РЕШЕНИЯ

РЕШЕНИЕ (ЕС, Евратом) 2017/46 НА КОМИСИЯТА

от 10 януари 2017 година

относно сигурността на комуникационните и информационните системи в Европейската комисия

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 249 от него,

като взе предвид Договора за създаване на Европейската общност за атомна енергия,

като има предвид, че:

(1) Комуникационните и информационните системи на Комисията представляват неразделна част от функционирането на Комисията и инцидентите, свързани с информационната сигурност, могат да окажат сериозно въздействие върху операциите както на Комисията, така и на трети страни, включително физически лица, стопански субекти и държави членки.

(2) Съществуват редица заплахи, които могат да навредят на поверителността, целостта и наличността на комуникационните и информационните системи на Комисията, и на обработваната в тях информация. Тези инциденти включват аварии, грешки, умишлени атаки и природни събития, като те трябва да бъдат разпознавани като оперативни рискове.

(3) Комуникационните и информационните системи (КИС) трябва да разполагат с ниво на защита, съответстващо на вероятността, въздействието и характера на рисковете, на които те са изложени.

(4) Информационната сигурност в Комисията следва гарантира, че КИС на Комисията осигуряват защита на обработваната с тях информация и функционират както трябва и когато трябва, под контрола на легитимни потребители.

(5) Политиката за информационна сигурност на Комисията следва да бъде прилагана по начин, който съответства на политиките за сигурност в Комисията.

(6) Дирекция „Сигурност“ към Генерална дирекция „Човешки ресурси и сигурност“ носи общата отговорност за сигурността в Комисията под ръководството и отговорността на члена на Комисията, който отговаря за сигурността.

(7) Подходът на Комисията следва да отчита политическите инициативи и законодателството на ЕС по отношение на мрежовата и информационната сигурност, отрасловите стандарти и добри практики, да съответства на приложимото законодателство и да създава условия за оперативно взаимодействие и съвместимост.

(8) Службите на Комисията, които отговарят за комуникационните и информационните системи, следва да разработват и прилагат подходящи мерки, като мерките за информационна сигурност, предназначени за защитата на комуникационните и информационните системи, следва да бъдат координирани във всички звена на Комисията, за да се осигури ефикасност и ефективност.

(9) Правилата и процедурите за достъп до информация в контекста на информационната сигурност, включително управлението на инциденти, свързани с информационната сигурност, следва да бъдат пропорционални на заплахата за Комисията и за нейните служители, да съответстват на принципите, установени в Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета ([1]) относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Съюза и за свободното движение на такива данни, и да са съобразени с принципа на професионалната тайна, предвиден в член 339 от ДФЕС.

([1]) Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1).

(10) Политиките и правилата за комуникационните и информационните системи, които обработват класифицирана информация на ЕС (КИЕС), чувствителна некласифицирана информация и некласифицирана информация, трябва изцяло да съответстват на решения (ЕС, Евратом) 2015/443 ([1]) и (ЕС, Евратом) 2015/444 ([2]) на Комисията.

(11) Необходимо е Комисията да преразглежда и актуализира разпоредбите относно сигурността на използваните от нея комуникационни и информационни системи.

(12) В тази връзка следва да бъде отменено Решение C(2006) 3602 на Комисията,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

ГЛАВА 1

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и област на приложение

1. Настоящото решение се прилага за всички комуникационни и информационни системи (КИС), които се притежават, придобиват, управляват или експлоатират от Комисията или от нейно име, и за всяко използване на тези КИС от Комисията.

2. Настоящото решение установява основните принципи, цели, организация и отговорности по отношение на сигурността на тези КИС, и по-конкретно за службите на Комисията, които притежават, придобиват, управляват или експлоатират КИС, включително КИС, осигурявани от вътрешен доставчик на информационни услуги. Когато дадена КИС е осигурявана, притежавана, управлявана или експлоатирана от външно лице въз основа на двустранно споразумение или договор с Комисията, условията на споразумението или договора трябва да отговарят на разпоредбите на настоящото решение.

3. Настоящото решение се прилага за всички служби и изпълнителни агенции на Комисията. Когато КИС на Комисията се използва от други органи и институции въз основа на двустранно споразумение с Комисията, условията на споразумението трябва да отговарят на разпоредбите на настоящото решение.

4. Независимо от специалните разпоредби, отнасящи се до определени групи служители, настоящото решение се прилага към членовете на Комисията, към служителите на Комисията, за които се отнасят Правилникът за длъжностните лица на Европейския съюз („Правилник за длъжностните лица“) и Условията за работа на другите служители на Съюза („УРДСС“) ([3]), към командированите национални експерти в Комисията („КНЕ“) ([4]), към външните доставчици на услуги и техните служители, към стажантите и към всяко физическо лице с достъп до КИС, попадащи в приложната област на настоящото решение.

