициране и оценка на риска и при определяне на реакциите на риска;

6. Консултиране, организиране и провеждане на обучения по теми, свързани с управлението на риска.

Работната група по подпомагане на ДКСИ в процеса по управление на целите, съгласно ЗФУКПС, има качеството на звено/лице, отговорно за управлението на риска (риск-мениджмънт) за ДКСИ.

Директори на дирекции, началници на отдели – отговарят в рамките на функционалните си задължения за идентифицирането на рисковете и прилагането на мерките по управлението им. Оценяват установените рискове с помощта на работната група. Наблюдават рисковете в дирекциите и отделите си за състоянието им, както и за напредъка, адекватността и ефективността на прилаганите мерки в изпълнение на плана за действие. Ръководителите на структурните звена (дирекции, отдели) докладват на работната група периодично за състоянието на рисковете, които да се включат в риск-регистъра, или при възникване на кризисна ситуация или промяна във вероятността и влиянието на един или група рискове.

Всеки ръководител на структурно звено в организациите от публичния сектор е „собственик на риска“ по отношение на целите, функциите и дейностите, стоящи за изпълнение пред ръководеното от него звено.

Служителите в Комисията - участват в процеса по управлението на риска и изпълняват плановете за действие като прилагат определени контролни процедури в процеса по управлението на риска. Докладват за идентифицирани рискове на прекия си ръководител и управляват рисковете в рамките на своите задължения.

Отговорностите на служителите са:

1. Да подпомагат оперативните ръководители в процеса на управление на риска, като осигуряват нужната за целта информация и участват активно в дейностите по оценка на идентифицираните рискове и въведените контролни процедури;

2. Да докладват на оперативното ръководство за възникващи проблеми, които могат да застрашат постигането на целите;

3. Да докладват на оперативното ръководство за потенциални възможности за подобрение на СВК.

Вътрешен одитор - подпомага въвеждането на процеса по управление на риска и предоставя независимо мнение по отношение на адекватността и ефективността на управлението на риска. При планирането на одитните ангажименти за годината взема предвид резултатите от управлението на риска. Вътрешният одит задължително трябва да оценява ефективността и да допринася за подобряването на процесите на управление на риска. Когато подпомагат ръководството при изграждането или подобряването на процесите по управление на риска, вътрешните одитори задължително трябва да не поемат управленска отговорност за практическото управление на рискове. В този смисъл отговорността на вътрешния одит е да предоставя обективно мнение по отношение на управлението на риска чрез извършване на одитни ангажименти при спазване на приложимата нормативна рамка и стандарти.

IV. СИСТЕМА ЗА УПРАВЛЕНИЕ НА РИСКА (СТЪПКИ)

1. Създаване на условия за управление на риска

Система за управление на риска е механизъм за вземане на решения, подпомагащ Комисията за постигане на целите й и чрез който ресурсите й се разпределят така, че да се получи оптимално третиране на риска.

Основните цели на процеса по управление на риска са:

- своевременно откриване и противодействие на значимите за Комисията рискове;
- разпределение на ресурсите (човешки, финансови, информационни), съобразно степента и значимостта на различните рискове;
- своевременни промени в политиката за управление на риска въз основа на оценката на ефективността на процеса.

1.1 Описание на процеса по управлението на риска

Процесът по управление на риска може да бъде представен със следния модел:
СТРАТЕГИЯ
ИДЕНТИФИЦИРАНЕ И ОЦЕНКА НА РИСКА
ОПРЕДЕЛЯНЕ НА РИСК АПЕТИТА
РЕАКЦИЯ НА РИСКА
МОНИТОРИНГ НА РИСКА

1.2 Документиране на процеса по управление на риска

Необходимо е всяка дейност, свързана с управлението на риска да бъде документирана. Чрез документиране на всеки етап от процеса по управление на риска, както и избора на подходяща реакция или действие на служителите, които отговарят за тези действия в определени срокове, се създават условия за редовен и

