BG 2022

05

Специален доклад

Киберсигурност в институциите, органите и агенциите на ЕС —

нивото на подготвеност като цяло не съответства на заплахите

ЕВРОПЕЙСКА СМЕТНА ПАЛАТА

Съдържание

	Точки
Кратко изложение	I—VII
Въведение	01—12
Какво представлява киберсигурността?	01—03
Киберсигурността в институциите, органите и агенциите на ЕС	04—12
Обхват и подход на одита	13—19
Констатации и оценки	20—94
EUIBA имат много различни равнища на зрялост в областта на киберсигурността и невинаги се съобразяват с добрите практики	20—44
Управлението на ИТ сигурността в EUIBA често не е добре развито, а оценките на риска не са изчерпателни	21—29
EUIBA не разполагат с последователен подход към киберсигурността и невинаги са налице основни механизми за контрол	30—38
Механизмите в областта на киберсигурността в няколко EUIBA не са обект на редовна независима проверка	39—44
EUIBA разполагат с установени механизми за сътрудничество, но са налице слабости	45—63
Налице е формализирана структура за координиране на дейностите на ENISA, макар и с известни проблеми, свързани с управлението	46—53
Потенциалните полезни взаимодействия чрез сътрудничество все още не се използват изцяло	54—63
ENISA и CERT-EU все още не предоставят на EUIBA цялата подкрепа, от която те се нуждаят	64—94
ENISA е ключов елемент в областта на киберсигурността в ЕС, но досега нейната подкрепа е достигнала до много малко EUIBA	65—73
CERT-EU е високо ценен от участниците в него, но възможностите му не съответстват на актуалните предизвикателства в областта на киберсигурността	74—94
Заключения и препоръки	95—100

Приложения

Приложение I — Списък на EUIBA, обхванати от проучването

Приложение II —Допълнителна информация относно ключовите междуинституционални комитети

Акроними и съкращения

Речник на термините

Отговори на Комисията

Отговори на CERT-EU и ENISA

Хронология

Кратко изложение

I Актът на ЕС за киберсигурността определя киберсигурността като „дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и други лица, засегнати от киберзаплахи“. Поради чувствителния характер на информацията, която те обработват, институциите, органите и агенциите на ЕС (EUIBA) са примамлива мишена за потенциални нападатели, особено за групи, които са способни да извършват високотехнологични скрити атаки за кибершпионаж и други цели. Въпреки тяхната институционална независимост и административна автономност, EUIBA са силно взаимосвързани. Поради това слабостите в отделни EUIBA могат да изложат останалите на заплахи за сигурността.

II Предвид факта, че броят на кибератаките върху EUIBA рязко се увеличава, целта на одита беше да се определи дали EUIBA като цяло разполагат с установени практически механизми за защита срещу киберзаплахи. Нашето заключение е, че общността от EUIBA не е постигнала ниво на подготвеност в областта на киберсигурността, което да съответства на заплахите.

III ЕСП установи, че ключовите добри практики в областта на киберсигурността невинаги се прилагат, включително редица основни механизми за контрол, както и че някои EUIBA не инвестират достатъчно средства за киберсигурност. Стабилното управление на киберсигурността също така не е въведено в някои EUIBA: в много случаи стратегии за информационна сигурност липсват или такива не са одобрени от висшето ръководство, политиките за сигурност не са винаги официално определени, а оценките на риска не обхващат цялата ИТ среда. В не всички EUIBA киберсигурността е обект на редовна независима проверка.

IV Обученията, свързани с киберсигурността, невинаги се провеждат систематично. Едва малко над половината EUIBA предлагат текущо обучение в областта на киберсигурността за ИТ служителите и специалистите по ИТ сигурност. Само някои EUIBA осигуряват задължително обучение в тази област за служителите, които отговарят за управлението на информационни системи, съдържащи чувствителна информация. Фишинг ученията са важен инструмент за обучение на персонала и за повишаване на осведомеността, но не всички EUIBA ги използват систематично.

V Въпреки че EUIBA разполагат с установени структури за сътрудничество и обмен на информация относно киберсигурността, ЕСП констатира, че потенциалните полезни взаимодействия не са напълно използвани. EUIBA не обменят систематично помежду си информация относно свързани с киберсигурността проекти, оценки на сигурността и договори за услуги. Освен това инструментите за комуникация, например криптирана електронна поща или решения за видеоконферентна връзка, не са напълно оперативно съвместими. Това може да доведе до понижена сигурност на обмена на информация, дублиране на усилията и повишени разходи.

VI Екипът за незабавно реагиране при компютърни инциденти на EUIBA (CERT-EU) и Агенцията на Европейския съюз за киберсигурност (ENISA) са двете основни организации, на които е възложена задачата да предоставят подкрепа на EUIBA в областта на киберсигурността. Поради ограничени ресурси или отдаване на приоритет на други области те не са в състояние да предоставят на EUIBA цялата необходима подкрепа, особено във връзка с изграждането на капацитет в EUIBA с по-ниски равнища на зрялост. Макар и CERT-EU да е високо ценен от EUIBA, неговата ефективност не е оптимална поради нарастващото работно натоварване, променливото финансиране и численост на персонала, както и поради недостатъчното сътрудничество с някои EUIBA, които невинаги обменят своевременна информация относно уязвимостите и сериозните киберинциденти, които ги засягат или могат да засегнат други институции.

VII Въз основа на тези заключения ЕСП препоръчва:

- Комисията следва да подобри подготвеността на EUIBA в сектора на киберсигурността чрез изготвяне на законодателно предложение, което да въведе обвързващи правила в тази област за всички EUIBA и да увеличи наличните ресурси за CERT-EU;

- Комисията, в контекста на Междуинституционалния комитет за цифрова трансформация, следва да насърчи допълнителни полезни взаимодействия сред EUIBA в избрани области;

- CERT-EU и ENISA следва да отделят по-голямо внимание на онези EUIBA, които имат по-ниски равнища на зрялост в областта на киберсигурността;

Въведение

Какво представлява киберсигурността?

01 Актът на ЕС за киберсигурността[1] определя киберсигурността като „дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и други лица, засегнати от киберзаплахи“. Киберсигурността разчита на информационната сигурност, която се отнася до опазването на поверителността, целостта и наличността на информацията[2], било то във физическа или в електронна форма. Освен това защитата на мрежите и информационните системи, където се съхранява такава информация, е известна като информационно-технологична (ИТ) сигурност (вж. ***фигура 1***).

Фигура 1 — Киберсигурността е свързана с информационната сигурност и ИТ сигурността

Източник: ЕСП.

02 Като дисциплина киберсигурността включва установяване, предотвратяване, разкриване, реагиране и възстановяване от киберинциденти. Инцидентите могат да варират например от неволно разкриване на информация до атаки, които имат за цел да компрометират критични инфраструктури, и до кражба на самоличности и лични данни[3].

---

1 Регламент (ЕС) 2019/881.

2 ISO/IEC 27000:2018.

3 ЕСП, Преглед 02/2019 „Предизвикателства пред ефективната политика на ЕС в областта на киберсигурността“ (Информационно-аналитичен документ).

03 Рамката в областта на киберсигурността обхваща много елементи, включително изисквания и технически проверки по отношение на сигурността на мрежите и информационните системи, както и подходящи механизми на управление и програми за повишаване на осведомеността по въпросите на киберсигурността за персонала.

Киберсигурността в институциите, органите и агенциите на ЕС

04 Поради чувствителния характер на информацията, която те обработват, институциите, органите и агенциите на ЕС (EUIBA) са примамлива мишена за потенциални нападатели, особено за групи, които са способни да извършват високотехнологични скрити атаки („комплексни устойчиви заплахи“) за кибершпионаж и други цели[4]. Успешните кибератаки срещу EUIBA могат да имат значителни политически последици, да нанесат вреда върху цялостната репутация на ЕС и да подкопаят доверието в неговите институции.

05 Пандемията от COVID-19 принуди EUIBA, както и други организации по света, рязко да ускорят цифровата трансформация и да преминат към дистанционна работа. Това доведе до значително увеличаване на броя на потенциалните възможности за достъп за нападателите („повърхност, уязвима за атаки“) поради разширяването на периметъра на всяка организация до свързани с интернет домове и мобилни устройства, където могат да бъдат използвани нови уязвимости. Услугите за достъп от разстояние са един от най-разпространените начини, с помощта на който групите, насочващи постоянни високотехнологични заплахи към EUIBA, получават първоначален достъп до техните мрежи[5].

06 Броят на киберинцидентите се увеличава, като особено тревожна е тенденцията към драматично нарастване на сериозните инциденти, засягащи EUIBA[6]. Техният брой през 2021 г. е рекордно висок. Като сериозни инциденти се определят инцидентите, които не са систематични или незначителни. Обикновено те са свързани с използването на нови методи и технологии, а разследването им и възстановяването след тях могат да отнемат седмици или

---

[4] CERT-EU, Доклад за картината на заплахите, юни 2021 г.

[5] Пак там.

[6] Пак там.

месеци. Сериозните инциденти са се увеличили повече от десет пъти между 2018 г. и 2021 г.[7] Само през последните две години най-малко 22 отделни EUIBA са засегнати от сериозни инциденти. Пример за това е неотдавнашната кибератака срещу Европейската агенция по лекарствата, при която настъпи изтичане и манипулиране на чувствителни данни по начин, целящ да подкопае доверието във ваксините[8].

07 EUIBA представляват много разнородна група, включваща институции, агенции и различни органи. Седемте институции на ЕС са учредени с Договорите. Децентрализираните агенции на ЕС, от друга страна, са учредени с актове на вторичното законодателство и всяка една от тях представлява отделен правен субект. Агенциите имат различна правна форма: шест изпълнителни агенции на Комисията и 37 децентрализирани агенции на ЕС[9]. EUIBA включва и служби на ЕС, дипломатически корпус (Европейската служба за външна дейност), съвместни предприятия и други органи. Всяка отделна институция или орган отговаря за определянето на свои собствени изисквания за киберсигурност и мерки за сигурност.

08 За укрепването на киберсигурността на EUIBA през 2012 г. Комисията създаде екип за незабавно реагиране при компютърни инциденти на EUIBA (CERT-EU) като постоянна оперативна група. CERT-EU действа като координационен център за EUIBA за обмен на информация в областта на киберсигурността и реагиране при инциденти. Екипът си сътрудничи с други екипи за реагиране при инциденти с компютърната сигурност (CSIRTs) в държавите членки и със специализирани предприятия в областта на ИТ сигурността. Организацията и функционирането на CERT-EU понастоящем се уреждат от междуинституционален договор от 2018 г.[10] (IIA) между EUIBA, които той обслужва, известни още като „участници“ в екипа. Понастоящем участниците са 87 на брой.

09 Друг ключов орган, подкрепящ EUIBA, е Агенцията на Европейския съюз за киберсигурност (ENISA), която цели постигане на високо общо равнище на киберсигурност в ЕС. Агенцията е учредена през 2004 г. и нейната мисия е да

---

[7] Пак там.

[8] Cyberattack on EMA – update 6, 25.1.2021 г.

[9] Специален доклад 22/2020 на ЕСП „Бъдещето на агенциите на ЕС — съществува потенциал за по-голяма гъвкавост и сътрудничество“, точка 01.

[10] ОВ C 12, 13.8.2018 г., стр. 1.

повиши надеждността на продуктите, процесите и услугите, свързани с информационни и комуникационни технологии (ICT), чрез прилагането на схеми за сертифициране на киберсигурността, както и да си сътрудничи с EUIBA и държавите членки и да им помага да се подготвят за киберзаплахите. ENISA съдейства на EUIBA при изграждането на капацитет и оперативното сътрудничество.

10 Въпреки тяхната институционална независимост EUIBA са силно взаимосвързани. Те обменят информация ежедневно и споделят редица общи системи и мрежи. Слабостите в отделни EUIBA могат да изложат останалите на заплахи за сигурността, тъй като за много кибератаки са необходими повече от една стъпка за постигане на тяхната основна задача или крайна цел[11]. Успешната атака срещу по-слаба част от EUIBA може да се използва като трамплин към атакуване на останалите. EUIBA също са свързани с публични и частни организации в държавите членки и ако не са достатъчно подготвени в областта на киберсигурността, могат да изложат и тези организации на киберзаплахи.

11 Понастоящем в EUIBA не съществува правна рамка за информационна сигурност и киберсигурност. Те не са обект на най-широкообхватното законодателство на ЕС в областта на киберсигурността — Директивата от 2016 г. относно сигурността на мрежите и информационните системи (Директива за МИС)[12], както и на предложеното ѝ изменение на — Директива МИС2[13]. Не съществува и изчерпателна информация относно размера на средствата, изразходвани от EUIBA за киберсигурност.

12 През юли 2020 г. Комисията публикува съобщение относно Стратегията на ЕС за Съюза на сигурност[14] за периода 2020—2025 г.. Предвидените в нея ключови действия включват „общи правила относно сигурността на информацията и киберсигурността“ за всички EUIBA. Тази нова рамка има за цел да постави основата на силно и ефикасно оперативно сътрудничество с акцент върху ролята на CERT-EU. В Стратегията на Европейския съюз за киберсигурност за цифровото

---

[11] ENISA, Threat Landscape 2020, Анализ на заплахите по сектори/тематична област.

[12] Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

[13] Предложение за Директива относно мерките за високо общо ниво на киберсигурност в Съюза.

[14] COM(2020) 605 final.

десетилетие[15], публикувана през декември 2020 г., Комисията пое ангажимент да предложи регламент относно общи правила за киберсигурност за всички EUIBA. Предложено е и установяването на нова правна уредба за CERT-EU, която да укрепи неговия мандат и да увеличи финансирането му.

[15] JOIN(2020) 18 final.

Обхват и подход на одита

13 Предвид факта, че броят на кибератаките върху EUIBA рязко се увеличава, а слабостите в една от организациите може да изложат и останалите на заплахи за сигурността им, целта на настоящия одит беше да се определи дали EUIBA като цяло разполагат с подходящи механизми за защита от киберзаплахи. За да отговорим на този основен одитен въпрос, разгледахме три подвъпроса:

1) Приети ли са ключови практики в областта на киберсигурността в EUIBA?

2) Съществува ли ефикасно сътрудничество между EUIBA в областта на киберсигурността?