5. Настоящото решение се прилага към Европейската служба за борба с измамите (OLAF), доколкото това е съвместимо със законодателството на Съюза и с Решение 1999/352/ЕО, ЕОВС, Евратом на Комисията ([5]). По-конкретно, възможно е мерките, предвидени в настоящото решение, включително указания, проверки, анкети и равностойни мерки, да не се прилагат към КИС на Службата, когато това не е съвместимо с независимостта на функцията за разследване на Службата и/или с поверителността на информацията, получена от Службата при упражняването на тази функция.

Член 2

Дефиниции

За целите на настоящото решение се прилагат следните дефиниции:

(1) „Лице, което носи отговорност“ е лице, отговарящо за действия, решения и ефективност.

([1]) Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 година относно сигурността в Комисията (ОВ L 72, 17.3.2015 г., стр. 41).
([2]) Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 година относно правилата за сигурност за защита на класифицираната информация на ЕС (ОВ L 72, 17.3.2015 г., стр. 53).
([3]) Установени с Решение (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета (ОВ L 56, 4.3.1968 г., стр. 1.)
([4]) Решение на Комисията от 12 ноември 2008 година относно правилата, приложими към командированите национални експерти и националните експерти на обучение към службите на Комисията (C(2008) 6866 final).
([5]) Решение 1999/352/ЕО, ЕОВС, Евратом на Комисията от 28 април 1999 година за създаване на Европейска служба за борба с измамите (OLAF) (ОВ L 136, 31.5.1999 г., стр. 20).

(2) „CERT-EU“ е екипът за незабавно реагиране при компютърни инциденти в институциите и агенциите на ЕС. Мисията му е да подпомага европейските институции в защитата им срещу умишлени и злонамерени атаки, които могат да нарушат целостта на техните информационни активи и да накърнят интересите на ЕС. Обхватът на дейностите на CERT-EU включва предотвратяване, разкриване, реагиране и възстановяване.

(3) „Служба на Комисията“ означава всяка генерална дирекция или служба на Комисията, както и всеки кабинет на член на Комисията.

(4) „Орган по сигурността на Комисията“ се отнася до функцията, установена в Решение (ЕС, Евратом) 2015/444.

(5) „Комуникационна и информационна система“ или „КИС“ означава всяка система, която позволява обработката на информация в електронен вид, включително всички активи, необходими за нейната експлоатация, както и съответните инфраструктурни, организационни, кадрови и информационни ресурси. Тази дефиниция включва бизнес приложения, споделени информационни ресурси, системи, предоставяни от външни доставчици и устройства на крайни потребители.

(6) „Общ управителен съвет“ (ОУС) е орган, осъществяващ вътрешноведомствен управленски надзор на най-високо равнище върху оперативните и административните въпроси в Комисията.

(7) „Отговорник за данни“ е физическото лице, което отговаря за осигуряването на защитата и използването на конкретен масив от данни, обработвани в КИС.

(8) „Набор от данни“ означава определена информация, обслужваща определен бизнес процес или дейност на Комисията.

(9) „Процедура при извънредни ситуации“ означава предварително определен комплекс от методи и отговорности за реагиране на спешни ситуации с оглед недопускането на значително въздействие върху Комисията.

(10) „Политика за информационна сигурност“ означава комплекс от цели по отношение на информационната сигурност, които са или трябва да бъдат установени, прилагани и проверявани. Тази политика включва решения (ЕС, Евратом) 2015/444 и (ЕС, Евратом) 2015/443, но не се ограничава с тях.

(11) „Управителен съвет за информационна сигурност“ (УСИС) е управителният орган, който подпомага Общия управителен съвет по отношение на задачите му, свързани с информационната сигурност.

(12) „Вътрешен доставчик на информационни услуги“ означава служба на Комисията, която предоставя споделени информационни услуги.

(13) „Информационна сигурност“ или „сигурност на КИС“ означава опазването на поверителността, целостта и наличността на КИС и на обработваните от тях данни.

(14) „Насоки за информационна сигурност“ представляват препоръчителни, но доброволно прилагани мерки, които спомагат за поддържането на стандартите за информационна сигурност или служат за референтен източник при липсата на приложим стандарт.

(15) „Инцидент, свързан с информационната сигурност“ означава събитие, което може да има неблагоприятни последици за поверителността, целостта или готовността за работа на КИС.

(16) „Мярка за информационна сигурност“ означава техническа или организационна мярка, насочена към ограничаването на рисковете за информационната сигурност.

(17) „Потребност, свързана с информационната сигурност“ означава точна и недвусмислена дефиниция на равнищата на поверителност, цялост и наличност, свързани с определена информация или информационна система с оглед определянето на необходимото ниво на защита.