систематичен преглед на процеса. Риск-регистърът е документ, в който се отразяват резултатите от управлението на риска. Той съдържа следната информация:

- Идентифицираните рискове за дейността на ДКСИ;
- Оценка на вероятността и влиянието на идентифицираните рискове при липса на контролни дейности;
- Предприетите действия и текущи контролни дейности;
- Нивото на риска след предприемане на действия, въвеждане на контролни дейности/остатъчен риск/;
- Оценка на нивото на остатъчния риск спрямо апетита към риска
- Предложени /планирани действия за намаляване на остатъчния риск;
- Срокове и отговорни длъжностни лица за изпълнение на мерките.

2. Идентифициране и оценка на риска

2.1 Идентифициране на риска - това е първият етап от процеса по управление на риска, при който се откриват рисковете, които биха могли да повлияят негативно върху изпълнението на целите на ДКСИ. От съществено значение при идентифицирането на рисковете е:

- тяхното възможно по-пълно откриване, тъй като съществува голяма вероятност рисковете, които не са идентифицирани в тази фаза, да не бъдат открити никога;
- моментът на идентифициране на рисковете, тъй като колкото по-рано е открит един риск, толкова по-успешно ще бъде неговото противодействие.

2.1.1 Дейности по идентифициране на рисковете

Текущо идентифициране – всеки служител, който счита, че е идентифицирал нов риск или промяна във вероятността или влиянието на съществуващ риск, трябва да информира директора на дирекцията, в която работи. Директорът преценява дали да информира Риск-ръководителя.

Периодично идентифициране – създадена е постоянно действаща работна и експертна група за подпомагане на ДКСИ в процеса по определянето на целите на ДКСИ, съгласно Закона за управление и контрол в публичния сектор.

2.1.2 Анализ на целите - целите на Комисията играят съществена роля в цялостния процес по управление на риска. Те служат като отправна точка при идентифицирането на рисковете, техния анализ, приоритизиране и противодействие. Всяко решение, което се взема в рамките на процеса по управление на риска следва да бъде обвързано с крайния резултат, към който се стреми Комисията.

Следователно, процесът по управление на риска ще бъде насочен към осигуряване на благоприятни условия за постигане на стратегическите цели/основни приоритети/ на Комисията:

1. Защита на класифицираната информация от нерегламентиран достъп.
2. Усъвършенстване, развитие, координация и общ контрол на системата за защита на класифицираната информация по персонална, документална, физическа, индустриална сигурност, сигурност на КИС и криптографска сигурност.
3. Усъвършенстване на системата за обучение по защита на класифицирана информация с цел изграждане на съзнание за сигурност сред лицата, ангажирани по ЗЗКИ.

4. Подобряване на институционалния и административен капацитет на ДКСИ за успешно изпълнение на мисията и функциите.

Всяка една промяна на стратегическите цели/основни приоритети на ДКСИ ще се отрази на дейността по управление на риска.

2.1.3 Класификация на рисковете - оперативната среда, в която работи администрацията е рамката, в която следва да се прилага управлението на риска. Тя се състои от външни и вътрешни за Комисията рискове, които влияят на дейността ѝ.

Външни рискове са: съществуващата нормативна уредба; общественото мнение; икономическите условия в страната; финансирането от държавния бюджет и наличието на бюджетни ограничения.

Вътрешни рискове са: организацията на оперативните дейности в администрацията на Комисията; наличните ресурси; разполагаемите финансово-счетоводна функция и тези на IT-системите; вътрешно преструктуриране на дейности, международни дейности и изяви и др.