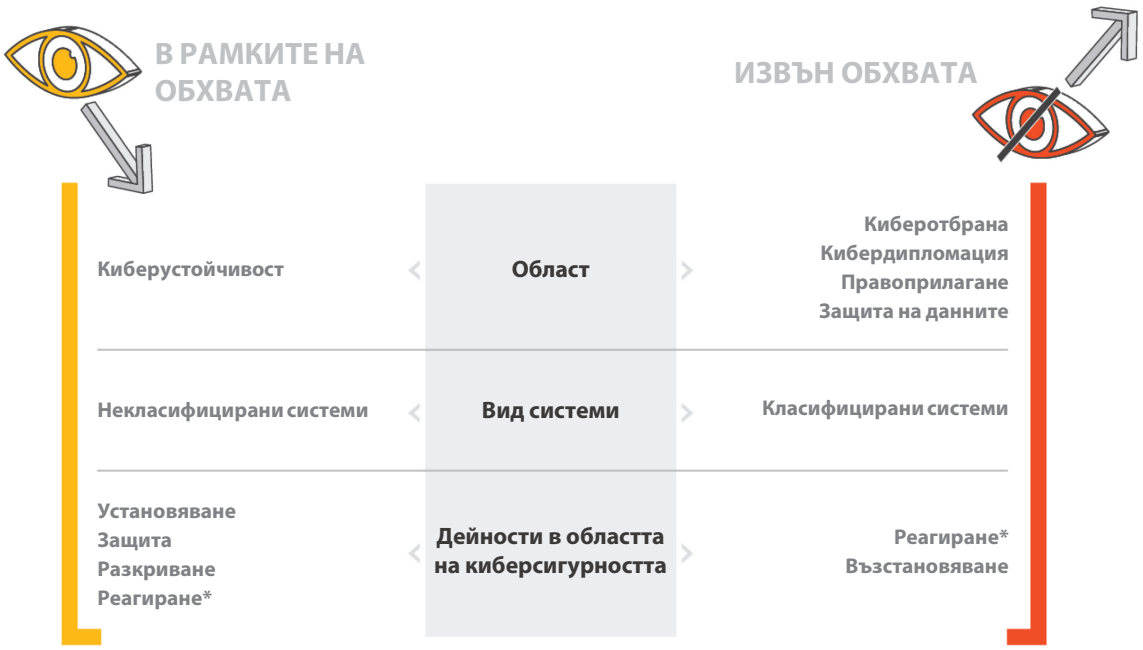
3) Осигуряват ли ENISA и CERT-EU адекватна подкрепа на EUIBA в областта на киберсигурността?

14 Моментът на провеждане на одита е съгласуван със Стратегията на ЕС за Съюза на сигурност. Чрез оценката на настоящите договорености на EUIBA в областта на киберсигурността ЕСП цели да определи областите, в които има нужда от подобрения, за да може Комисията да ги вземе предвид при изготвянето на законодателно предложение за задължителни общи правила за киберсигурност за всички EUIBA.

15 Одитът обхвана разработките и инициативите в областта на киберсигурността от януари 2018 г. (когато е сключен междуинституционалният договор на CERT-EU) до октомври 2021 г.

16 ЕСП ограничи обхвата на одита до киберустойчивостта и некласифицираните системи. Основно внимание беше обърнато на аспектите на подготвеността (дейности за „установяване, защита, разкриване“). Извън обхвата на одита останаха дейностите по реагиране и възстановяване. Въпреки това ЕСП разгледа някои организационни елементи на реагирането при инциденти. Извън обхвата на одита са и аспектите, свързани със защитата на данните, правоприлагането, киберотбраната и кибердипломацията (вж. ***фигура 2***).

Фигура 2 — Обхват на одита



** ЕСП разгледа само някои организационни аспекти на реагирането при инциденти. Останалите аспекти са извън обхвата на одита.*

Източник: ЕСП.

17 Одитните констатации на ЕСП се основават на обширен анализ на наличната документация и проведени събеседвания. Извършихме проучване за самооценка, включващо 65 EUIBA, чрез което да съберем информация относно механизмите, които те прилагат в областта на киберсигурността, и техните виждания по въпросите на междуинституционалното сътрудничество. В проучването бяха включени всички EUIBA, които попадат в обхвата на одитните правомощия на ЕСП и които управляват своя собствена ИТ инфраструктура, както и нашата собствена институция. Между тях има институции, децентрализирани агенции, съвместни предприятия и други органи. Извършихме проучване и на граждански мисии, които са временни автономни субекти, финансирани от бюджета на ЕС и независими от гледна точка на ИТ. В ***приложение I*** е представен пълен списък на проучените EUIBA. Европейският омбудсман и Европейският надзорен орган по защита на данните не са включени в обхвата на този одит.

18 Проучването получи отговор от 100 % от респондентите и послужи като начало за допълнителен анализ. Освен това беше формирана извадка от седем EUIBA, която отразява тяхната хетерогенност, като получените отговори бяха проследени допълнително с провеждане на събеседвания и искания за предоставяне на документи. ЕСП взе предвид критерии за подбор като правно база, размер (от гледна точка на брой служители и бюджет) и сектор. Извадката от EUIBA включва Европейската комисия, Европейския парламент, Агенцията на

Европейския съюз за киберсигурност (ENISA), Европейския банков орган (EBA), Европейската агенция за морска безопасност (EMSA), Консултативната мисия на ЕС в Украйна (EUAM Ukraine) и Съвместното предприятие за изпълнение на инициативата за иновативни лекарства (IMI JU).

19 Бяха проведени и видеоконференции със CERT-EU, Консултативния комитет по въпросите на ИКТ на Мрежата на агенциите на ЕС (ICTAC), Междуинституционалния комитет за цифрова трансформация (ICDT) и други заинтересовани страни.

Констатации и оценки

EUIBA имат много различни равнища на зрялост в областта на киберсигурността и невинаги се съобразяват с добрите практики

20 В този раздел се разглеждат отделните механизми и рамки в областта на киберсигурността на EUIBA. ЕСП разгледа доколко те подхождат последователно и адекватно към киберсигурността от гледна точка на управлението на ИТ сигурността, управлението на риска, разпределението на ресурси, обучението за повишаване на осведомеността, механизмите за контрол и независимата проверка.

Управлението на ИТ сигурността в EUIBA често не е добре развито, а оценките на риска не са изчерпателни

В много EUIBA се наблюдават пропуски в управлението на ИТ сигурността

21 Доброто управление е от основно значение за изграждането на ефективна рамка за сигурност на информацията и ИТ системите, тъй като то очертава целите на организацията и дава насоки чрез определяне на приоритети и вземане на решения. Според Асоциацията за одит и контрол на информационни системи (ISACA)[16] рамката за управление на ИТ сигурността следва най-общо да включва няколко елемента:

- цялостна стратегия за сигурност, неразривно свързана с целите на дейността;
- ръководни политики за сигурност, които да разглеждат всеки аспект на стратегията, механизмите за контрол и нормативната уредба;
- пълен набор от стандарти за всяка политика, описващи операционните стъпки, които следва да бъдат предприети за постигане на съответствие с политиката;

[16] ISACA, Наръчник за преглед на сертифициран одитор на информационни системи, 2019 г.

- институционализирани процеси за мониторинг, с които да се осигури съответствието и да се предостави обратна информация относно ефективността;

- ефективна организационна структура без конфликт на интереси.

22 В много EUIBA ЕСП установи пропуски в управлението на ИТ сигурността. Само 58 % от EUIBA (38 от общо 65) разполагат със стратегия за ИТ сигурност или най-малко с план за ИТ сигурност, одобрен на ниво управителен съвет/висше ръководство. Разбивката по вид EUIBA показва, че гражданските мисии и децентрализираните агенции (които заедно съставляват 71 % от проучените EUIBA) отчитат най-ниските проценти (вж. ***таблица 1***). Липсата на стратегия за ИТ сигурност или план за ИТ сигурност, който да е одобрен на ниво висше ръководство, поражда риск от това висшето ръководство да не е запознато с въпросите, свързани със сигурността, или да не им отдава достатъчно приоритет.

Таблица 1 — Процент от EUIBA, които разполагат със стратегия или план за ИТ сигурност, одобрен от висшето ръководство

Разбивка по численост на персонала

По-малко от 100 служители (22 EUIBA)	Между 100 и 249 служители (17 EUIBA)	Между 250 и 1 000 служители (16 EUIBA)	> 1 000 служители (10 EUIBA)
45 %	53 %	69 %	80 %

Разбивка по вид EUIBA

Децентрали-зирани агенции (35 EUIBA)	Граждански мисии (11 EUIBA)	Организации (4 EUIBA)	Институции (6 EUIBA)	Съвместни предприятия (9 EUIBA)
45 %	56 %	75 %	83 %	89 %

Източник: Проучване на ЕСП.

23 ЕСП разгледа стратегиите/плановете за ИТ сигурност, предоставени от седемте EUIBA от извадката (вж. точка ***18***). Установихме, че стратегиите на EUIBA са сравнително добре съвместени с целите на тяхната дейност. Например стратегията за ИТ сигурност на Комисията обхваща частта от Стратегията на Европейската комисия в областта на цифровите технологии[17], касаеща ИТ сигурността, и е предназначена да подкрепя нейната пътна карта и цели. Само

[17] Съобщение до Комисията, Стратегия на Европейската комисия в областта на цифровите технологии: Цифрово трансформирана, ориентирана към потребителя и основана на данни Комисия, C(2018) 7118 final, 21.11.2018 г.

три EUIBA от нашата извадка обаче разполагат с конкретни цели и график за тяхното постигане, включени в техните стратегии/планове за ИТ сигурност.

24 Политиките за сигурност определят правилата и процедурите, които лицата, използващи или управляващи информация или ИТ ресурси, следва да спазват. Те спомагат за ограничаване на рисковете за киберсигурността и за предоставят насоки за това какво следва да се предприеме в случай на инциденти. Установихме, че 78 % от EUIBA разполагат с официална политика за информационна сигурност, а само 60 % разполагат с официални политики за ИТ сигурност (вж. ***фигура 1*** за определенията за информационна и ИТ сигурност). Установихме още, че четири от седемте EUIBA в нашата извадка разполагат с политики за сигурност, които са в съответствие с техните стратегии за ИТ сигурност. В три от тези четири EUIBA обаче политиките за ИТ сигурност са само частично допълнени от актуализирани подробни стандарти за сигурност, описващи практическите стъпки за изпълнение на политиките. Липсата на официални стандарти за сигурност увеличава риска от това въпросите, свързани с ИТ сигурността, да не бъдат разглеждани правилно и последователно в една и съща институция или орган. Освен това става по-трудно да бъде измерено доколко организацията следва своята политика за ИТ сигурност. От седемте EUIBA от извадката само Комисията разполага със структурирани процедури за мониторинг на спазването на нейните политики и стандарти за ИТ сигурност, макар и те да се използват само от ограничен брой генерални дирекции (ГД) (вж. ***каре 1***).

Каре 1

Съответствие с изискванията за ИТ сигурност в Комисията

В съответствие с децентрализираното управление на ИТ на Комисията ръководителят на всяка ГД е собственикът на услугата, който е отговорен за съответствието на системите със стандартите за ИТ сигурност. Генерална дирекция „Информатика“ (DG DIGIT) и Генерална дирекция „Човешки ресурси и сигурност“ (DG HR) извършват наблюдение върху и улесняват прилагането на практики за управление на съответствието с изискванията. DG DIGIT е създала инструмент (известен като „GRC“), който позволява на генералните дирекции да измерват и докладват относно степента, в която се спазват изискванията на политиките за контрол на ИТ сигурността.

580-те механизми за контрол са разпределени в три групи: общи механизми за контрол (основно на управлението), механизми за контрол, специфични за конкретната ГД, и механизми за контрол, специфични за системата. Инструментът е в действие, но досега се използва само от пет ГД. Поради това DG DIGIT не разполага с общ поглед върху съответствието в Комисията като цяло. Съветът по информационни технологии и киберсигурност (ITCB) на Комисията обаче може да поиска от DG DIGIT да проучи съответствието с конкретен стандарт (напр. многофакторното установяване на автентичността през 2021 г.) и може да изготвя становища и препоръки с незадължителен характер, а когато става дума за критични рискове — и формални изисквания.

25 Друг важен елемент от доброто управление на киберсигурността е назначаването на Главен служител по въпросите на информационната сигурност (CISO). Макар и не изрично изискуемо съгласно набора от стандарти ISO 27000[18], наличието на CISO или на еквивалентна длъжност става широкоразпространена практика сред организациите и е част от насоките на ISACA. Обикновено CISO носи цялостна отговорност за програмите за информационна и ИТ сигурност на организацията. С цел избягване на конфликт на интереси CISO следва да разполага с определено ниво на независимост от ИТ функцията/отдела[19].

26 Съгласно нашето проучване в 60 % от EUIBA не е назначен независим CISO или лице на еквивалентна длъжност. Дори когато са назначени CISO (или служител с еквивалентни функции), техните роли се различават много по своя характер и техните функции се възприемат различно в различните EUIBA. Особено в малките и средните EUIBA, CISO обикновено се свързват с упражняването на по-

[18] Стандарт ISO/IEC 27000:2018, глава 5.

[19] COBIT 5 за информационна сигурност, раздел 4.2.

оперативни функции, които не са функционално независими от ИТ отдела. Това може да ограничи автономността на CISO за изпълнението на техните приоритети в областта на сигурността. Понастоящем ENISA разработва рамка на ЕС за уменията в областта на киберсигурността, която, наред с другото, има за цел създаването на общо разбиране на функциите, компетенциите и уменията.

Извършваните от EUIBA оценки на риска, свързан с ИТ сигурността, в по-голямата си част не обхващат цялата им ИТ среда

27 Всички международни стандарти за ИТ сигурност подчертават важността от установяването на подходящ метод за оценка и справяне с рискове, свързани със сигурността, които засягат ИТ системите и съхраняваните в тях данни. Оценките на риска следва да бъдат извършвани периодично, за да могат да се разглеждат промените, настъпили в изискванията за информационна сигурност на организацията и в рисковете, пред които тя се изправя[20]. Оценките следва да бъдат последвани от план за намаляване на риска (или план за ИТ сигурността).

28 По-голямата част от EUIBA, които отговориха на проучването (58 от общо 65) посочват, че при извършването на оценки на риска на техните ИТ системи те следват определена рамка или методология. Липсва обаче обща методология за всички EUIBA. Най-малко 26 EUIBA използват частично или изцяло методологиите, разработени от Комисията; по-специално 31 % от EUIBA използват методологията за управление на риска, свързан с ИТ сигурността от 2018 г. (ITSRM2). Останалите следват методологии, основаващи се на добре известни отраслови стандарти (например ISO27001, ISO27005, рамката в областта на киберсигурността на Националния институт за стандарти и технологии (NIST-CSF) или механизмите за

[20] Вж. например ISO/IEC 27000:2018, раздел 4.5.

контрол на Центъра за интернет сигурност (CIS) или използват други вътрешни методологии.