(18) „Цел по отношение на информационната сигурност“ означава заявено намерение за противодействие на определени заплахи и/или за изпълнение на определени изисквания или предпоставки по отношение на информационната сигурност.

(19) „План за информационна сигурност“ означава документация на мерките за информационна сигурност, необходими за удовлетворяване на потребностите, свързани с информационната сигурност на дадена КИС.

(20) „Политика за информационна сигурност“ означава комплекс от цели по отношение на информационната сигурност, които са или трябва да бъдат установени, прилагани и проверявани. Тази политика включва настоящото решение и правилата за неговото прилагане.

(21) „Изискване по отношение на информационната сигурност“ означава потребност, свързана с информационната сигурност, която е установена официално по предварително определен ред.

(22) „Риск за информационната сигурност“ означава ефект, който може да бъде предизвикан в КИС от заплаха за информационната сигурност, възползваща се от слабост в системата. В този смисъл, рискът за информационната сигурност се характеризира от два фактора: 1) неопределеност, тоест вероятността заплаха за информационната сигурност да предизвика нежелано събитие и 2) въздействие, тоест последствията, което такова нежелано събитие може да има за КИС.

(23) „Стандарти за информационна сигурност“ означава специфични задължителни мерки за информационна сигурност, които спомагат за прилагането и за поддържането на политиката за информационна сигурност.

(24) „Стратегия за информационна сигурност“ означава комплекс от проекти и дейности, които са предназначени за постигане на целите на Комисията и следва да бъдат установявани, прилагани и проверявани.

(25) „Заплаха за информационната сигурност“ означава фактор, който може да доведе до нежелано събитие, което на свой ред да навреди на КИС. Тези заплахи могат да са неумишлени или умишлени и се характеризират със застрашаващи елементи, потенциални цели и методи за атакуване.

(26) „Локален служител по информатика и сигурност“ или „ЛСИС“ означава служител за връзка по въпросите на информационната сигурност, определен за дадена служба на Комисията.

(27) „Лични данни“, „обработка на лични данни“, „контролиращ орган“ и „система за архивиране на лични данни“ имат същото значение както в Регламент (ЕО) № 45/2001 и по-конкретно в член 2 от него.

(28) „Обработка на информация“ означава всички функции на КИС по отношение на наборите от данни, включително създаване, промяна, показване, съхранение, предаване, изтриване и архивиране на информация. Една КИС може да обработва информация като набор от функционалности, предназначени за потребители, или като информационни услуги за друга КИС.

(29) „Професионална тайна“ означава защитата на стопанска информация, включена в обхвата на професионалната тайна, в частност информация относно предприятия, техните стопански отношения или факторите за ценообразуване в тях, както е посочено в член 339 от ДФЕС.

(30) „Отговорно лице“ означава лице, имащо задължението да извършва действия и взема решения за постигането на необходимите резултати.

(31) „Сигурност в Комисията“ означава сигурността на лица, активи и информация в Комисията и по-конкретно физическата неприкосновеност на лица и активи, целостта, поверителността и наличността на информация и на комуникационни и информационни системи, както и безпрепятственото изпълнение на операциите на Комисията.

(32) „Споделена информационна услуга“ означава услуга, която КИС предоставя на други КИС при обработката на информация.

(33) „Отговорник на система“ е физическо лице, което носи цялостна отговорност за придобиването, разработването, внедряването, изменянето, експлоатацията, обслужването и извеждането от експлоатация на КИС.

(34) „Потребител“ означава всяко физическо лице, което използва функционалност, предоставяна от КИС, независимо дали в Комисията или извън нея.

Член 3

Принципи на информационната сигурност в Комисията

1. Информационната сигурност в Комисията се основава на принципите на законосъобразност, прозрачност, пропорционалност и отчетност.

2. Въпросите, свързани с информационната сигурност, се вземат предвид от самото начало на разработването и внедряването на всички КИС на Комисията. За тази цел Генерална дирекция „Информатика“ и Генерална дирекция „Човешки ресурси и сигурност“ вземат участие в своите области на отговорност.

3. Ефективната информационна сигурност гарантира подходящи нива на:

а) Автентичност: гаранция, че информацията е истинска и от добросъвестни източници.

б) Наличност: свойството на един обект да бъде достъпен и използваем по искане на упълномощен субект.

в) Поверителност: информацията не се разкрива на неупълномощени физически лица, субекти или процеси.

г) Цялост: опазване на точността и пълнотата на активите и информацията.

д) Неопровержимост: възможността да се докаже извършването на действие или настъпването на събитие по начин, изключващ отричането на това събитие или действие впоследствие.

е) Защита на личните данни: осигуряване на подходящи предпазни мерки по отношение на личните данни в пълно съответствие с Регламент (ЕО) № 45/2001.