Критични рискове – рискове, при които влиянието и вероятността са високи и изискват незабавно и подробно разглеждане на дейностите, свързани с управление на риска;

Рискове с високо влияние и ниска до средна вероятност. Тези рискове трябва да бъдат контролирани веднага след като се вземат мерки по отношение на критичните рискове, тъй като въздействието им може да бъде значително, въпреки че вероятността да се случат е по-малка отколкото при критичните рискове;

Рискове с висока вероятност и сравнително ниско влияние са такива рискове обикновено не се взимат предпазни мерки. По-скоро трябва да се има предвид и да се следи ефектът на натрупването, който може да повиши ефекта (например поредица от малки проблеми, които придобиват голямо влияние при натрупване или системно нарушение);

Неотносими рискове: Тук се отнасят рисковете, при които и двата фактора – вероятност и влияние, са ниски. Те трябва да бъдат наблюдавани, но не изискват мерки. Третирането им зависи от наличните ресурси и от изискванията на заинтересованите страни.

Категоризацията на рисковите области за ДКСИ е представена в Приложение № 1, неразделна част от самата стратегия.

2.3 Оценка на рисковете - При този етап ще бъдат изследвани вероятността от настъпване, честотата, последиците и причините за възникване на конкретните рискове. Извършва се оценка на идентифицираните рискове - от гледна точка на **вероятност и въздействие.** Оценката се прави по три степенна скала от 1 до 3:

1 – нисък риск
2 – среден риск
3 – висок риск

Рейтингът на риска се изчислява по следната формула:
P x S = V

Където: P - вероятност от настъпването на събитието;
S - значимост на събитието - въздействие;
V - рейтинг на риска

След направената оценка се изготвя Регистър на идентифицираните рискове в Комисията /риск-регистър/, имащи отношение към конкретните цели.

Подходът за оценка на риска в ДКСИ е представен в Приложение № 2, неразделна част от самата стратегия.

3. Определяне на риск-апетита

Риск-апетитът на ДКСИ се дефинира като „Риск, който ДКСИ е готова да поеме при осъществяване на нейната дейност, за да бъде в съответствие със стратегическите и оперативните си цели".

В хода на този етап от процеса се сравняват честотата, вероятността и последиците от риска с очакваните разходи за Комисията по неговото противодействие. Така отделните рискове ще се подредят по приоритет, като ще се определят тези от тях, които задължително следва да бъдат третирани в Комисията, както и начините/подходите за тяхното противодействие. Определя се областта, в която попадат оценените рискове - зона с висок приоритет, зона за наблюдение и зона с нисък приоритет.

Спрямо рисковете, попадащи в зоната с висок приоритет задължително се предприемат мерки, чрез изготвяне на план за действие и се определят срокове и отговорни лица.

Рисковете от зоната за наблюдение се следят периодично и се анализират механизмите и действията, чрез които тези рискове ще се поддържат в рамките на приемливото ниво.

Рисковете с нисък приоритет се преглеждат поне веднъж годишно и се анализира вероятността и влиянието, което биха имали при промени във вътрешните и външните фактори. Възможно е в хода на приоритизирането, някои рискове да отпаднат и за тях ДКСИ да не предприеме никакви последващи действия.

4. Реакция на риска

След като рисковете са идентифицирани, анализирани и оценени, ще бъдат предприети избраните адекватни мерки за противодействие в подходящ времеви момент. Мерките или така наречената реакция на риска може да бъде:

- **Толериране на риска** - приемане на риска на нивото, на което е оценен. Такава реакция е възможна само, ако оценката на остатъчния риск е в рамките на приемливо ниво, или са налице ограничени възможности за предприемане на ефективни действия;

- **Ограничаване на риска /третиране/** - въвеждане на контролни дейности, с цел ограничаване на въздействието и/или вероятността от настъпването му. По-голяма част от рисковете попадат в тази категория. Целта на това действие не е непременно да се елиминира даден риск, а по-скоро да се вземат мерки, чрез които да се ограничи риска до приемливо ниво;

- **Прехвърляне на риска** - в случай, че рискът е неприемливо висок, може да се търси възможност за прехвърлянето му или споделянето му с друга организация. Основните начини за прехвърляне на риска са застраховането, сключването на партньорски споразумения и осигуряването на определени дейности като външна услуга;