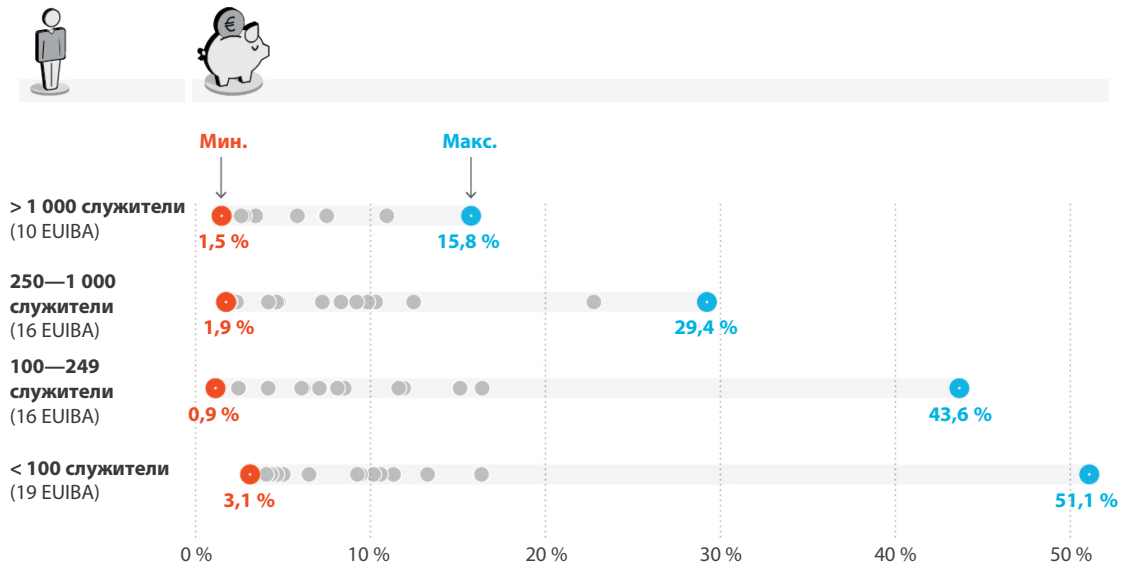
29 От седемте EUIBA, включени в извадката, само две извършват цялостни оценки на риска, обхващащи цялата им ИТ среда (т.е. всички техни ИТ системи). Повечето от тях извършват индивидуални оценки на риска само за техните най-важни ИТ системи. ЕСП идентифицира няколко примера за оценки на риска, извършени преди внедряването на нови системи. Не открихме обаче данни за последващи оценки на риска, свързани например с последващи промени в системите/инфраструктурата.

EUIBA не разполагат с последователен подход към киберсигурността и невинаги са налице основни механизми за контрол

Има значителна разлика в разпределението на ресурси за киберсигурност сред EUIBA

30 В извършеното от ЕСП проучване EUIBA трябваше да предоставят информация за общите им разходи за ИТ през 2020 г. и оценка на сумата, изразходвана за киберсигурност. Данните ни показват значителни разлики в процента на разходите за ИТ, които отделните EUIBA разпределят за киберсигурност. Такава е ситуацията дори и сред EUIBA със сходна численост на персонала. Както е показано във ***фигура 3***, различията обикновено са особено големи сред онези EUIBA, които имат по-малко персонал.

Фигура 3 — Разходи за киберсигурност като процент от общите разходи за ИТ (EUIBA, групирани по численост на персонала)



Бележка: Четири EUIBA не предоставиха данни за разходите, свързани с киберсигурност.

Източник: Проучване на ЕСП.

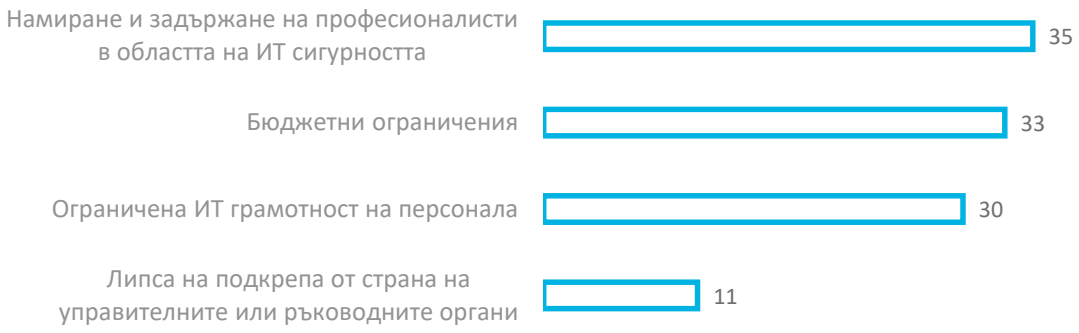
31 Трудно е да бъде изчислено оптималното ниво на разходите за киберсигурност в абсолютни стойности. То зависи от много фактори, например каква е повърхността, уязвима за атаки, в дадена организация, чувствителността на данните, които тя обработва, нейния профил на риска и склонност към поемане на риск, както и секторни нормативни/регулаторни изисквания. Данните ни обаче подчертават, че различията са значителни, а причините за това — невинаги очевидни. Някои EUIBA са имали значително по-ниски разходи за киберсигурност в сравнение с организациите с подобни размери, което може да е показател за отделяне на недостатъчно средства, ако те са изложени на сходни заплахи и рискове.

32 По-голямата част от EUIBA са с малък до среден размер от гледна точка както на числеността на персонала, така и на размера на разходите за ИТ, като две трети от EUIBA имат по-малко от 350 служители. Персоналът на най-малката EUIBA се състои само от 15 служители. Управлението на киберсигурността за по-малките EUIBA е по-сложно и изисква по-големи ресурси. В повечето случаи те не могат да се възползват от икономии от мащаба и не разполагат с достатъчно вътрешни експертни познания. Въз основа на нашето проучване и интервюта беше установено, че най-големите институции като Комисията и Европейския парламент разполагат с екипи от експерти, които управляват киберсигурността на пълно работно време. Най-малките EUIBA обаче, в които персоналът и ресурсите са особено ограничени, не разполагат с експерти, а киберсигурността се

управлява от служители на непълно работно време с познания и професионален опит в областта на ИТ. Тъй като EUIBA са силно взаимосвързани, това поражда по-голям риск (вж. също точка ***10***).

33 В нашето проучване EUIBA бяха запитани кои са най-големите предизвикателства, пред които са били изправени при прилагането на ефективни политики в областта на киберсигурността в техните организации (вж. ***фигура 4***). Най-голямото предизвикателство е това, че експертите по киберсигурност представляват ограничен ресурс и много EUIBA срещат проблеми да ги привлекат, което се дължи на конкуренцията както от страна на частния сектор, така и от други EUIBA. Между често срещаните проблеми са продължителните процедури по набиране на персонал, неконкурентните договорни условия и липсата на привлекателни перспективи за професионално развитие. Недостигът на специализирани кадри поражда значителен риск за ефективните действия, свързани с киберсигурността.

Фигура 4 — Предизвикателства при изпълнението на ефективни политики в областта на киберсигурността в EUIBA (може да бъде избран повече от един фактор)



Източник: Проучване на ЕСП.

По-голямата част от EUIBA предлагат обучения под различна форма за повишаване на осведомеността в областта на киберсигурността, но те не са систематични или добре насочени

34 Възползването от уязвимостите в системите и устройствата не е единственият начин, по който потенциалните нападатели могат да предизвикат вреда. Те могат и да принудят потребителите да разкрият чувствителна информация или да изтеглят зловреден софтуер, например чрез фишинг или социално инженерство. Служителите са част от защитата от първа линия за всяка организация. Следователно осведомеността в областта на киберсигурността и

обучителните програми са основен елемент от ефективната рамка в областта на киберсигурността.

35 По-голямата част от проучените EUIBA (95 %) предоставят някаква форма на обучение за повишаване на общата осведоменост в областта на киберсигурността за целия персонал, с изключение на три. Само 41 % от EUIBA обаче организират специфични обучения или семинари за повишаване на осведомеността за служителите на ръководни длъжности и само 29 % предоставят на служителите, които отговарят за ръководството на ИТ системите с чувствителна информация, задължително обучение в областта на киберсигурността. Осведомеността и ангажираността на ръководството са изключително важни за ефективното управление на киберсигурността. От единадесетте EUIBA, които отбелязват, че липсата на подкрепа от страна на ръководството е предизвикателство за ефективната киберсигурност, само три предоставят обучение за повишаване на осведомеността на своето ръководство. Текущо обучение в областта на киберсигурността за ИТ служителите и специалистите по ИТ сигурност се предлага съответно от 58 % и 51 % от EUIBA.

36 Не всички EUIBA разполагат с механизми за наблюдение на присъствието на служителите на обученията за повишаване на осведомеността и на последващата промяна в тяхната осведоменост и поведение. Особено в по-малките организации дейностите за повишаване на осведомеността в областта на киберсигурността могат да бъдат извършвани в контекста на неформални срещи на персонала. Основният начин, по който организациите могат да определят степента на осведомеността на служителите си, е като периодично провеждат проверки на тяхното поведение, включително чрез проучвания за зрялост или фишинг учения. През последните пет години 55 % от EUIBA са организирали една или повече симулирани фишинг кампании (или подобни учения). Като се има предвид, че фишингът е една от основните заплахи, пред които е изправен персоналът в публичната администрация[21], тези учения са важен инструмент за обучение на служителите и повишаване на осведомеността. ЕСП установи, че действията на Комисията за повишаване на осведомеността в областта на киберсигурността са добра практика и са достъпни за други заинтересовани EUIBA (вж. ***каре 2***).

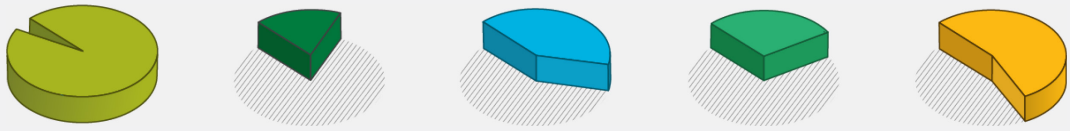
[21] ENISA, Thread Landscape 2020, Анализ на заплахите по сектори/тематика.

Каре 2

Обучение за повишаване на осведомеността в областта на киберсигурността в Комисията

Комисията разполага със специален екип „Cyber Aware“ в ГД „Информатика“, който ръководи корпоративната програма за повишаване на осведомеността в областта на киберсигурността. Програмата се управлява и ръководи съвместно с ГД „Човешки ресурси и сигурност“, Генералния секретариат, Генерална дирекция „Съобщителни мрежи, съдържание и технологии“ и CERT-EU. Качеството на обучението е високо и в много случаи — с междуинституционален обхват. Учебните дейности се рекламират чрез Учебен бюлетин (Learning Bulletin), който достига до приблизително 65 000 служители на ЕС. Чрез платформата „Cyber Aware“ през последните пет години Комисията е организирала 15 фишинг учения, а неотдавна е провела първото такова учение за цялата Комисия.

ОСНОВНИ ЦИФРИ: **Обучение за осведоменост в областта на киберсигурността в EUIBA**



95 %
предлагат някаква форма на **обучение за повишаване на общата осведоменост** на персонала

19 %
не информират/ обучават систематично новопостъпили служители

41 %
провеждат специфични **обучения за ръководството**

29 %
провеждат **задължително обучение** за служителите, отговорни за управлението на ИТ системите, които съдържат чувствителна информация

55 %
са извършили проверка на персонала със **симулиран фишинг**

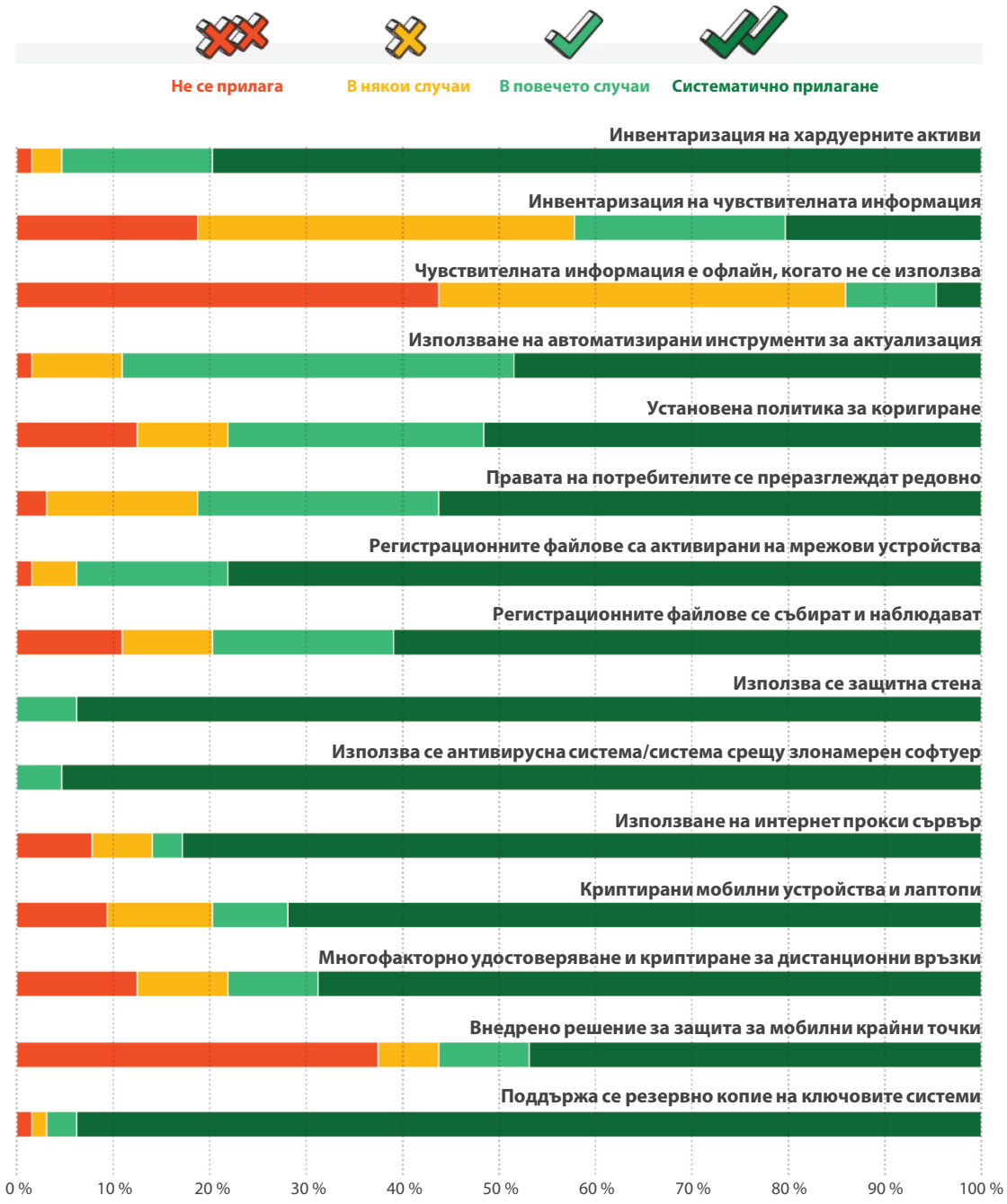
Някои основни механизми за контрол невинаги се прилагат или не се въвеждат като стандарти

37 ЕСП поиска от EUIBA да извършат самооценка на това как прилагат няколко избрани основни механизми за контрол[22]. Подбрахме набор от най-добри практики, които дори и по-малките организации биха могли да прилагат разумно[23]. Резултатите са представени на ***фигура 5***. По-голямата част от разгледаните EUIBA прилагат тези основни механизми за контрол. В някои области обаче за поне 20 % от EUIBA механизмите за контрол изглеждат недостатъчни или ограничени.