ж) „Професионална тайна“: защитата на информацията, включена в обхвата на професионалната тайна, в частност информация относно предприятия, техните стопански отношения или факторите за ценообразуване в тях, както е посочено в член 339 на ДФЕС.

4. Информационната сигурност се основава на процес за управление на риска. Този процес е насочен към установяването на нивата на рисковете за информационната сигурност и към определянето на мерки за сигурност с оглед намаляването на тези рискове до подходящо ниво и при съобразени разходи.

5. Всяка КИС се идентифицира, възлага се на отговорник на система и се регистрира в инвентарен опис.

6. Изискванията по отношение на информационната сигурност на всяка КИС се определят въз основа на потребностите, свързани със сигурността на самите системи и на обработваната от тях информация. КИС, които предоставят услуги на други КИС, могат да бъдат проектирани така, че да поддържат определени нива на потребности, свързани със сигурността.

7. Плановете за информационна сигурност и мерките за информационна сигурност трябва да са пропорционални на потребностите, свързани със сигурността на КИС.

Процесите, свързани с тези принципи и дейности, се доразвиват в правила за прилагане.

ГЛАВА 2

ОРГАНИЗАЦИЯ И ОТГОВОРНОСТИ

Член 4

Общ управителен съвет

Общият управителен съвет поема общата отговорност за цялостното управление на информационната сигурност в Комисията.

Член 5

Управителен съвет по информационна сигурност (УСИС)

1. УСИС се председателства от заместник генералния секретар, който отговаря за управлението на информационната сигурност в Комисията. Членовете на УСИС представляват всички звена в службите на Комисията, които имат отношение към стопанската дейност, технологиите и сигурността, и включват представители на Генерална дирекция „Информатика“, Генерална дирекция „Човешки ресурси и сигурност“, Генерална дирекция „Бюджет“ и чрез ротация през две години — на четири други служби на Комисията, в които информационната сигурност е от съществено значение за тяхната дейност. За членове на УСИС се определят служители, които заемат висши ръководни длъжности.

2. УСИС подпомага Общия управителен съвет в неговите задачи, свързани с информационната сигурност. УСИС поема оперативната отговорност за цялостното управление на информационната сигурност в Комисията.

3. УСИС представя политиката за информационна сигурност на Комисията, която я одобрява.

4. На всеки две години УСИС извършва преглед и докладва на Общия управителен съвет по въпросите на управлението, както и по проблемите на информационната сигурност, включително за сериозни инциденти, свързани с информационната сигурност.

5. УСИС наблюдава и разглежда цялостното изпълнение на настоящото решение и докладва за изпълнението пред Общия управителен съвет.

6. По предложение на Генерална дирекция „Информатика“ УСИС разглежда, одобрява и наблюдава изпълнението на актуалната стратегия за информационна сигурност. УСИС докладва за това пред Общия управителен съвет.

7. УСИС наблюдава, оценява и контролира ведомствената рамка за третиране на информационния риск и има право при необходимост да издава официални предписания за подобрения.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

Член 6

Генерална дирекция „Човешки ресурси и сигурност“

Генерална дирекция „Човешки ресурси и сигурност“ има следните отговорности по отношение на информационната сигурност. Генералната дирекция:

1) осигурява съгласуваност между политиката за информационна сигурност и политиката на Комисията за сигурност на информацията;

2) установява рамка за разрешаване на използването на криптографски технологии при съхраняването и предаването на информация от КИС;

3) уведомява Генерална дирекция „Информатика“ за специфични заплахи, които могат да окажат значително въздействие върху сигурността на КИС и на обработваните от тях набори от данни;

4) осъществява проверки, свързани с информационната сигурност, за да оцени съответствието на КИС на Комисията с политиката за сигурност, и докладва резултатите на УСИС;

5) установява рамка за разрешаване на достъпа до КИС на Комисията от външни мрежи, включително подходящи правила за сигурност в тази връзка, разработва съответните стандарти и насоки за информационна сигурност в тясно сътрудничество с Генерална дирекция „Информатика“;

6) предлага принципи и правила за използването на КИС от външни доставчици с оглед поддържането на подходящ контрол върху сигурността на информацията;

7) разработва свързаните с член 6 стандарти и насоки за информационна сигурност в тясно сътрудничество с Генерална дирекция „Информатика“.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

Член 7

Генерална дирекция „Информатика“

Генерална дирекция „Информатика“ има следните отговорности във връзка с цялостната информационна сигурност на Комисията. Генералната дирекция:

1) разработва, в тясно сътрудничество с Генерална дирекция „Човешки ресурси и сигурност“, стандарти и насоки за информационна сигурност, с изключение на предвидените в член 6, с оглед осигуряването на съгласуваност между политиката на информационна сигурност и политиката на Комисията за сигурност на информацията, и предлага тези стандарти и насоки на УСИС;