- **Приемане на риска** - приемане на риска на нивото, на което е оценен. Такава реакция е възможна само, ако оценката на остатъчния риск е в рамките на приемливо ниво, или са налице ограничени възможности за предприемане на ефективни действия;

- **Прекратяване** - намаляване и/или ограничаване на вероятността и/или влиянието на риска чрез прекратяване на дейността, която го поражда;

- **Планове за действие при непредвидени обстоятелства** - Всеки един от рисковете може внезапно да се прояви и да създаде кризисна ситуация, дори тези, които са оценени с ниска вероятност/влияние. Това може да се дължи на неправилна оценка, промени в обстоятелствата или външни събития. Планове за действие при непредвидени обстоятелства се прилагат спрямо всички рискове, които могат да имат критично или катастрофално влияние за комисията.

5. Мониторинг и докладване на процеса по управление на риска

Осигуряване на ефективност на процеса по управление на рисковете налага текущо наблюдение (мониторинг) на всеки етап и периодично докладване на идентифицираните рискове и предприетите действия за тяхното намаляване (реакции). Наблюдението на рисковия профил дава разумна увереност на ръководството на ДКСИ, че процесът по управлението на риска е адекватен и ефективен и предприетите действия са довели до намаляване на идентифицираните рискове до приемливо ниво. За осъществяване на систематичното наблюдение Председателят на Комисията и работната група следва да преглеждат поне веднъж годишно целия риск-регистър. При възникване на внезапни събития риск-регистърът може да бъде разгледан извънредно.

Рисковете, определени като „значителни“ според Приложение 2, т. 3 и т. 4, при идентифициране от служители и ръководители в ДКСИ, се докладват на Риск-мениджъра и/или Работната група по подпомагане на ДКСИ в процеса по управление на целите, съгласно ЗФУКПС, незабавно чрез директора на съответната дирекция на ДКСИ. Изисквания към доклада на рисковете са:

- Ясно описание на риска, включително на контекста на риска;
- Целта, над чието постигане влияе;
- Оценката на влиянието, вероятността, стойността на риска, рейтинга и на остатъчния размер на риска;
- Съществуващи варианти за реакция на риска;
- Предложената стратегия за намаляване на остатъчния риск с допълнителни действия/контроли;
- Собственик на риска (дирекция, отдел, сектор).

Инициативата за мониторинг и докладване на риска е на звеното/лицето, отговорно за управлението на риска (риск-мениджмънт). Мониторингът се осъществява със съдействието на ръководителите от всички нива в ДКСИ.

За всички срещи, проведени във връзка с прегледа и актуализирането на риск-регистъра се изготвя протокол, в който се отразяват взетите решения.

Председателят на комисията, чиято отговорност е процесът по управление на риска, одобрява попълнения риск-регистър.

Неразделна част от стратегията са:
Приложение № 1 - Категоризация на рисковите области
Приложение № 2 - Подход за оценка на риска
Приложение № 3 - Риск-регистър

Стратегията за управление на риска в Държавната комисия по сигурността на информацията се приема с Решение на Комисията и може да бъде актуализирана при възникване на нови обстоятелства.