[22] Набор от механизми за контрол, извлечени от механизмите за контрол на CIS 7.1 — рамка на най-добрите практики, специално подбрани от Центъра за интернет сигурност.

[23] Група за прилагане 1 (IG1) на механизмите за контрол на CIS.

Фигура 5 — Прилагане на основни механизми за контрол в EUIBA (резултати от самооценката)



Източник: Проучване на ЕСП.

38 ЕСП поиска от седемте EUIBA, включени в извадката, да представят придружаващи документи и съответните стандарти/политики за всеки механизъм за контрол, деклариран от тяхна страна като внедрен. Такива документи получихме за 62 % от механизмите за контрол. Както беше изяснено по време на проведените интервюта, в някои случаи механизмите за технически контрол са въведени, но без да бъдат официално формулирани като актуални стандарти или

политики, което повишава риска от това въпросите, свързани с ИТ сигурността, да не бъдат разглеждани последователно в една и съща организация (вж. също точка ***24***).

Механизмите в областта на киберсигурността в няколко EUIBA не са обект на редовна независима проверка

39 Съгласно ISACA[24] вътрешният одит е една от трите основни линии на защита в организацията, като другите две са управлението и управлението на риска. Вътрешните одити допринасят за подобряване на управлението на информационната и ИТ сигурността. ЕСП проучи колко често EUIBA извършват независими проверки на своята рамка за ИТ сигурност чрез вътрешни и външни одити, както и чрез активна проверка на механизмите за киберотбрана.

40 Службата за вътрешен одит на Комисията (IAS) е отговорна, наред с другото, за извършването на ИТ одити в Комисията и децентрализираните агенции, съвместните предприятия и Европейската служба за външна дейност. Правомощията на IAS обхващат 46 (70 %) от 65-те EUIBA, разгледани от ЕСП, като през последните пет години тя е извършила одити, свързани с ИТ сигурността, на 6 различни EUIBA. Освен това ГД „Човешки ресурси и сигурност“ има правомощия да извършва проверки на ИТ сигурността, които обхващат аспекти от техническата информационна сигурност[25]. Седем от останалите EUIBA докладват, че собствените им служби за вътрешен одит обхващат и аспектите, свързани с ИТ, но за дванадесет EUIBA отговорите на нашето проучване не са достатъчни, за да се определи дали те разполагат с такъв капацитет за вътрешен одит.

41 Външните одити на ИТ сигурността, извършени от независими дружества, са друг начин за извършване на независими проверки. Независимо от бързо променящата се ситуация, свързана с киберсигурността, между началото на 2015 г. и първото тримесечие на 2021 г. 34 % от EUIBA не са били обект на вътрешен или външен одит на ИТ сигурността. Разбивката на тази цифра по вид EUIBA показва, че от 2015 г. насам в 75 % от органите на ЕС, 66 % от съвместните предприятия и 45 % от гражданските мисии не е провеждан вътрешен или външен одит на ИТ сигурността.

---

[24] ISACA, Одит на киберсигурността: Оценка на механизмите за контрол на риска и одита, 2017 г.

[25] Решение 46/2017 относно сигурността на комуникационните и информационните системи в Европейската комисия.

42 Освен вътрешните и външните одити друг начин, чрез който организациите могат да получат увереност по отношение на тяхната рамка за ИТ сигурност, е активната проверка на механизмите за киберзащита с цел идентифициране на уязвимостите. Един от методите за това са проверките за проникване (известни още като „етични хакерски атаки“), състоящи се от разрешени симулирани кибератаки срещу отделните компютърни системи. В отговор на нашето проучване 69 % от EUIBA заявяват, че са извършили поне една проверка за проникване през последните пет години. В 45 % от случаите CERT-EU е органът, който извършва проверките за проникване.

43 Тестовите кибератаки с цел подобряване на сигурността са друг начин за проверка на киберзащитата чрез симулирани атаки, като се прилагат актуални техники от реални атаки. Те са по-сложни и всеобхватни в сравнение с проверките за проникване, тъй като включват множество системи и потенциални пътища за атака. EUIBA извършват такива проверки по-рядко: 46 % от EUIBA докладват за поне едно тестова кибератака с цел подобряване на сигурността през последните пет години. CERT-EU е провел 75 % от тези атаки. За подготовката и провеждането на тестови кибератаки с цел подобряване на сигурността се изисква значителен обем от работа и понастоящем CERT-EU има възможност да провежда не повече от пет до шест такива учения всяка година.

44 Като изключим две неотдавна учредени EUIBA, 16 (25 %) от проучените EUIBA не са извършили проверки за проникване или тестови кибератаки с цел подобряване на сигурността през последните пет години. Общо седем EUIBA (10 %) не са били обект на каквато и да било форма на независима проверка на техните правила в областта на ИТ сигурността: едно съвместно предприятие, една децентрализирана агенция и пет граждански мисии.

ОСНОВНИ ЦИФРИ: **Независима проверка на ИТ сигурността в EUIBA през последните 5 години**

66 %
от EUIBA са били **обект** на най-малко **един вътрешен или външен одит**, свързан с ИТ сигурността

69 %
са извършили поне **една проверка за проникване**

46 %
са извършили поне **една тестова кибератака с цел подобряване на сигурността**

10 %
не са **били обект** на каквато и да било форма на **независим одит или проверка** на ИТ сигурността

EUIBA разполагат с установени механизми за сътрудничество, но са налице слабости

45 В този раздел се разглеждат участващите страни и комитети, създадени за насърчаване на сътрудничеството между EUIBA в областта на киберсигурността, както и междуинституционалните договорености за управление и координация. По-конкретно ЕСП проучи двама междуинституционални участници — ENISA и CERT-EU, както и два междуинституционални комитета — Междуинституционалния комитет за цифрова трансформация (ICDT), в частност неговата подгрупа по киберсигурност (CSSG), и Консултативния комитет по въпросите на информационните и комуникационните технологии (ICTAC). Извършихме оценка и на това доколко те предоставят възможност за полезни взаимодействия с цел повишаване на подготвеността на EUIBA в областта на киберсигурността.

Налице е формализирана структура за координиране на дейностите на ENISA, макар и с известни проблеми, свързани с управлението

46 ICDT и ICTAC са двата основни комитета, които насърчават сътрудничеството по въпросите на ИТ сред EUIBA. ICDT представлява форум за засилване на обмена на информация и сътрудничеството, съставен от ръководителите на ИТ звената в институциите и органите на ЕС. Комитетът разполага с подгрупа по киберсигурността (ICDT CSSG), която докладва на ICDT и може да прави препоръки за вземане на решения по конкретни въпроси. ICTAC, от друга страна, е подгрупа на Мрежата на агенциите на ЕС (EUAN) — неформална мрежа, създадена от ръководителите на агенциите на ЕС, която се фокусира върху сътрудничеството между агенциите и съвместните предприятия. Както ICDT, така и ICTAC имат ясно определени, взаимнодопълващи се роли: ICTAC обхваща децентрализираните

агенции и съвместните предприятия, а ICDT обхваща институциите и органите. По своя характер ICDT и ICTAC са по-скоро неформални консултативни групи и форуми за обмен на информация и добри практики. Допълнителна информация относно междуинституционалните комитети е представена в ***приложение II***.

EUIBA невинаги са добре представени в съответните форуми

47 Макар и структурите за представителство да са ясни, не всички EUIBA считат, че тяхното действително представителство е достатъчно. Когато в нашето проучване бяха помолени да дадат мнението си относно твърдението „Междуинституционалните форуми обръщат достатъчно внимание на моите нужди и моята организация е подходящо представена в органите за вземане на решения“ 42 % от EUIBA изразиха несъгласието си с него. Някои от най-малките организации считат, че не разполагат с достатъчно ресурси, за да могат да участват активно в междуинституционалните форуми.

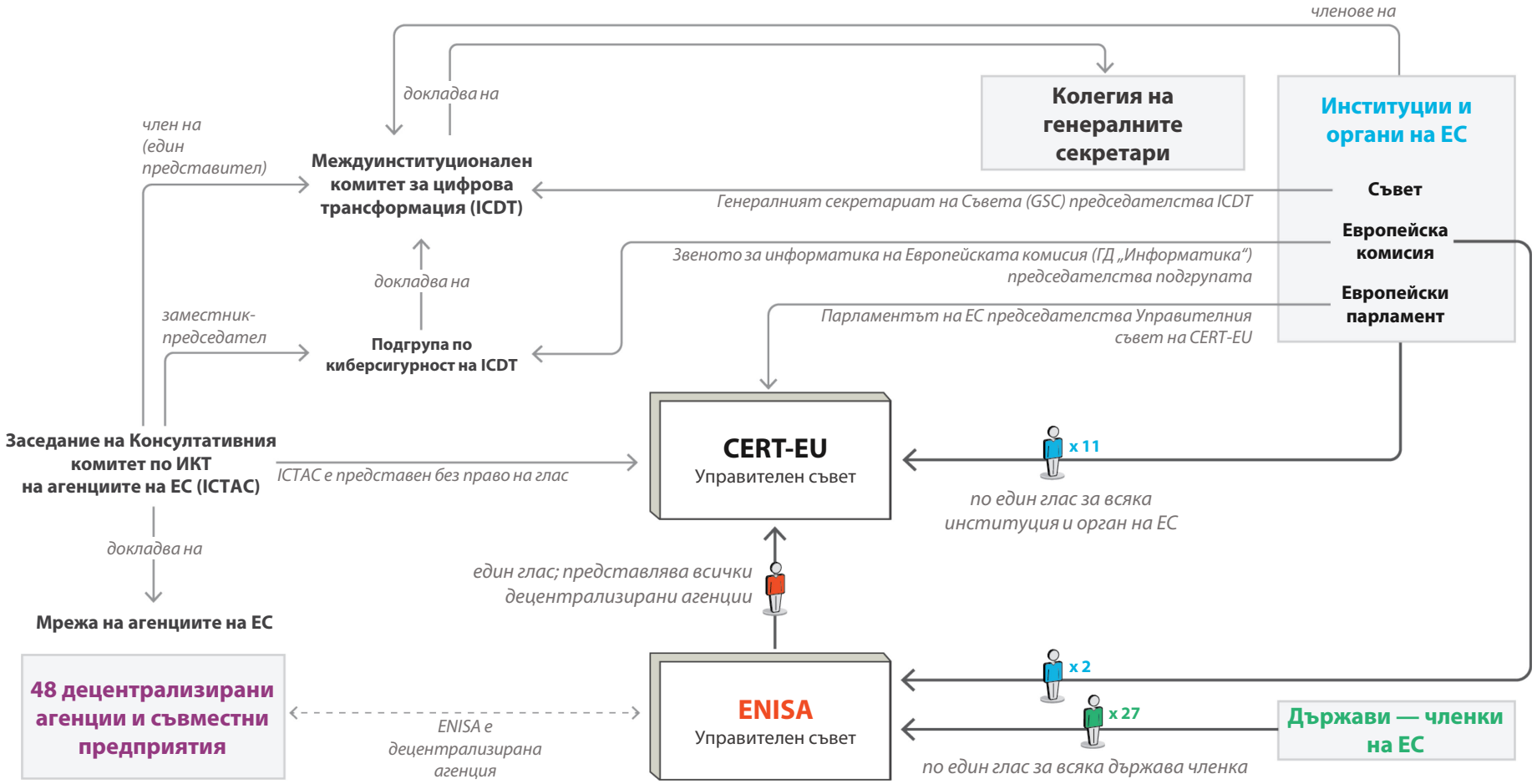
48 Управителният съвет на CERT-EU — неговият основен орган за вземане на решения, също като цяло не е представителен за участниците в екипа. CERT-EU предоставя услуги на 87 EUIBA и 3 други организации. Неговият управителен съвет обаче включва само представителите на 11-те страни по междуинституционалното споразумение (седемте институции на ЕС, Европейската служба за външна дейност, Икономическият и социален комитет, Комитетът на регионите и Европейската инвестиционна банка), както и представител на ENISA, като всеки един от тях има право на един глас[26].

49 Повече от половината от участниците в CERT-EU са децентрализирани агенции и съвместни предприятия на ЕС, които заедно разполагат с приблизително 12 000 служители. Техните интереси официално се представляват в управителния съвет на CERT-EU от ENISA. Правомощията на ENISA да представлява агенциите и съвместните предприятия обаче е са слаби, тъй като нейният представител не е директно определен или избран от тях. На практика мненията на децентрализираните агенции и на съвместните предприятия се изразяват на заседанията на управителния съвет от представител на ICTAC, който може да присъства, за да съдейства на ENISA в нейната задача да представлява агенциите. Макар че дава гласност на мненията и интересите на 48 EUIBA, представителят на ICTAC понастоящем няма официално място или глас в управителния съвет. През април 2021 г. ICTAC отправи до председателя на управителния съвет на CERT-EU формално искане за предоставяне на право на

[26] Член 7 от Междуинституционалното споразумение (IIA), подписано на 20.12.2017 г.

глас в съвета. Към момента на изготвяне на доклада това искане все още не е уважено. Общ преглед на представителството на EUIBA в органите за вземане на решения е представен на ***фигура 6***.

Фигура 6 — Общ преглед на управлението на киберсигурността и представителството в съветите и комитетите за вземане на решения



Източник: ЕСП.

50 Междуинституционалното управление на киберсигурността на EUIBA е фрагментирано и понастоящем нито един субект няма цялостен поглед върху зрелостта на EUIBA по отношение на киберсигурността, нито правомощията да поеме водещата роля или да наложи общи задължителни правила. Както ENISA, така и CERT-EU могат единствено да „подкрепят“ и да „съдействат“ на EUIBA. Съответните комитети не разполагат с правомощия за вземане на решения и могат единствено да изготвят препоръки за EUIBA. Освен това за една пета от разгледаните EUIBA не е ясно към кого могат да се обърнат за конкретна услуга, инструмент или решение.