2) оценява методите, процесите и резултатите, свързани с управлението на информационния риск във всички служби на Комисията, и докладва редовно на УСИС;

3) предлага подлежаща на редовно актуализиране стратегия за информационна сигурност за преглед и одобряване от УСИС и за утвърждаване от Общия управителен съвет, а освен това предлага програма за изпълнение на Стратегията за информационна сигурност, включително план за проекти и дейности;

4) наблюдава изпълнението на стратегията на Комисията за информационна сигурност и докладва по този въпрос на УСИС;

5) наблюдава рисковете за информационната сигурност и приложените в КИС мерки за информационна сигурност и докладва редовно по тези въпроси на УСИС;

6) докладва редовно на УСИС относно цялостното изпълнение и спазване на настоящото решение;

7) след съгласуване с Генерална дирекция „Човешки ресурси и сигурност“ изисква от отговорниците на системи да вземат конкретни мерки за информационна сигурност с оглед на ограничаването на рисковете за информационната сигурност на КИС на Комисията;

8) гарантира, че отговорниците на системи и отговорниците за данни разполагат с адекватен списък с услуги за сигурност, предлагани от Генерална дирекция „Информатика“, за да изпълняват своите задължения по отношение на информационната сигурност и за да спазват политиката и стандартите за информационна сигурност;

9) осигурява подходяща документация на отговорниците на системи и отговорниците за данни и при необходимост провежда с тях консултации по мерките за информационна сигурност, внедрени в техните информационни услуги, за да съдейства за спазването на политиката за информационна сигурност и за да подпомага отговорниците на системи в дейностите им по управление на риска;

10) организира редовни срещи на мрежата от ЛСИС и подпомага ЛСИС в изпълнението на техните задължения;

11) установява потребностите от обучение и координира програмите за обучение по информационна сигурност в сътрудничество със службите на Комисията, и разработва, изпълнява и координира разяснителни кампании в областта на информационната сигурност в тясно сътрудничество с Генерална дирекция „Човешки ресурси“;

12) взема необходимите мерки с оглед на това отговорниците на системи, отговорниците за данни и другите служители със задължения в областта на информационната сигурност да бъдат запознати с политиката за информационна сигурност;

13) информира Генерална дирекция „Човешки ресурси и сигурност“ относно конкретни заплахи и инциденти, свързани с информационната сигурност, както и за отклоненията от политиката за информационна сигурност на Комисията, съобщени от отговорниците на системи, които могат да окажат значително въздействие върху сигурността в Комисията;

14) във връзка с функцията си на вътрешен доставчик на информационни услуги, предоставя на Комисията каталог на споделените информационни услуги, които осигуряват определени нива на сигурност. Това се осъществява чрез систематично оценяване, управление и наблюдение на рисковете за информационната сигурност с оглед прилагането на мерки за сигурност, насочени към постигането на определеното ниво на сигурност.

Свързаните процеси и по-конкретни отговорности се доразвиват в правила за прилагане.

Член 8

Служби на Комисията

Във връзка с информационната сигурност в своята служба, всеки ръководител на служба на Комисията:

1) назначава официално отговорник на система за всяка отделна КИС и нейната информационна сигурност, който може да е щатен или срочно нает служител, и отговорник за данни по отношение на всеки набор от данни, обработван в КИС, като този отговорник следва да е служител на административното звено, което е администратор на лични данни за наборите от данни, обхванати от Регламент (ЕО) № 45/2001;

2) определя официално локален служител по информатика и сигурност (ЛСИС), който е в състояние да изпълнява задълженията независимо от отговорниците на системи и отговорниците за данни. Един ЛСИС може да бъде определен за една или повече служби на Комисията;

3) осигурява изготвянето и изпълнението на оценки на рисковете за информационната сигурност и планове за информационна сигурност;

4) осигурява редовното докладване на обобщения на рисковете и мерките за информационна сигурност на Генерална дирекция „Информатика“;

5) осигурява, със съдействието на Генерална дирекция „Информатика“, наличието на подходящи процеси, процедури и средства за ефективно разкриване, докладване и преодоляване на инциденти, свързани със сигурността на техните КИС;

6) стартира процедура при извънредни ситуации в случай на извънредни ситуации, свързани с информационната сигурност;

7) носи пълна отговорност за информационната сигурност, включително за задълженията на отговорниците на системи и отговорниците за данни;

8) отговаря за рисковете, свързани с КИС и с наборите от данни в службата;

9) решава евентуалните разногласия между отговорници за данни и отговорници на системи, а при невъзможност за намиране на решение представя въпроса за решаване от УСИС;

10) осигурява изпълнението на плановете и мерките за информационна сигурност, както и обхващането на рисковете по подходящ начин;

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

Член 9

Отговорници на системи

1. Отговорникът на система отговаря за информационната сигурност на КИС и докладва на ръководителя на службата на Комисията.