Приложение № 1

КАТЕГОРИЗАЦИЯ НА РИСКОВИТЕ ОБЛАСТИ ЗА ДЪРЖАВНАТА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

- **Стратегически рискове** - Промяна на поставените цели. Ограничаване на планираните дейности, функции и задачи на ДКСИ.
- **Оперативни рискове** - Ежедневни трудности по изпълнение на оперативните процеси и дейности. Текучество и непопълнен щат на администрацията, липса на подготвени и обучени служители за изпълнение на целите, задачите и дейностите, както и допускане на грешки, поради голяма натовареност.
- **Политически рискове** - Промени в Правителството могат да доведат до промяна на нормативната уредба, която от своя страна може да предизвика промяна на изискванията за извършване на дадени дейности.
- **Икономически и финансови рискове** - Необезпечаване с необходимите бюджетни средства. Несъобразяване на планираните бюджетни средства по размери и периоди /тригодишен, годишен, тримесечен, месечен/ с вида дейности. Липса на актуализирана счетоводна политика, индивидуален сметкоплан и вътрешно нормативни документи. Липса на актуализирани вътрешни правила и процедури за одит.
- **Рискове за репутацията** - Некоректно отразяване на дейността на Комисията от медиите, неспособност на служителите
да предоставят качествени услуги на потребителите.
- **Технологични рискове** - Използване на технологии водещи до пробив в информационните системи и системите за сигурност и охрана. Използването на нови информационни системи и системите за сигурност и охрана.
- **Рискове за сигурността** - Срив в КИС, загуба, подправяне или неподходящо управление на данни, както и осъществяване на нерегламентиран достъп.

злоупотреба, умишлено или зловредно /неумишлено/ въздействие върху физическата сигурност на документалната информационна база /регистри на хартиен носител или материални носители на многократен запис/. Кражби или злоупотреби с материални активи или парични средства.

- **Правни /регулаторни рискове** - Промяна на националното или законодателствата на страните от НАТО и ЕС, което от своя страна може да доведе до промяна на изискванията за извършване на дадени дейности.

- **Управленски рискове** - Неспособност на ръководството и персонала за прилагане на нормативните актове и вътрешните правила, както и незадоволителен вътрешен контрол.

- **Договорни или партньорски рискове** - Неуспешно изпълнение на сключени договори за услуги и доставки.

- **Екологични и здравни рискове** – възникващи в резултат на въвеждането на нови екологични стандарти или поради настъпили екологични катастрофи, промени в климата, пандемии и др.

Приложение № 2

ПОДХОД ЗА ОЦЕНКА НА РИСКА В ДЪРЖАВНАТА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

При оценката на всеки риск ще се прилага единен и последователен подход - двуизмерна скала на която се отразяват вероятността от настъпването им и тяхното влияние.

1. За всеки от рисковете се оценява **потенциалното влияние** върху изпълнението на дейността, надеждността на финансовата и оперативната информация в съответствие със законодателството и вътрешните нормативни актове. Използва се скала с три степени на влияние - **ниско, средно и високо.**

2. За всеки от рисковете се оценява **вероятността** за неговото проявление. Използва се скала с три степени на вероятност - **ниска, средна и висока.**

3. При оценяване на влиянието и вероятността, рисковете, оценени като **високи/високи, високи/средни или високи/ниски** ще се приемат като **значителни рискове.** Те ще се управляват активно чрез предприемане на действия за намаляването им.

4. Рисковете, оценени като **средни/средни, ниски /високи или средни /високи** ще се приемат като **значителни рискове.** Те ще се наблюдават, като се прилагат действия за контролирането им или за предотвратяване преминаването им в по-висока категория. По преценка на Председателя на ДКСИ могат да се категоризират като съществени и рисковете, които са високи/ниски и ниски/високи.

5. Рисковете оценени като **ниски/ниски, ниски/средни или средни/ниски** ще се наблюдават като се контролира, разходите да не надвишават ползата от намалението на риска.

УТВЪРЖДАВАМ
ПРЕДСЕДАТЕЛ НА ДКСИ:
.....
БОРИС ДИМИТРОВ
.....12.12. 2021 г.

ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА
Рег. № КОМ-ВП-40/06.01.2020 / 20.12.2021
/дата, месец, година/

РИСК-РЕГИСТЪР
НА ДЪРЖАВНАТА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Риск	Оценка на присъщия риск		Предприети действия	Оценка на остатъчния риск		Допълнителни действия	Срок, до който допълните лните действия следва да бъдат предприети	Отговорен служител за пред-приемане на допълни-телните действия
	Влияние	Вероятност		Влияние	Вероятност			
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Цел: **Защита на класифицираната информация от нерегламентиран достъп.**								
1. Промени в нормативната уредба, които могат да доведат до ограничаване/разширяване или значително изменение на	високо	средна	Участие на Комисията и експерти в обсъжданията на промени и допълнения					