Между ключовите участници са сключени меморандуми за разбирателство, които обаче досега не са дали конкретни резултати

51 През май 2018 г. е подписан меморандум за разбирателство (MoU) между ENISA, CERT-EU, Европейския център за борба с киберпрестъпността към Европол (EC3) и Европейската агенция по отбрана (EDA). Той се фокусира върху пет области на сътрудничество: обмен на информация, образование и обучение, учения в областта на киберсигурността, техническо сътрудничество и стратегически и административни въпроси. Макар и този меморандум да може да помогне за избягване на дублирания посредством обща работна програма, ЕСП не откри данни, че това е довело до конкретни резултати и съвместни действия.

52 Актът за киберсигурността (CSA), който влезе в сила през юни 2019 г., предвижда подписването на ново и специфично споразумение за сътрудничество между CERT-EU и ENISA. Следва да се отбележи, че подписването на меморандума за разбирателство е отнело над година и половина до приключването му през февруари 2021 г. Целта на този меморандум е да установи структурирано сътрудничество между CERT-EU и ENISA. Той определя областите, в които те да си сътрудничат (изграждане на капацитет, оперативно сътрудничество и обмен на знания и информация), и определя широко разграничение на ролите между тях: CERT-EU поема инициативата да съдейства на EUIBA, а ENISA следва да допринася за това. Меморандумът не определя практическите договорености, тъй като същите са посочени в годишния план за сътрудничество. Първият годишен план за сътрудничество за 2021 г. е приет от управителния съвет на ENISA през юли 2021 г. и от управителния съвет на CERT-EU през септември 2021 г. Следователно е твърде рано в рамките на одита да се направи оценка на това дали този план е довел до видим резултат.

53 Като се има предвид, че и двата меморандума, посочени в точки ***51*** и ***52***, имат общи цели и области на сътрудничество, например обучение, учения или обмен на информация, съществува риск от припокриване и дублиране.

Потенциалните полезни взаимодействия чрез сътрудничество все още не се използват изцяло

Стъпки напред за постигане на полезни взаимодействия

54 Работните програми на комитетите ICTAC и ICDT CSSG определят актуалните области, в които може да бъде постигнато повишаване на ефективността чрез сътрудничество. Между практическите примери за инициативите, които позволяват на EUIBA да се възползват от полезните взаимодействия, са:

- междуинституционални рамкови договори;
- общ център за възстановяване при бедствия, поддържан от 2019 г. насам от Службата на Европейския съюз за интелектуална собственост (EUIPO) за децентрализираните агенции, който позволява разходите да бъдат намалени с най-малко 20 % спрямо пазарните цени (девет агенции са приели това решение за възстановяване при бедствия);
- споразумения между шест съвместни предприятия, намиращи се в същата сграда, да споделят обща инфраструктура и обща рамка за ИТ сигурност (от 2014 г. насам).

55 Друг важен пример е „GovSec“ — система, която помага на EUIBA да извършват оценки на риска с оглед приемането на решения „в облак“. Според резултатите от нашето проучване 75 % от EUIBA вече използват някои публични платформи „в облак“, а няколко от организациите, които не използват такива платформи, планират да преминат към „облака“. От 2019 г. насам Комисията следва подход за „облачните технологии“, който предвижда сигурни хибридни многооблачни услуги[27]. Комисията действа и в качеството си на посредник при предоставянето на услуги в сферата на облачните технологии за всички EUIBA, в контекста на рамковия договор „Cloud II“. За управлението на рисковете, свързани със сигурността и защитата на данните в облачните платформи, са необходими нови умения и различен подход в сравнение с традиционната ИТ инфраструктура в локална среда. Ефективното управление на риска за

[27] Европейска комисия, Стратегия на Европейската комисия за услуги в облак, 2019 г.

информационната сигурност в облака е общо предизвикателство за EUIBA и GovSec е пример за решение, което може да отговори на нуждите на няколко, ако не и всички EUIBA.

Сътрудничеството и споделянето на практики сред EUIBA все още не е достатъчно добро

56 Съществуването на междуинституционални комитети не води автоматично до полезни взаимодействия и EUIBA невинаги споделят най-добрите практики, експертни познания, методологии и извлечени поуки. Освен това всяка EUIBA решава до каква степен ще участва в дейността на ICDT CSSG. Макар и да присъстват на заседанията, членовете на ICDT CSSG имат ограничен принос в рамките на техните обичайни задължения в EUIBA. Това вече е забавило напредъка при изпълнението на действията, договорени от някои оперативни групи.

57 ЕСП установи няколко конкретни области, в които лисват механизми за споделяне на опит и инициативи между EUIBA. Например съгласно рамковия договор за възможностите за защита на мрежата EUIBA могат да поискат провеждането на проучвания за консолидиране на изискванията по отношение на киберсигурността и откриването на решения. Не съществува обаче регистър на извършените или поискани от други EUIBA такива проучвания, което означава, че EUIBA могат да поискат едно и също проучване няколко пъти. Освен това EUIBA не споделят систематично помежду си информация за договорните си отношения с конкретни доставчици или за използването на конкретно софтуерно решение. Тези пропуски в информацията могат да доведат до допълнителни разходи и пропуснати полезни взаимодействия.

58 Освен това EUIBA не споделят систематично помежду си информация относно своите проекти в областта на киберсигурността, дори когато те биха могли да имат междуинституционално въздействие. Мандатът на ICDT CSSG предвижда EUIBA да споделят информация относно нови проекти, които е възможно да засегнат киберсигурността на други EUIBA и/или защитата на информацията, която произтича от тях. ICDT CSSG обаче не получава информация за такива проекти.

59 При създаването на нова агенция тя е принудена да изгради своята ИТ инфраструктура и рамка за ИТ сигурност от нулата. За новите агенции не съществуват „каталог на услугите“, инструментариум или ясни насоки/изисквания. В резултат на това ИТ средата в различните EUIBA е много

хетерогенна и всяка организация е потенциално свободна да си набави независимо софтуер, хардуер, инфраструктура и услуги. Подобна е ситуацията и с рамката за ИТ сигурност при липса на общи изисквания и стандарти. Това води до потенциално дублиране на усилията и до неефективно използване на средства на ЕС, но също и до усложняване на работата на CERT-EU по отношение на подкрепата, която е необходимо да предоставя.

Съществуват практически слабости при обмена на чувствителна информация

60 Някои EUIBA все още не разполагат с подходящи решения за обмена на чувствителна некласифицирана информация. Тези от тях, които разполагат с такива, са приели техни собствени различни продукти и системи, което създава проблеми с оперативната съвместимост. Общи платформи за сигурност съществуват само за конкретни цели, като пример за това са платформите за обмен на чувствителна информация относно инциденти, заплахи и уязвимости, които CERT-EU предлага на всички участници.

61 Например повече от 20 % от EUIBA не разполагат с услуга за криптирана електронна поща. Тези, които разполагат с такава, често са изправени пред проблеми, свързани с оперативната съвместимост, и сертификатите не се признават взаимно. ICTAC и ICDT обсъждат от години възможностите за решение, което да е приспособимо и оперативно съвместимо, и през 2018 г. е представен пилотен проект. Този проблем обаче все още не е решен.

62 Друг проблем е липсата на общи обозначения за чувствителна некласифицирана информация. Обозначенията представляват категоризация, посочваща на притежателя на информация какви са специфичните изисквания за защита на тази информация. Те са различни между отделните EUIBA, поради което обменът и правилната обработка на информацията се усложняват.

63 През 2020 г., в резултат на пандемията от COVID-19, EUIBA бяха принудени да приемат инструменти за комуникация и видеоконферентна връзка в широки мащаби, за да осигурят непрекъснатост на своята дейност. ЕСП установи, че EUIBA използват поне 15 различни софтуерни решения за видеоконферентна връзка. Дори и в случаите, когато различни EUIBA използват едно и също решение/платформа, оперативната съвместимост често продължава да е проблем, дори и когато всички страни използват еднакви софтуерни решения. Освен това насоките за това каква информация (от гледна точка на чувствителността) би могла да бъде споделяна или обсъждана в дадена платформа са различни в отделните EUIBA. Тези проблеми водят до

икономическа и оперативна неефективност и могат да се отразят негативно на сигурността.

ENISA и CERT-EU все още не предоставят на EUIBA цялата подкрепа, от която те се нуждаят

64 В този раздел се разглеждат двете основни организации, на които е възложена задачата да предоставят подкрепа на EUIBA в областта на киберсигурността: ENISA и CERT-EU. ЕСП провери дали предоставената от двете организации подкрепа достига до EUIBA и отговаря на техните нужди, като очерта причините, които стоят зад установените слабости.

ENISA е ключов елемент в областта на киберсигурността в ЕС, но досега нейната подкрепа е достигнала до много малко EUIBA

65 През юни 2019 г. Актът за киберсигурността (CSA)[28], който замени предходното правно основание на ENISA[29], влезе в сила и предостави на Агенцията силен мандат. По конкретно, в него се предвижда, че ENISA следва да подкрепя активно както държавите членки, така и EUIBA с цел подобряване на киберсигурността чрез изграждане на капацитет, подобряване на оперативното

[28] Задачите на ENISA са изброени в Глава II (членове 5—12) от Регламент (ЕС) 2019/881.

[29] Регламент (ЕС) 526/2013 на Европейския парламент и на Съвета; за задачите на ENISA съгласно този регламент, вж. член 3.

сътрудничество и установяване на полезни взаимодействия. В областта на изграждането на капацитет ENISA понастоящем има правомощия да съдейства на EUIBA „в усилията им да подобрят предотвратяването, установяването, анализа и способностите си за реагиране на киберзаплахи и киберинциденти, по-специално чрез целесъобразна подкрепа за CERT-EU“[30]. Освен това ENISA следва да съдейства на институциите на ЕС при разработването и преглеждането на стратегиите на Европейския съюз за киберсигурност, като насърчава тяхното разпространение и проследява напредъка при тяхното изпълнение.

66 Макар и в CSA ясно да се посочва, че ENISA следва да оказва подкрепа на EUIBA за подобряване на тяхната киберсигурност, ENISA не е завършила нито един план за действие по отношение на целите си, свързани с подпомагането на EUIBA за изграждане на капацитет (за повече информация вж. ***каре 3***).

[30] Член 6 от Регламент (ЕС) 2019/881.

Каре 3

Недостатъчна съгласуваност между целите и резултатите на ENISA по отношение на EUIBA

Някои от тригодишните приоритети на ENISA, изброени в многогодишната работна програма за 2018—2020 г. по цел 3.2 „Съдействие за изграждането на капацитета на институциите на ЕС“, са:

- Предлагане на активни консултации на институциите на Съюза относно укрепването на сигурността на тяхната мрежова и информационна сигурност (NIS) (определяне на приоритети за агенциите и органите на ЕС, които имат най-голяма нужда от изграждане на капацитет в областта на NIS, чрез редовно взаимодействие с тях (напр. ежегодни работни форуми) и фокусиране върху тези приоритети);
- Стремеж към подпомагане и улесняване на институциите на ЕС във връзка с подходите към NIS (изграждане на партньорства със CERT-EU и институции, които имат силен капацитет за NIS, с оглед осигуряване на подкрепа на техните действия по тази цел.)

В работните програми на ENISA за 2018, 2019 и 2020 г. са налице само две оперативни цели (крайни продукти/услуги) по цел 3.2:

- Участие в управителния съвет на CERT-EU и представляване на агенциите на ЕС чрез използване на услугите на CERT-EU.
- Сътрудничество със съответните органи на ЕС по инициативи, включващи аспектите на NIS, които имат отношение към техните мисии (включително EASA, CERT-EU, EDA, EC3).

Оперативните цели не включват дейности, свързани с консултации по собствена инициатива на Агенцията. Освен това целта да се установят приоритетите за онези от агенциите, които имат най-големи нужди, не е преобразувана в практически крайни продукти/услуги, тъй като е заменена от целта за сътрудничество с агенциите, за да се представляват техните нужди в управителния съвет на CERT-EU.

67 Основният орган за вземане на решения на ENISA е нейният управителен съвет, който се състои от един член, назначен от всяка от 27-те държавни членки, и от двама членове, назначени от Комисията[31] (вж. ***фигура 6***). Всеки член има право на един глас, а решенията се взимат с мнозинство[32]. В резултат на това

[31] Член 14 от CSA.

[32] Член 18 от CSA.

действията, засягащи държавите членки, могат да бъдат с по-голям приоритет в сравнение с тези за EUIBA. Например в работната програма на ENISA за 2018 г. управителният съвет, поради липса на достатъчно ресурси, в взел решение да даде приоритет на определени дейности, и да премахне три планирани дейности, едната от които е „подкрепа за оценката на съществуващите политики/процедури/практики в областта на NIS в рамките на институциите на ЕС“. Целта на тази дейност е да позволи на ENISA да изгради обща картина на практиките и индикативното ниво на зрялост в областта на киберсигурността на EUIBA като основа за бъдещи целеви действия.

68 Следователно амбицията на ENISA да предоставя активно съдействие на EUIBA, както е посочено в нейните стратегически цели, не е трансформирана в оперативни цели или конкретни действия. Подкрепа в областта на изграждането на капацитет и оперативното сътрудничество засега е предоставяна при поискване само на някои конкретни EUIBA.

69 В CSA се посочва също, че за да съдейства на EUIBA в процеса на изграждане на капацитет, ENISA следва да предоставя съответната подкрепа на CERT-EU. Към момента на одита такава подкрепа е оказвана само за няколко специфични действия. Например през 2019 г. ENISA е извършила партньорска проверка на CERT-EU в контекста на неговото членство в мрежата на EU CSIRT (създадена с Директивата относно сигурността на мрежите и информационните системи).

70 Съгласно отговорите на нашето проучване ENISA публикува висококачествени доклади и насоки в областта на киберсигурността, някои от които се използват от EUIBA. Не съществуват обаче никакви специфични насоки, насочени към EUIBA и към тяхната собствена среда и нужди. EUIBA, и особено тези от тях, които са по-малко напреднали в областта на киберсигурността, се нуждаят от практически насоки не само по отношение на това „какво“ да правят, но и „как“ да го направят. Досега ENISA и CERT-EU са предоставяли такава подкрепа ограничено и несистематично.

71 ENISA е провела редица обучения в областта на киберсигурността, които са били насочени предимно към отговорните органи в държавите членки, но в тях са участвали и ограничен брой участници от EUIBA. Агенцията е организирала само два курса за самообучение, конкретно насочени към EUIBA. ENISA предлага също и учебни материали онлайн на своя уебсайт, до които EUIBA имат достъп, но към момента това са основно курсове за технически експерти на CSIRT и поради това не са от голяма полза за повечето EUIBA.