2. Във връзка с информационната сигурност, отговорникът на система:

а) осигурява съответствието на КИС с политиката за информационната сигурност;

б) осигурява точното регистриране на КИС в съответния инвентарен опис;

в) извършва оценка на рисковете за информационната сигурност и определя потребностите по отношение на информационната сигурност за всяка КИС във взаимодействие с отговорниците за данни и в консултация с Генерална дирекция „Информатика“;

г) изготвя план за сигурност, включващ по целесъобразност данни за оценените рискове и допълнителни мерки за сигурност, ако са необходими;

д) прилага подходящи мерки за информационна сигурност, които са пропорционални на установените рискове за информационната сигурност и изпълнява препоръките, утвърдени от УСИС;

е) установява всички зависимости от други КИС или от споделени информационни услуги и прилага по целесъобразност мерки за сигурност съобразно нивата на сигурност, предлагани от тези КИС или споделени информационни услуги;

ж) управлява и наблюдава рисковете за информационната сигурност;

з) докладва редовно на ръководителя на службата на Комисията за профила на риска за информационната сигурност на съответните КИС и докладва на Генерална дирекция „Информатика“ за свързаните рискове, дейностите по управление на риска и предприетите мерки за сигурност;

и) провежда консултации с ЛСИС на съответните служби на Комисията по аспекти на информационната сигурност;

й) издава указания за потребителите относно използването на КИС и свързаните данни, както и за отговорностите на потребителите, отнасящи се до КИС;

к) иска одобрение от Генерална дирекция „Човешки ресурси и сигурност“, в качеството ѝ на орган за криптографско одобрение, за всяка КИС, която използва криптографска технология;

л) провежда предварителни консултации с органа по сигурността в Комисията относно всяка система, която обработва класифицирана информация на ЕС;

м) осигурява съхраняването на резервни копия от кодовете за декриптиране в строго ограничен потребителски профил. Възстановяването на криптирани данни се извършва само с разрешение, предоставено в съответствие с рамката, определена от Генерална дирекция „Човешки ресурси и сигурност“;

н) спазва указанията от съответните администратори на лични данни относно защитата на лични данни и прилагането на правилата за защита на данните във връзка със сигурността на обработката;

о) уведомява Генерална дирекция „Информатика“ за всички отклонения от политиката на Комисията за информационна сигурност, включително съответните мотиви;

п) докладва на ръководителя на службата на Комисията за всички неуредени разногласия между отговорника за данните и отговорника на системата, съобщава своевременно и адекватно инцидентите, свързани с информационната сигурност, на съответните заинтересовани страни по степен на сериозност, както е предвидено в член 15;

р) за системите, осигурявани от външни доставчици, осигурява включването на подходящи разпоредби за информационна сигурност в договорите с външните доставчици, както и докладването в съответствие с член 15 на инцидентите, свързани с информационната сигурност и възникнали в тези системи;

с) за КИС, които предоставят споделени информационни услуги, осигурява предоставянето и ясното документиране на определено ниво на сигурност, както и прилагането на мерки за сигурност за тези КИС с оглед достигането на определеното ниво на сигурност.

3. Отговорниците на системи могат да делегират изцяло или частично своите задачи, свързани с информационната сигурност, но продължават да носят отговорност за информационната сигурност на своите КИС.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

Член 10

Отговорници за данни

1. Отговорникът за данни отговаря за информационната сигурност на конкретния набор от данни пред ръководителя на службата на Комисията и носи отговорност за поверителността, целостта и наличността на набора от данни.

2. Във връзка с този набор от данни, отговорникът за данни:

а) осигурява правилното класифициране на всички данни, за които носи отговорност, в съответствие с решения (ЕС, Евратом) 2015/443 и (ЕС, Евратом) 2015/444;

б) определя потребностите, свързани с информационната сигурност, и информира съответните отговорници на системи за тези потребности;

в) участва в оценките на риска за КИС;

г) докладва на ръководителя на службата на Комисията за всички неуредени разногласия между отговорника за данните и отговорника на системата;

д) съобщава инцидентите, свързани с информационната сигурност, в съответствие с предвиденото в член 15.