*Заличена информация на основание чл. 5, &1, б. "в" от Регламент (ЕС) 2016/679

планираните цели и задачи.			в нормативната уредба по ЗЗКИ и ППЗКИ.					
2. Пропуски в обучението и подготовката на експертния състав, пораждащи затруднения в прилагането на нормативните разпоредби и технологичните изисквания в областта на сигурността на КИС в ОЕ, вкл. ОЕ ДКСИ.	високо	висока	Провеждане на тематични обучения на органи по сигурността на КИС в организационните единици. Активно участие в междуведомствената работна група по промени в ЗЗКИ, НСКИС, НКСКИ.					
3. Пропуски в прилаганите мерки и контрол на преноса на класифицирана информация на НАТО и ЕС по КИС в ОЕ, вкл. ОЕ ДКСИ.	средно	средна	Извършване на периодични дейности по акредитиране на КИС на ДКСИ. Извършване на дейности по акредитиране и преакредитиране на КИС за работа с чуждестранна КИ, КИ на НАТО и ЕС и точки на присъствие на КИС на НАТО и ЕС.					
4. Технически сривове, водещи до нежелана загуба или промяна на информацията и на режима на достъп в електронните регистри.	средно	средна	Поддържане и усъвършенстване на електронните регистри					
5. Недостатъчно финансиране от държавния бюджет на бюджета на ДКСИ, което да се	високо	средна	Аргументиране на нуждата от допълнително					

отрази негативно върху изпълнението на целите и функциите на комисията			финансиране на бюджета на ДКСИ пред Министерство на финансите, Министерския съвет и Народното събрание.					
Цел: Усъвършенстване, развитие, координация и общ контрол на системата за защита на класифицираната информация по персонална, документална, физическа, индустриална сигурност, сигурност на КИС и криптографска сигурност.								
1. Пропуски в анализа, оценката, подготовката и реализирането на промени в нормативната уредба, водещи до компрометиране на устойчивостта и надеждността на Националната система за защита на класифицираната информация (НСЗКИ).	високо	средна	Актуализиране на нормативната база въз основа на задълбочен анализ, обоснована оценка, адекватна подготовка и реализиране на необходимите мерки за защита на класифицираната информация.					
2. Пропуски в контрола, координацията и взаимодействието между проучващите органи от НСЗКИ.	високо	средна	Задълбочаване на контрола, координацията и взаимодействието между проучващите органи от НСЗКИ.					
3. Пропуски в координацията и взаимодействието между ОЕ от НСЗКИ.	високо	средна	Разширяване на обхвата и повишаване на контрола при координацията и взаимодействието между ОЕ от НСЗКИ.					
4. Технически сривове,	високо	средна	Изготвяне и контрол					

водещи до нежелана загуба или промяна на информацията, на режима на достъп и на управлението и контрола на работата с класифицирана информация в КИС.			при спазването на вътрешни правила и процедури за сигурност на КИС и мрежи на ДКСИ. Първоначално и периодично обучение на потребителите на КИС и мрежи на ДКСИ за класифицирана информация по процедурите за сигурност.					
5. Неизградени системи за видеонаблюдение в помещенията на териториалните структури на ДСКС: - КП - Русе. Възможни сривове при поддръжката на системите за сигурност	средно	средна	Планиране, изграждане и въвеждане в експлоатация и поддържане на системи за сигурност – видеонаблюдение в териториални структури на ДСКС.					
6. Морално остарели системи за контрол на физическия достъп в зоните за сигурност на териториалните структури на ДСКС – КП – Благоевград, Кюстендил, Враца, Монтана, Русе, Плевен, Добрич, Бургас, Ямбол, Стара Загора, Кърджали, Пловдив, Смолян, Пазарджик	средно	средна	Изграждане, въвеждане в експлоатация и поддържане на надеждни, съвременни системи за контрол на физическия достъп в териториални структури на ДСКС.					