72 Освен чрез обучения, ENISA може да оказва подкрепа на EUIBA чрез учения в областта на киберсигурността. През октомври 2020 г. ENISA, заедно със CERT-EU, е съдействала за провеждането на учение в областта на киберсигурността за ICTAC, което е единственото организирано от нея учение, предназначено изрично за участници от EUIBA. Освен това ENISA е съдействала за организирането на редица учения по молба на някои EUIBA (напр. EU-LISA, EMSA, Европейския парламент и Европол), предназначени основно за заинтересовани страни от органите на държавите членки, и с участието на някои служители на EUIBA.

73 Със CSA се въвежда също и нова роля за ENISA при подпомагането на EUIBA по отношение на техните политики за оповестяване на уязвимости, която е на доброволна основа. ENISA обаче все още не разполага с общ поглед върху политиките за оповестяване на уязвимите места на отделните EUIBA и не им предоставя съдействие при тяхното създаване и изпълнение.

CERT-EU е високо ценен от участниците в него, но възможностите му не съответстват на актуалните предизвикателства в областта на киберсигурността

74 В отговор на серия от инициативи (вж. ***фигура 7***) през септември 2012 г. с решение на Комисията[33] се създава екипът за незабавно реагиране при компютърни инциденти (CERT-EU), като постоянна оперативна група за EUIBA (вж. точка ***08***).

[33] Съобщение за медиите на Европейската комисия: По-засилена киберсигурност в институциите на ЕС след успешно реализиран пилотен проект.

Фигура 7 — История на CERT-EU

Източник: ЕСП.

75 Макар и независима при осъществяване на своята дейност, CERT-EU остава оперативна група без юридическа правосубектност. В административно отношение екипът е базиран в Европейската комисия (ГД „Информатика“), от която получава логистична и административна подкрепа. Целта на CERT-EU е да направи по-сигурна инфраструктурата на EUIBA в областта на информационните и

комуникационните технологии, като повиши техния капацитет за справяне с киберзаплахи и уязвимости и за предотвратяване, установяване и реагиране на кибератаки. CERT-EU разполага с около 40 служители, организирани в екипи от специалисти, които са съсредоточени например върху разузнавателни сведения за заплахи, цифрова криминалистика и реагиране при инциденти.

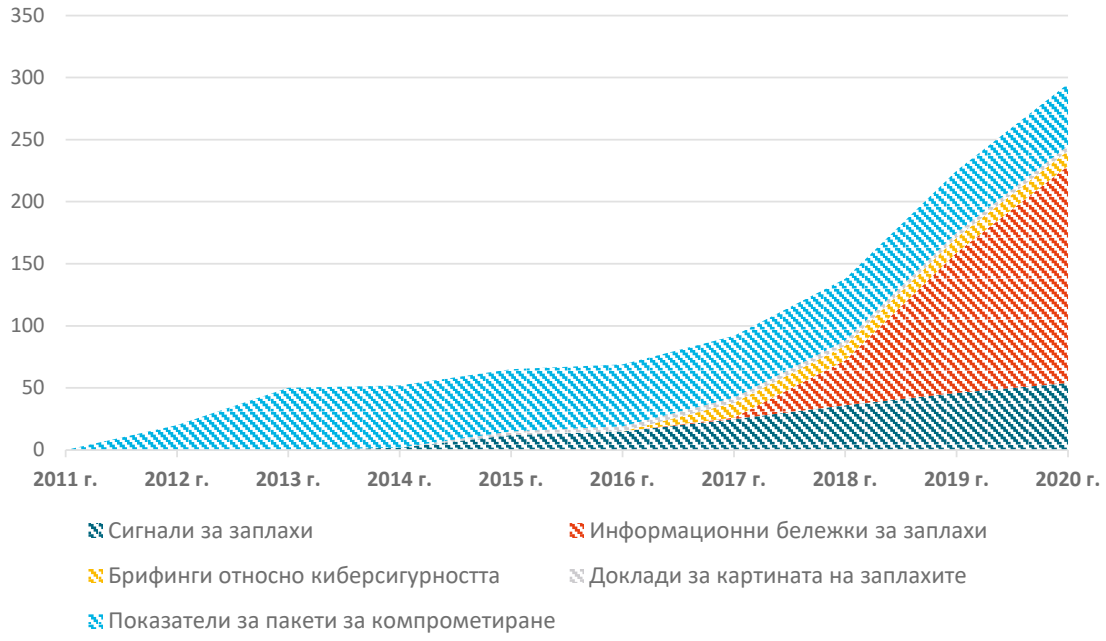
CERT-EU е ценен партньор с нарастващ обем на работа

76 CERT-EU изисква от участниците в него обратна информация и препоръки чрез провеждане на работни форуми на всяко тримесечие, годишни двустранни срещи и проучвания на удовлетвореността. Съгласно резултатите от проучванията на удовлетвореността, както и от извършеното от ЕСП проучване, участниците са до голяма степен удовлетворени от услугите, предоставяни от CERT-EU. Развитието на каталога на услугите на CERT-EU свидетелства за усилията му да се адаптира към нуждите на EUIBA.

77 Големите EUIBA, разполагащи със значителни собствени възможности, са склонни да използват CERT-EU основно като център за обмен на информация и източник на разузнавателни сведения за заплахи, но по-малките EUIBA разчитат на него за по-широк спектър от услуги, като регистри на дейности по мониторинг, проверки за проникване, тестови кибератаки с цел подобряване на сигурността и подкрепа за реагиране при инциденти. Услугите на CERT-EU са особено ценни за по-малките EUIBA поради техните ограничени вътрешни експертни познания и липса на икономии от мащаба (вж. точки ***31*** и ***33***).

78 През последните години CERT-EU засили своите възможности и процедури на фона на рязкото увеличаване на заплахите и инцидентите. Броят на информационните продукти на CERT-EU, в частност сигналите и информационните бележки за заплахи, непрекъснато нараства (***фигура 8***). През 2020 г. CERT-EU е издал 171 информационни бележки и 53 сигнала за заплахи (значително повече от 80-те бележки и 40-те сигнала, които първоначално е очаквал да изготви).

Фигура 8 — Увеличаване на броя на продуктите за обмен на информация за заплахи



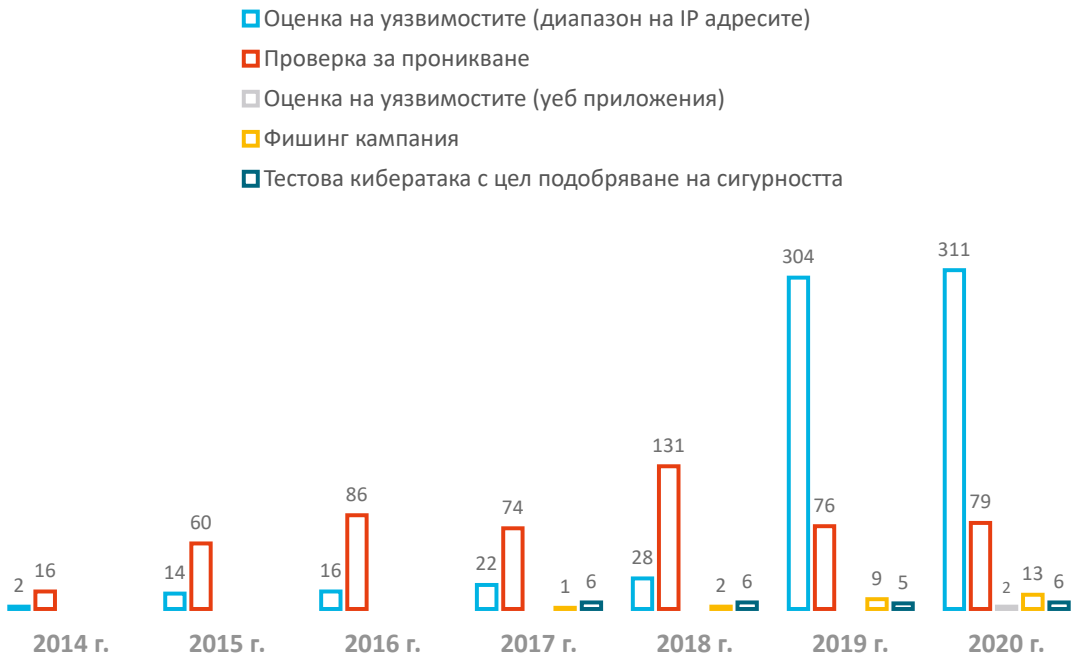
Източник: ЕСП въз основа на данни на CERT-EU.

79 CERT-EU оказва подкрепа на EUIBA и при справянето с инциденти в областта на киберсигурността. Въпреки че 52 % от EUIBA разполагат с вътрешен екип за реагиране или поне с координатор инциденти, останалите 48 % разчитат на CERT-EU и/или на други външни доставчици в случай на инцидент. Дори и големите EUIBA, разполагащи със собствени възможности за реагиране, могат да поискат подкрепа от CERT-EU за справяне със сложни инциденти.

80 Общият брой инциденти, обработени от CERT-EU, се е увеличил от 561 през 2019 г. до 884 през 2020 г. Броят на сериозните инциденти в частност се увеличил от само 1 през 2018 г. до 13 през 2020 г. През 2021 г. броят на сериозните инциденти е достигнал 17 спрямо 13 за 2020 г., която сама по себе си е година, бележеща рекорд. Тези сериозни инциденти се дължат най-общо на високотехнологични заплахи. Те могат да засегнат няколко EUIBA, да изискват контакт с отговорните органи и на засегнатите страни и на CERT-EU обикновено са необходими седмици до месеци работа за тяхното разследване и отстраняване.

81 CERT-EU е и единственият орган, който изготвя по собствена инициатива оценки и проверки на киберотбраната на EUIBA. Резюме на дейността на CERT-EU в тази област е представено на ***фигура 9*** по-долу. Освен това, от 2020 г. насам, CERT-EU извършва и външно сканиране на мрежите.

Фигура 9 — Проверки и оценки, извършени от CERT-EU



Източник: ЕСП въз основа на данни на CERT-EU.

Участниците не споделят своевременно съответната информация със CERT-EU

82 В IIA[34] се посочва, че участниците следва да уведомяват CERT-EU за сериозни инциденти в областта на киберсигурността. На практика обаче това невинаги се случва. IIA не предвижда механизъм за налагане на задължително и своевременно докладване на „сериозни“ инциденти от участниците в CERT-EU. Посоченото в IIA общо определение за „сериозни инциденти“ дава свобода на EUIBA сами да определят дали да докладват даден инцидент. Съгласно информацията, получена от ръководството на CERT-EU, някои от участниците не споделят своевременно информация за такива сериозни инциденти, което затруднява CERT-EU да изпълнява ролята на център за обмен на информация в областта на киберсигурността и за координация на реакциите при инциденти за всички EUIBA. Например един от участниците, изправен пред високотехнологична заплаха, не е информирал CERT-EU за това или не е потърсил подкрепа от него. Това е попречило на CERT-EU да събере данни за киберзаплахите, които биха били полезни при предоставянето на подкрепа на други организации, сблъскващи се със същите заплахи. Поне шест EUIBA са били засегнати от тази атака.

[34] Член 3.3 от Междуинституционалното споразумение (IIA), подписано на 20.12.2017 г.

83 Участниците също така не споделят активно със CERT-EU своевременна информация относно киберзаплахите и уязвимостите, които ги засягат, макар и съгласно IIA[35] да са задължени да го правят. Екипът по цифрова криминалистика и реагиране при инциденти на CERT-EU не получава известия за уязвимости или пропуски в механизмите за контрол извън контекста на инцидентите, които активно разследва. Участниците не споделят активно актуалните резултати от вътрешните или външните одити на сигурността.

84 Освен това IIA не задължава EUIBA да докладват на CERT-EU относно значителните промени в тяхната ИТ среда, в резултат на което участниците не уведомяват CERT-EU систематично за актуалните промени. Например EUIBA невинаги информират CERT-EU за промените, настъпили в диапазона на техните IP адреси (т.е. списъка на интернет адресите на тяхната инфраструктура). CERT-EU има нужда от актуалните диапазони на IP адресите, за да може например да извършва сканиране, когато бъдат установени сериозни уязвимости. Ако EUIBA не уведомяват CERT-EU за такива промени, това засяга неговите възможности да им окаже подкрепа. Ако CERT-EU не получава навременна информация, това оказва влияние и върху възможностите му за наблюдение на системите и създава повече работа за корекция на неточните данни в инструментите за наблюдение. Съгласно ръководството на CERT-EU, понякога при работа по даден инцидент екипът открива непозната дотогава ИТ инфраструктура. Освен това, извън някои конкретни случаи, в момента CERT-EU не разполага с пълна обзорна картина на ИТ системите и мрежите на общността от EUIBA.

85 Поради липсата на механизми за налагане на изпълнението в IIA, известията от EUIBA до CERT-EU — които са основен елемент от изграждането на общност от EUIBA, подготвена в областта на киберсигурността и изградена около CERT-EU — ще останат несистематични.