3. Отговорниците за данни могат официално да делегират изцяло или частично своите задачи, свързани с информационната сигурност, но запазват своите отговорности по настоящия член.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

Член 11

Локален служител по информатика и сигурност (ЛСОС)

Във връзка с информационната сигурност, ЛСОС:

а) активно набелязва и информира отговорниците на системи, отговорниците за данни и на останалите служители, имащи задължения по отношение на информационната сигурност в службата или службите на Комисията, относно политиката за информационна сигурност;

б) осъществява връзка по въпроси, свързани с информационната сигурност в службата или службите на Комисията с Генерална дирекция „Информатика“ като част от мрежата на ЛСОС;

в) участва в редовните срещи на всички ЛСОС;

г) поддържа общ поглед върху процеса за управление на риска за сигурността на информацията и върху разработването и изпълнението на планове за сигурност на системите за информация;

д) съветва отговорниците за данни, отговорниците на системи и ръководителите на служби в Комисията по въпроси, свързани с информационната сигурност;

е) сътрудничи с Генерална дирекция „Информатика“ за разпространяването на добри практики в областта на информационната сигурност и предлага конкретни разяснителни и обучителни програми;

ж) докладва по въпросите на информационната сигурност, посочва недостатъците и възможностите за подобрения пред ръководителя на съответната служба на Комисията.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

Член 12

Потребители

1. Във връзка с информационната сигурност потребителите:

а) изпълняват политиката за информационна сигурност и указанията за използването на КИС, дадени от отговорника на системата.

б) съобщават за инцидентите, свързани с информационната сигурност, в съответствие с предвиденото в член 15.

2. Използването на КИС на Комисията в нарушение на политиката за информационна сигурност или на указанията, дадени от отговорника на системата, може да е основание за образуване на дисциплинарна процедура.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

ГЛАВА 3

ИЗИСКВАНИЯ И ЗАДЪЛЖЕНИЯ, СВЪРЗАНИ СЪС СИГУРНОСТТА

Член 13

Прилагане на настоящото решение

1. Правилата за прилагане в член 6 и съответните стандарти и насоки се приемат въз основа на решение на Комисията за оправомощаване на члена на Комисията, който отговаря за въпросите, свързани със сигурността.

2. Всички останали правила за прилагане във връзка с настоящото решение и съответните стандарти и насоки за информационна сигурност се приемат въз основа на решение на Комисията за оправомощаване на члена на Комисията, който отговаря за информатиката.

3. УСИС одобрява правилата за прилагане, стандартите и насоките, упоменати в параграфи 1 и 2 по-горе преди тяхното приемане.

Член 14

Задължително спазване

1. Разпоредбите, предвидени в политиката и стандартите за информационна сигурност, се спазват задължително.

2. Неспазването на политиката и на стандартите за информационна сигурност може да стане основание за прилагане на дисциплинарни мерки в съответствие с Договорите, Правилника за длъжностните лица и Условията за работа на другите служители на Европейския съюз, за налагане на санкции по договори и/или за образуване на съдебни производства по съответното национално законодателство.

3. Генерална дирекция „Информатика“ се уведомява за всички отклонения от политиката за информационна сигурност.

4. Ако по преценка на УСИС съществува постоянен неприемлив риск за определена КИС на Комисията, Генерална дирекция „Информатика“ предлага, в сътрудничество с отговорника на системата, мерки за ограничаване на риска, които УСИС трябва да одобри. Тези мерки могат да включват усилено наблюдение и докладване, въвеждане на ограничения върху услуга и изключване.

5. При необходимост УСИС осигурява налагането на одобрените ограничаващи риска мерки. УСИС може да препоръча на генералния директор на Генерална дирекция „Човешки ресурси и сигурност“ да образува административно разследване. Генерална дирекция „Информатика“ докладва на УСИС за всички случаи, в които са наложени ограничаващи риска мерки.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

Член 15

Управление на инциденти, свързани с информационната сигурност

1. Генерална дирекция „Информатика“ отговаря за осигуряването на основния оперативен капацитет за реагиране на инциденти, свързани с информационната сигурност в Европейската комисия.

2. В качеството си на заинтересована страна, която участва в реагирането на инциденти, свързани с информационната сигурност, Генерална дирекция „Човешки ресурси и сигурност“:

а) има право да достъп до обобщена информация за всички регистрирани инциденти и до пълните им записи при поискване;

б) участва в групи за управление на кризи при инциденти, свързани с информационната сигурност, и в процедурите при спешни ситуации, свързани с информационната сигурност;

в) отговаря за взаимоотношенията с правоприлагащите и разузнавателните служби;

г) извършва криминологични анализи във връзка с киберсигурността в съответствие с член 11 от Решение (ЕС, Евратом) 2015/443;

д) приема решения относно необходимостта от образуване на официални разследвания;

е) уведомява Генерална дирекция „Информатика“ за всички инциденти, свързани с информационната сигурност, които могат да представляват риск за други КИС.

3. Генерална дирекция „Информатика“ и Генерална дирекция „Човешки ресурси и сигурност“ поддържат редовна комуникация за обмен на информация и за координиране на управлението на инциденти, свързани със сигурността, по-конкретно на всеки инцидент, свързан с информационната сигурност, за който може да се изисква официално разследване.