Цел: Усъвършенстване на системата за обучение по защита на класифицираната информация с цел изграждане на съзнание за сигурност.								
1. Пропуски в обучението и подготовката на служителите от ОЕ за практическо прилагане на разпоредбите на ЗЗКИ и подзаконовите актове по прилагането му.	средно	средна	Организиране на обучения по изучаване и практическо прилагане на разпоредбите на нормативните актове в областта на защитата на класифицираната информация.					
2. Пропуски в обучението и подготовката на РОЕ и ССИ за управлението и контрола на работата с класифицирана информация в ОЕ.	средно	средна	Задълбочаване на общия и прекия контрол по изпълнение на задълженията на РОЕ и ССИ по прилагане на принципите и мерките за защита на класифицираната информация.					
3. Пропуски в обучението и подготовката на експерти от ДКСИ и ССИ в ОЕ с оглед провеждане на ефективно обучение за работа с класифицирана информация и изграждане на съзнание за сигурност.	високо	средна	Поддържане на високо ниво на квалификация на експертите на ДКСИ и ССИ в ОЕ чрез непрекъснато запознаване и обучение относно промените в нормативната уредба и средата за сигурност.					
Цел: Подобряване на институционалния и административен капацитет на ДКСИ за успешно изпълнение на мисията и функциите.								

1. Предизвикателствата на променената работна среда и дигитализацията на процесите пораждат необходимостта от иновативно организационно поведение на ръководния, експертния и техническия персонал.	високо	средна	Създаване на благоприятна работна среда и изграждане на позитивно отношение към промените. Анализ на степента на дигитализацията на работните места и преценка за съответствие с експертизата на всеки служител.					
2. Текучество на кадри поради ниско заплащане на труда на служителите от администрацията на ДКСИ, назначени по ЗДСл и КТ, и невъзможност за конкуриране заплащането в комисията с други държавни структури	високо	средна	Мотивиране необходимостта от допълнително финансиране от държавния бюджет за привеждане заплатите на служителите от администрацията на конкурентно ниво спрямо заплащането в други държавни структури с цел назначаване и задържане на квалифицирани кадри					
3. Текучество на кадри и недоокомплектоване на персонала на дирекция „Специална куриерска служба" (ДСКС) поради ниско заплащане на труда на	високо	средна	Мотивиране необходимостта от допълнително финансиране от държавния бюджет за осигуряване на					

служителите, назначени по ЗМВР, и невъзможност за конкуриране заплащането в комисията със заплащането в МВР и други структури, чиито служители са назначени по ЗМВР			финансов ресурс за цялостно попълване щата на ДСКС и привеждане заплатите на служителите от дирекцията на конкурентно ниво спрямо заплащането в МВР и други държавни структури с цел назначаване и задържане на квалифицирани кадри					
4. Несвоевременна или липса на адаптация от служителите към условията на променената работна среда и динамичното изменение на длъжностните изисквания.	високо	средна	Анализ, планиране и провеждане на обучения за поддържане на достигнатото ниво на експертиза и непрекъсната актуализация на знанията и уменията, включително дигиталните.					
5. Нецелесъобразно изразходване на бюджетни средства.	високо	средна	Прецизно изразходване на бюджетните средства, съобразно реалните потребности, при спазване на принципите за законосъобразност, ефективност, ефикасност и икономичност.					