Ресурсното обезпечаване на CERT-EU е нестабилно и не съответства на актуалните нива на заплахи

86 В IIA[36] се посочва, че „на CERT-EU следва да се предостави устойчиво финансиране и персонал, като същевременно се гарантира икономическа изгода и достатъчно ядро от постоянен персонал, а административните разходи на CERT-EU се държат възможно най-ниски“. Най-важното преимущество на CERT-EU е неговият висококвалифициран и специализиран персонал. ***Фигура 10*** показва

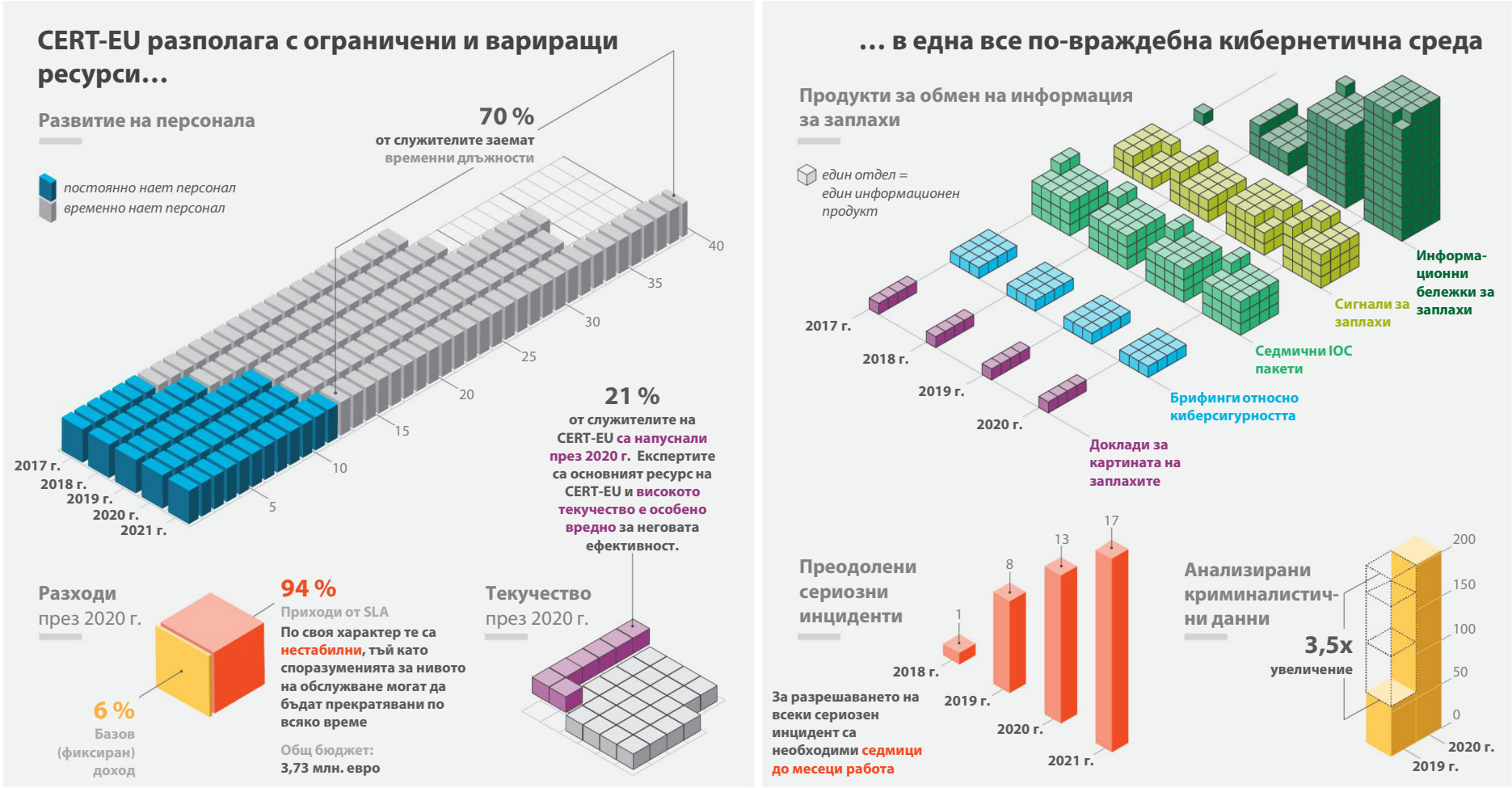
[35] Член 3.2 от Междуинституционалното споразумение (IIA).

[36] Съображение 7 от Междуинституционалното споразумение (IIA).

промяната в броя на служителите на CERT-EU от неговото създаване през 2011 г. до настоящия момент.

87 Над две трети от служителите на CERT-EU са назначени с временни договори. Възнаграждението им не е особено конкурентно на пазара на експертите в областта на киберсигурността и съгласно информацията, предоставена от ръководството на CERT-EU, назначаването и задържането им става все по-трудно. Когато възнаграждението не е достатъчно привлекателно за кандидатите с голям опит, CERT-EU е принуден да наема младши служители и да инвестират време в обучението им. Освен това максималната продължителност на договорите е шест години, което означава, че CERT-EU няма друг избор, освен да изгуби договорно наетите служители в разцвета на техния професионален опит. Текучеството на персонал е било особено високо през 2020 г.: 21 % от служителите са напуснали CERT-EU, като не за всички е било възможно да се намерят заместници. Що се отнася до предходните години, 9 % от служителите са напуснали през 2019 г. и 13 % — през 2018 г.

Фигура 10 — Ресурси и предизвикателства пред CERT-EU



Източник: ЕСП въз основа на данни на CERT-EU.

88 Ръководството на CERT-EU подчертава, че понастоящем екипът на CERT-EU за цифрова криминалистика и реагиране при инциденти е претоварен, а останалите екипи не могат да отговорят на търсенето. В резултат на това CERT-EU е принуден да намали драстично обема на дейностите си. Например CERT-EU понастоящем не извършва оценка за зрялост на своите участници поради липса на ресурси. Услугата на CERT-EU „предупреждение при подозрителна дейност“ е започнала да се предлага по-късно от очакваното, отново поради недостиг на ресурси. Освен това няколко от интервюираните от ЕСП участници отбелязаха дългото изчакване за получаване на достъп до услугите на CERT-EU.

89 Ограниченията по отношение на ресурсите досега са принудили CERT-EU да се фокусира предимно върху защитата на традиционната ИТ структура „в локална среда“, вместо върху големите заплахи от (обикновено подкрепяни на национално ниво) групи, които създават високотехнологични постоянни заплахи. Но съгласно информацията, получена от неговото ръководство, разширеният ИТ периметър на EUIBA (в който понастоящем влизат услугите в облак, мобилните устройства и инструментите за работа от разстояние) се нуждае от по-засилен мониторинг и защита. По-голямо внимание изискват и заплахите от по-ниска степен (като киберпрестъпността и софтуера за изнудване).

90 IIA не предвижда CERT-EU да поддържа оперативен капацитет двадесет и четири часа дневно, седем дни в седмицата. Понастоящем CERT-EU не разполага с ресурси, нито с подходяща рамка, уреждаща въпросите във връзка с човешките ресурси, за да бъде оперативен извън установеното работно време по постоянен и структуриран начин, макар и атаките срещу киберсигурността да не се съобразяват с работните часове. Колкото до самите EUIBA, само 35 от проучените 65 организации имат ИТ служител, който е на разположение в извънработно време.

91 За финансиране на дейностите на CERT-EU през 2012 г. управителният съвет е одобрил модел на споразумение за нивото на обслужване (SLA). Всички участници получават основни услуги безплатно и могат да заплатят за получаване на разширени услуги с подписване на SLA. Бюджетът на CERT-EU за 2020 г. е 3 745 000 евро, от които 6 % се финансират от бюджета на ЕС, а 94 % от сключените SLA. Участниците обаче са много хетерогенни: някои разполагат с утвърдени изисквания за ИТ сигурност, а други — със скромен бюджет за ИТ и много ниско равнище на зрялост в областта на киберсигурността. Поради това дискусиите за SLA водят до комбинация от високи изисквания за сигурност за някои EUIBA и до относителна липса на желание или възможност за принос от страна на други от тях.

92 Нещо повече, необходимо е SLA да бъдат подновявани индивидуално всяка година. Освен административна тежест, това създава и проблеми, свързани с паричния поток, тъй като CERT-EU не разполага със средства, постъпващи по едно и също време от всички SLA. Освен това агенциите могат да прекратят SLA във всеки един момент. Това поражда риск от образуване на един порочен кръг, в който поради пропуснати приходи CERT-EU е принуден да намали драстично обема на услугите си, което води до невъзможност за удовлетворяване на търсенето, и на свой ред принуждава останалите EUIBA да прекратят своите SLA и да преминат към частни доставчици на услуги. Предвид посочените съображения прилаганият понастоящем модел на финансиране не е идеален за осигуряване на стабилно и оптимално ниво на услугите.

93 Изправен пред бързо развиваща се картина на заплахите за киберсигурността (вж. точки ***06*** и ***80***), на своето заседание на 19 февруари 2020 г. управителният съвет на CERT-EU е одобрил стратегическо предложение, съгласно което CERT-EU следва да разшири обема на услугите си в областта на киберсигурността и да развие „пълни оперативни способности“. Предложението е придружено от анализ на нуждите от персонал и финансиране на CERT-EU. Заключението от този анализ е, че CERT-EU би имал нужда от 14 допълнителни постоянни длъжности за администратори, които да се добавят постепенно в периода 2021—2023 г. След това CERT-EU би могъл да функционира с пълен капацитет от 2023 г. нататък. Съгласно това предложение, по отношение на финансирането, CERT-EU ще е необходимо да увеличи бюджета си с 7,6 млн. евро за периода 2021—2023 г., така че до 2024 г. той да достигне 11,3 млн. евро.

94 Въпреки че EUIBA са одобрили стратегическото предложение за предоставяне на допълнителни ресурси за CERT-EU, те все още не са постигнали споразумение по отношение на практическите му аспекти — първо за междинния период 2021—2023 г., и второ — в дългосрочен план, след влизането в сила на бъдещия регламент за киберсигурността (вж. точка ***12***).

Заключения и препоръки

95 Заключението на ЕСП е, че общността на институциите, органите и агенциите на ЕС (EUIBA) не е постигнала ниво на подготвеност в областта на киберсигурността, което да съответства на заплахите. Одитната дейност на ЕСП показа, че EUIBA имат различни равнища на зрялост в областта на киберсигурността, и тъй като те често са свързани както помежду си, така и с публични и частни организации в държавите членки, слабостите в киберсигурността на една EUIBA могат да изложат останалите организации на киберзаплахи.

96 Установихме, че невинаги се прилагат ключови добри практики в областта на киберсигурността, включително някои основни механизми за контрол. Доброто управление на киберсигурността е от основно значение за сигурността на информацията и ИТ системите, но в някои EUIBA такова все още липсва: в много случаи липсват стратегии и планове за ИТ сигурност или те не са одобрени от висшето ръководство, политиките за сигурност са невинаги са официално определени, а оценките на риска не обхващат цялата ИТ среда. Разходите за киберсигурност са неравномерно разпределени, като някои EUIBA не разходват достатъчно средства в сравнение с техните партньори от същия мащаб (вж. точки ***21***—***33*** и ***37***—***38***).

97 Осведомеността в областта на киберсигурността и обучителните програми са основен елемент от ефективната рамка за киберсигурност. Само 29 % от EUIBA обаче предоставят задължително обучение по киберсигурност за служителите, отговарящи за управлението на ИТ системите, които съдържат чувствителна информация, като предлаганото обучение често е неформално. През последните пет години 55 % от EUIBA са организирали една или повече симулирани фишинг кампании (или подобни учения). Тези учения са важен инструмент за обучение на персонала и за повишаване на осведомеността, но EUIBA не ги използват систематично (вж. точки ***34***—***36***). Освен това не във всички EUIBA киберсигурността редовно е обект на независима проверка (вж. точки ***39***—***44***).

98 Екипът за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU) е високо ценен от EUIBA, които се възползват от неговите услуги, но капацитетът му е превишен. Работното му натоварване, свързано с проучванията за заплахи и действията при инциденти, нараства с бързи темпове от 2018 г. насам. Сериозните киберинциденти са се увеличили повече от десет пъти. В същото време EUIBA невинаги споделят

навременна информация за сериозни инциденти, уязвимости и важни промени в тяхната ИТ инфраструктура. Това прави дейността на CERT-EU по-неефективна и му пречи да предупреждава други потенциално засегнати EUIBA, което може да доведе до неразкриване на сериозни инциденти. Освен това ресурсите на CERT-EU варират и понастоящем не съответстват на наблюдаваното в момента ниво на заплахи или на нуждите на EUIBA. Стратегическото предложение за предоставяне на допълнителни ресурси, необходими от CERT-EU, е одобрено от управителния съвет през 2020 г., но участниците все още не са постигнали споразумение по отношение на практическите аспекти на предоставянето на такива ресурси. В резултат на това персоналът на CERT-EU не може да отговори на търсенето и е принуден да намали обема на дейностите си (вж. точки ***74***—***93***).

Препоръка 1 — Подобряване на подготвеността на всички EUIBA в областта на киберсигурността чрез въвеждане на общи задължителни правила и увеличаване на ресурсите на CERT-EU

Комисията следва да включи следните принципи в своето предстоящо предложение за регламент относно мерките за постигане на високо общо ниво на киберсигурност във всички EUIBA:

а) Висшето ръководство следва да носи отговорност за управлението на киберсигурността чрез одобряване на стратегии за киберсигурност и основни политики за сигурност и назначаване на независими главни служители по въпросите на информационната сигурност (или служители с еквивалентна функция).

б) EUIBA следва да разполагат с рамка за управление на рисковете за ИТ сигурността, която да обхваща изцяло техните ИТ инфраструктури, както и да извършват редовни оценки на риска.

в) EUIBA следва да предоставят систематични обучения за повишаване на осведомеността за целия персонал, включително и за ръководството.

г) EUIBA следва да осигурят провеждането на редовни одити и проверки на своите механизми за киберзащита. Одитите следва да включват и проверка на целесъобразността на ресурсите, предназначени за киберсигурност.

д) EUIBA следва да докладват своевременно на CERT-EU всички сериозни инциденти в областта на киберсигурността и съответните промени и уязвимости, засягащи тяхната ИТ инфраструктура;

е) EUIBA следва да заделят целеви средства с увеличен размер в своите бюджети за CERT-EU в съответствие с нуждите, които са установени в стратегическото предложение, прието от неговия управителен съвет;

ж) В регламента следва да се предвидят разпоредби за създаване на организационен субект, който да е представителен за всички EUIBA и да разполага с необходимите правомощия и инструменти за наблюдение доколко те спазват общите правила за киберсигурност, както и за изготвяне на насоки, препоръки и покани за действие.

Целева дата на изпълнение — първо тримесечие на 2023 г.

99 EUIBA разполагат с установени механизми за сътрудничество в областта на киберсигурността, но ЕСП отбеляза, че потенциалните полезни взаимодействия не се използват напълно. Съществува формализирана структура за обмен на информация, в която участниците и комитетите имат взаимнодопълващи се роли. Участието на по-малките EUIBA в междуинституционални форуми обаче е затруднено поради ограничените им ресурси, а децентрализираните агенции и съвместните предприятия не са адекватно представени в управителния съвет на CERT-EU. Установихме още, че EUIBA не обменят систематично помежду си информация относно свързани с киберсигурността проекти, оценки на сигурността и договори за услуги. Това може да доведе до дублиране на усилията и повишени разходи. ЕСП отбеляза, че съществуват оперативни затруднения при обмена на чувствителна некласифицирана информация чрез криптирана електронна поща или видеоконферентна връзка поради липса на оперативна съвместимост на ИТ системите, непоследователни насоки относно тяхната позволена употреба и липса на общи правила за обозначаване и обработка на информацията (вж. точки ***45***—***63***).

Препоръка 2 — Насърчаване на допълнителни полезни взаимодействия между EUIBA в избрани области

Комисията, в контекста на Междуинституционалния комитет за цифрова трансформация, следва да насърчи следните действия сред EUIBA;

а) приемане на решения за оперативна съвместимост на сигурните канали за комуникация от криптирана електронна поща до видеоконферентна връзка, и насърчаване на общи обозначения и общи правила за обработка на чувствителна некласифицирана информация;

б) систематичен обмен на информация относно проекти, свързани с киберсигурността, с потенциално междуинституционално въздействие, извършване на оценки на сигурността на софтуера и действащи договори с външни доставчици, и

в) определяне на спецификации за общи обществени поръчки и рамкови споразумения за услуги в областта на киберсигурността, в които могат да участват всички EUIBA, с цел насърчаване на икономии от мащаба.