4. Екипът за незабавно реагиране при компютърни инциденти за институциите, службите и агенциите на ЕС (CERT-EU) може да бъде привлечен за съдействие в процеса на управление на инциденти по целесъобразност, както и за споделяне на знания с други институции и агенции на ЕС, които е вероятно да бъдат засегнати.

5. Отговорниците на системи, засегнати от инцидент, свързан с информационната сигурност:

а) уведомяват незабавно съответните ръководители на служби на Комисията, Генерална дирекция „Информатика“, Генерална дирекция „Човешки ресурси“, ЛСИС и по целесъобразност отговорника за данните относно всички важни инциденти, свързани с информационната сигурност, особено тези, в които е нарушена поверителността на данните;

б) съдействат и следват указанията на съответните органи на Комисията относно съобщаването, реакцията и отстраняването на последствията от инцидента.

6. Потребителите своевременно докладват всички реални или предполагаеми инциденти, свързани с информационната сигурност, на съответната служба за ИТ поддръжка.

7. Отговорниците за данни своевременно докладват за всички реални или предполагаеми инциденти, свързани с информационната сигурност, на съответния екип за реагиране на инциденти, свързани с информационната сигурност.

8. Генерална дирекция „Информатика“, с подкрепата на всички участващи заинтересовани страни, отговаря за управлението на всеки инцидент, свързан с информационната сигурност, регистриран във връзка с КИС на Комисията, които не се осигуряват от външни доставчици.

9. За инцидентите, свързани с информационната сигурност, Генерална дирекция „Информатика“ информира засегнатите служби на Комисията, съответните ЛСИС и по целесъобразност CERT-EU на принципа „необходимост да се знае“.

10. Генерална дирекция „Информатика“ редовно докладва на УСИС относно сериозни инциденти, свързани с информационната сигурност, които засягат КИС на Комисията.

11. При поискване съответните ЛСИС получават достъп до записите на инциденти, свързани с информационната сигурност, които засягат КИС на съответната служба на Комисията.

12. В случай на сериозен инцидент, свързан с информационната сигурност, Генерална дирекция „Информатика“ изпълнява функциите на звено за контакт по управлението на кризисни ситуации, като координира групите за управление на кризи при инциденти, свързани с информационната сигурност.

13. В случай на извънредна ситуация, Генералният директор на Генерална дирекция „Информатика“ може да вземе решение за стартиране на процедура при извънредни ситуации, свързани с информационната сигурност. Генерална дирекция „Информатика“ разработва процедури при извънредни ситуации, които се одобряват от УСИС.

14. Генерална дирекция „Информатика“ докладва за изпълнението на процедурите при извънредни ситуации на УСИС и на ръководителите на засегнатите служби на Комисията.

Процесите, свързани с тези отговорности и дейности, се доразвиват в правила за прилагане.

ГЛАВА 4

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 16

Прозрачност

Настоящото решение се довежда до вниманието на служителите на Комисията и на всички лица, за които то се прилага, и се публикува в *Официалния вестник на Европейския съюз*.

Член 17

Връзка с други актове

Разпоредбите на настоящото решение не засягат Решение (ЕС, Евратом) 2015/443, Решение (ЕС, Евратом) 2015/444, Регламент (ЕО) № 45/2001, Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета ([1]), Решение 2002/47/ЕО, ЕОВС, Евратом на Комисията ([2]), Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета ([3]), Решение 1999/352/ЕО, ЕОВС, Евратом.

Член 18

Отмяна на предходни актове и преходни мерки

Решение C(2006) 3602 от 16 август 2006 г. се отменя.

Доколкото не противоречат на настоящото решение, правилата за прилагане и стандартите за информационна сигурност, приети въз основа на член 10 от Решение C(2006) 3602, остават в сила до заместването им с правилата за прилагане и стандартите, които следва да бъдат приети по член 13 от настоящото решение. Позоваванията на член 10 от Решение C(2006) 3602 се считат за позовавания на член 13 от настоящото решение.

Член 19

Влизане в сила

Настоящото решение влиза в сила на двадесетия ден след датата на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 10 януари 2017 година.

За Комисията

Председател

Jean-Claude JUNCKER

([1]) Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 година относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (ОВ L 145, 31.5.2001 г., стр. 43).

([2]) Решение 2002/47/ЕО, ЕОВС, Евратом на Комисията от 23 януари 2002 година за изменение на нейния процедурен правилник (ОВ L 21, 24.1.2002 г., стр. 23).

([3]) Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 11 септември 2013 година относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), и за отмяна на Регламент (ЕО) № 1073/1999 на Европейския парламент и на Съвета и Регламент (Евратом) № 1074/1999 на Съвета (ОВ L 248, 18.9.2013 г., стр. 1).