			Утвърдени Счетоводна политика и Вътрешни правила за осъществяване на предварителен контрол в ДКСИ. Анализ на разходите и предложения за реализиране на икономии.					
6. Несъответствие на дейностите със законодателството, вътрешните актове и договорите.	високо	средна	Мониторинг *Стриктно изпълнение на:* Правила за вътрешния одит в ДКСИ. Стратегически план за дейността на звеното за вътрешен одит за периода 2021 - 2024 г. и Годишен план за дейността на звеното за вътрешен одит. Осъществяване на всички планирани одитни ангажименти. Изпълнение на дадените и приети препоръки.					
7. Пропуски и грешки при планиране, организиране и провеждане на обществените	високо	средна	*Стриктно изпълнение на:* Вътрешни правила за					

поръчки.			реда и организацията за възлагане на обществени поръчки, които регламентират процеса на планиране, организиране и провеждане на обществените поръчки, задълженията и отговорностите на участниците по подготовката и провеждането на обществени поръчки. План-график за изпълнение на дейностите по възлагане на обществени поръчки в ДКСИ. Съгласуване на дей-ствията между звената, отговорни за провеждането на процедурите. Обучение на служи-телите, отговарящи за провеждането на ОП.					
8. Пропуски в мониторинга/ контрола по изпълнение на сключените договори.	средно	средна	*Спазване на:* Вътрешни правила за реда и организацията за възлагане на обществени поръчки в ДКСИ.					

			Регистър на сключените договори, който да се актуализира своевременно.					
9. Нанасяне на щети върху държавната собственост, предоставена в управление на ДКСИ.	високо	средна	Изпълнение на Вътрешни правила и заповеди, определящи реда за ползване, опазване и поддържане на материалните активи на комисията. Ежедневен мониторинг на състоянието на сградите, оборудването, обзавеждането, уредбите, съоръженията, инсталациите и системите на техническата инфраструктура в имотите. Осигуряване на физическа охрана на имотите и ефективен пропускателен режим. Застраховане на сгради и автомобили.					
10. Амортизация на автопарка на ДКСИ и необходимост от подмяна на служебните автомобили.	високо	висока	Стриктно спазване на правила за ремонт и поддръжка на автомобилите,					

			планиране на действия за подмяна на автопарка.					
11. Пожар, наводнения и други природни бедствия и/или терористични действия, които могат да повлияят върху работата на ДКСИ и да нанесат физически вреди на материалната база.	високо	средна	Планирана обществена поръчка с предмет „Изграждане и въвеждане в експлоатация на системи за сигурност – видеонаблюдение в КП - Русе. Спазване на графика за обществени поръчки в ДКСИ и за сключване на договори през 2022 г. Застраховане на хора и имущество. Дейности за повишаване на мерките за сигурност.					
12. Риск от нови биологични агенти, причиняващи епидемични или пандемични заболявания от типа на Ковид-19, с потенциал за нарушаване на работната среда и изпълнението на служебни ангажименти	средно	висока	Разработен план за действие за предотвратяване на заразяване на работещите от COVID-19. Почистване и дезинфекциране на работни места и коридори. Хигиена на ръцете – диспенсъри и дезинфектанти на видими места, сапуни, кърпи за еднократна употреба. Носене на маски, проветряване.					

			Съобразяване с национ-налните политики в тази сфера, разпоре-дени от МЗ, РЗИ, Националния център по заразни и паразитни болести.					

Забележка: Риск-регистърът съдържа средни и високи рискове, но не и ниски такива, на основание Насоки за въвеждане на управление на риска в организациите от публичния сектор, утвърдени от Министерството на финансите.

Изготвили: 1. Проф. д-р Иво Великов - председател на работна група по заповед № 3-378/26.11.2021 г.....

2. Изидора Петкова - директор на дирекция „ФСДУС” .....

3. Нина Зарева - директор на дирекция „Канцелария” .....

4. Добромир Анев - директор на дирекция „ЗКИ” .....

5. Георги Панов - директор на дирекция „ИФС” .....

6. Венцислав Димитров - директор на дирекция „Сигурност” .....

7. Антон Борисов - директор на дирекция „ПМД” .....

8. Стоян Вълков - ВПД директор на дирекция „СКС” .....

9. Магделена Стоянова - директор на дирекция „ДЧРУМД“ .....

*Заличена информация на основание чл. 5, &1, б. "в" от Регламент (ЕС) 2016/679