Целева дата на изпълнение — четвърто тримесечие на 2023 г.

100 Агенцията на Европейския съюз за киберсигурност (ENISA) и CERT-EU са двете основни организации, на които е възложената задачата да предоставя подкрепа на EUIBA в областта на киберсигурността. Поради ограничените ресурси и приоритизирането на други области обаче те не са в състояние да предоставят на EUIBA цялата подкрепа, от която те се нуждаят, особено във връзка с изграждането на капацитет за EUIBA с по-ниски равнища на зрялост в областта на киберсигурността (вж. точки ***64***—***93***).

Препоръка 3 — Засилване на фокуса на CERT-EU и ENISA върху EUIBA с по-ниски равнища на зрялост

CERT-EU и ENISA следва да:

а) идентифицират приоритетните области, в които EUIBA имат нужда от най-голяма подкрепа, например чрез оценки на зрелостта;

б) изпълняват действия за изграждане на капацитет в съответствие с техните меморандуми за разбирателство.

Целева дата на изпълнение — четвърто тримесечие на 2022 г.

Настоящият доклад беше приет от Одитен състав III с ръководител Bettina Jakobsen — член на Европейската сметна палата, в Люксембург на 22 февруари 2022 г.

За Европейската сметна палата

Klaus-Heiner Lehne
Председател

Приложения

Приложение I — Списък на EUIBA, обхванати от проучването

Наименование на EUIBA	Вид
Европейски парламент (ЕП)	Институция (член 13, параграф 1 от Договора за Европейския съюз)
Съвет на Европейския съюз и Европейски съвет	Институция (член 13, параграф 1 от Договора за Европейския съюз)
Европейска комисия (ЕК)	Институция (член 13, параграф 1 от Договора за Европейския съюз)
Съд на Европейския съюз	Институция (член 13, параграф 1 от Договора за Европейския съюз)
Европейска централна банка (ЕЦБ)	Институция (член 13, параграф 1 от Договора за Европейския съюз)
Европейска сметна палата (ЕСП)	Институция (член 13, параграф 1 от Договора за Европейския съюз)
Европейска служба за външна дейност (ЕСВД)	Орган (член 27, параграф 3 от Договора за Европейския съюз)
Европейски икономически и социален комитет (ЕИСК) и Европейски комитет на регионите (КР)[37]	Органи (член 13, параграф 4 от Договора за Европейския съюз)
Европейска инвестиционна банка (ЕИБ)	Орган (член 308 от Договора за функционирането на Европейския съюз)
Европейски орган по труда (ELA)	Децентрализирана агенция
Агенция на Европейския съюз за сътрудничество между регулаторите на енергия (ACER)	Децентрализирана агенция
Служба на Органа на европейските регулатори в областта на електронните съобщения (BEREC)	Децентрализирана агенция
Служба на Общността за сортовете растения (CPVO)	Децентрализирана агенция
Европейска агенция за безопасност и здраве при работа (EU-OSHA)	Децентрализирана агенция

[37] ЕИСК и КР се считат за един орган.

Наименование на EUIBA	Вид
Европейска агенция за гранична и брегова охрана (Frontex/EBCGA)	Децентрализирана агенция
Агенция на Европейския съюз за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие (eu-LISA)	Децентрализирана агенция
Агенция на Европейския съюз в областта на убежището (EUAA)	Децентрализирана агенция
Агенция за авиационна безопасност на Европейския съюз (EASA)	Децентрализирана агенция
Европейски банков орган (EBA)	Децентрализирана агенция
Европейски център за профилактика и контрол върху заболяванията (ECDC)	Децентрализирана агенция
Европейски център за развитие на професионалното обучение (Cedefop)	Децентрализирана агенция
Европейска агенция по химикали (ECHA)	Децентрализирана агенция
Европейска агенция за околна среда (EEA)	Децентрализирана агенция
Европейска агенция за контрол на рибарството (EFCA)	Децентрализирана агенция
Европейски орган за безопасност на храните (EFSA)	Децентрализирана агенция
Европейска фондация за подобряване на условията на живот и труд (Eurofound)	Децентрализирана агенция
Агенция на Европейския съюз за космическата програма [заменя Европейската агенция за глобалните навигационни спътникови системи — GSA] (EUSPA)	Децентрализирана агенция
Европейски институт за равенство между половете (EIGE)	Децентрализирана агенция
Европейски орган за застраховане и професионално пенсионно осигуряване (EIOPA)	Децентрализирана агенция
Европейска агенция по морска безопасност (EMSA)	Децентрализирана агенция
Европейска агенция по лекарствата (EMA)	Децентрализирана агенция
Европейски център за мониторинг на наркотици и наркомании (EMCDDA)	Децентрализирана агенция
Агенция на Европейския съюз за киберсигурност (ENISA)	Децентрализирана агенция
Агенция на Европейския съюз за обучение в областта на правоприлагането (CEPOL)	Децентрализирана агенция
Европейска полицейска служба (Европол)	Децентрализирана агенция
Агенция за железопътен транспорт на Европейския съюз (ERA)	Децентрализирана агенция
Европейски орган за ценни книжа и пазари (ESMA)	Децентрализирана агенция
Европейска фондация за обучение (ETF)	Децентрализирана агенция
Агенция на Европейския съюз за основните права (FRA)	Децентрализирана агенция
Служба на Европейския съюз за интелектуална собственост [известна като OHIM до 23 март 2016 г.] (EUIPO)	Децентрализирана агенция
Единен съвет за преструктуриране (SRB)	Децентрализирана агенция

Наименование на EUIBA	Вид
Агенция на Европейския съюз за сътрудничество в областта на наказателното правосъдие (Евроюст)	Децентрализирана агенция
Център за преводи за органите на Европейския съюз (CdT)	Децентрализирана агенция
Европейска прокуратура (EPPO)	Децентрализирана агенция
Европейски институт за иновации и технологии (EIT)	Орган, създаден по R&I
Съвместно предприятие за изследване на управлението на въздушното движение в единното европейско небе (SESAR)	Съвместно предприятие съгласно ДФЕС
Съвместно предприятие „Електронни компоненти и системи за водещи позиции на Европа“ (ECSEL)	Съвместно предприятие съгласно ДФЕС
Съвместно предприятие „Горивни елементи и водород 2“ (ГКВ2)	Съвместно предприятие съгласно ДФЕС
Съвместно предприятие „Инициатива за иновативни лекарства 2“ (IMI2)	Съвместно предприятие съгласно ДФЕС
Съвместно предприятие „Чисто небе 2“ (Cleansky 2)	Съвместно предприятие съгласно ДФЕС
Съвместно предприятие „Биотехнологични производства“ (BBI)	Съвместно предприятие съгласно ДФЕС
Съвместна технологична инициатива Shift2Rail JU (S2R)	Съвместно предприятие съгласно ДФЕС
Съвместно предприятие за европейски високопроизводителни изчислителни технологии (EuroHPC)	Съвместно предприятие съгласно ДФЕС
Европейско съвместно предприятие за ITER — Термоядрен синтез за енергия (F4E)	Съвместно предприятие съгласно ДФЕС
Консултативна мисия на Европейския съюз в Украйна (EUAM Ukraine)	Гражданска мисия (CSDP)
Консултативна мисия на Европейския съюз за границите в Либия (EUBAM Libya)	Гражданска мисия (CSDP)
Мисия на Европейския съюз за изграждане на капацитет в Нигер (EUCAP Sahel Niger)	Гражданска мисия (CSDP)
Мисия на Европейския съюз за наблюдение в Грузия (EUMM Georgia)	Гражданска мисия (CSDP)
Координационно бюро на Европейския съюз за подпомагане на палестинската полиция (EUPOL COPPS)	Гражданска мисия (CSDP)
Консултативна мисия на Европейския съюз в Централноафриканска република (EUAM Central-African Republic)	Гражданска мисия (CSDP)
Консултативна мисия на Европейския съюз в Ирак (EUAM Iraq)	Гражданска мисия (CSDP)
Мисия на Европейския съюз за подпомагане на контролно-пропускателен пункт Рафа (EUBAM Rafah)	Гражданска мисия (CSDP)
Мисия на Европейския съюз за изграждане на капацитет в Мали (EUCAP Sahel Mali)	Гражданска мисия (CSDP)

Наименование на EUIBA	Вид
Мисия на Европейския съюз за изграждане на капацитет в Сомалия (EUCAP Somalia)	Гражданска мисия (CSDP)
Мисия на Европейския съюз в областта на върховенството на закона в Косово (EULEX Kosovo)	Гражданска мисия (CSDP)

Приложение II —Допълнителна информация относно ключовите междуинституционални комитети

Междуинституционален комитет за цифрова трансформация (ICDT)

ICDT представлява форум за обмен на информация и насърчаване на сътрудничеството в сферата на ИТ. Създаден е през май 2020 г. като наследник на бившия Comité Interinstitutionnel de l'Informatique (CII). В състава на ICDT влизат ръководителите на ИТ звената в EUIBA. ICDT разполага с подгрупа по киберсигурността (ICDT CSSG), чиято роля е да насърчава сътрудничеството между EUIBA в областта на киберсигурността, и служи като форум за обмен на информация.

Правомощията за вземане на решения на ICDT се свеждат до въпроси, които не засягат начина, по който институциите изпълняват своята мисия и или управлението в отделните институции“. За решения, които излизат извън неговите правомощия, ICDT може да дава препоръки на колегията на генералните секретари на институциите и органите на ЕС.

Съгласно мандата на ICDT неговите членове представляват всяка институция и орган на ЕС, а един представител е определен от агенциите на ЕС (ICTAC). Генералният секретариат на Съвета понастоящем председателства ICDT.

Подгрупа на ICDT по сигурността (ICDT CSSG)

ICDT CSSG в настоящата си конфигурация е учредена през септември 2020 г. като наследник на бившата постоянна група по сигурността на CII. В сравнение със своя предшественик, ICDT CSSG има по-структуриран, амбициозен и ориентиран към конкретни резултати подход. Дейностите ѝ се осъществяват от оперативни групи (ОГ), които провеждат редовни срещи и се фокусират върху основни общи проблеми:

- ОГ1 „Общи стандарти, сравнителен анализ и зрялост“
- ОГ2 „Споделяне на методи за платформи, инструменти и договори“
- ОГ3 „Сигурност на услугите в облак“
- ОГ4 „Развитие на способности и киберумения“
- ОГ5 „Осведоменост в областта на киберсигурността“
- ОГ6 „Сигурност на видеоконферентните връзки“

Съгласно мандата на CSSG нейният секретариат отговаря за редовното наблюдение и докладване за хода на дейностите на оперативните групи. Той предоставя периодични доклади на председателя и на заместник-председателя на подгрупата по киберсигурност на ICDT, като редовно взема предвид информацията, предоставена от координаторите на оперативните групи. В края на всяка година CSSG следва да представя и обобщен отчет за своята дейност.

Понастоящем Комисията председателства ICDT CSSG, а заместник-председател е представител на ICTAC. Макар и CSSG да няма правомощия за вземане на решения тя може да препоръчва решения по въпроси, свързани с ICDT.

Мрежа на агенциите

Мрежата на агенциите на ЕС (EUAN) е неформална мрежа, създадена от ръководителите на агенциите на ЕС през 2012 г. Понастоящем EUAN обхваща 48 децентрализирани агенции на ЕС и съвместни предприятия. Целта на мрежата е да предостави платформа за обмен и сътрудничество на членовете на мрежата по въпроси от общ интерес. Консултативната комисия на ICT (ICTAC) е подгрупа на EUAN, която отговаря за насърчаване на сътрудничеството в областта на ICT, включително и киберсигурността.

Консултативен комитет по информационни и комуникационни технологии (ICTAC)

ICTAC насърчава сътрудничеството сред агенциите и съвместните предприятия в областта на ICT. Неговата цел е откриване на ефективни и икономични решения на общи проблеми, обмен на информация и приемане на общи позиции при необходимост. Съгласно мандата на ICTAC общото събрание, което събира на едно място всички негови членове, се състои два пъти в годината. Провеждат се и редовни срещи всеки месец между представители на ICTAC по работните групи на CSSG, представител на ICTAC по CSSG и „Тройка“ на ICTAC. Тройка се състои от настоящите, бившите и бъдещите председатели на ICTAC (всеки председател се избира за период от една година). Ролята на Тройка е да оказва подкрепа на настоящия председател по всички въпроси, свързани с неговата/нейната роля, включително неговото/нейното заместване, ако го изискват обстоятелствата.

Акроними и съкращения

APT: Комплексна устойчива заплаха

CERT-EU: Екип за незабавно реагиране при компютърни инциденти на EUIBA

CIS: Комуникационни и информационни системи

CISO: Главен служител по сигурността на информацията

CSA: Акт за киберсигурността

CSIRT: Екип за реагиране при инциденти с компютърната сигурност

DG DIGIT: Генерална дирекция „Информатика“

DG HR: Генерална дирекция „Човешки ресурси и сигурност“

ENISA: Агенция на Европейския съюз за киберсигурност

EUAN: Мрежа на агенциите на Европейския съюз

EUIBA: Институции, органи и агенции на Европейския съюз

EU-LISA: Европейска агенция за оперативното управление на широкомащабни ИТ системи в областта на свободата, сигурността и правосъдието

FTE: Еквивалент на пълно работно време

ICDT CSSG: Подгрупа по киберсигурност на Междуинституционалния комитет за цифрова трансформация

ICDT: Междуинституционален комитет за цифрова трансформация

ICT: Информационни и комуникационни технологии

ICTAC: Консултативен комитет по информационни и комуникационни технологии

IIA: Междуинституционално споразумение

ISACA: Асоциация за одит и контрол на информационни системи

ITCB: Съвет по информационни технологии и киберсигурност

MoU: Меморандум за разбирателство

NIS: Мрежова и информационна сигурност

SLA: Споразумение за нивото на услугите

Речник на термините

Екип за незабавно реагиране при компютърни инциденти за EUIBA Център за обмен на информация и координация на реагирането при инциденти, чиито клиенти („участници“) са институциите, органите и агенциите на ЕС.

Киберпространство: Глобалната онлайн среда, в която хора, софтуер и услуги комуникират чрез мрежи от компютри и други свързани устройства.

Киберсигурност: Мерки за защита на ИТ мрежи и инфраструктура и информацията, която те съдържат, срещу външни заплахи.

Кибершпионаж: Актът или практиката на придобиване на поверителна или друга информация от интернет, мрежи или отделни компютри без разрешението и знанието на притежателя на информацията.

Комплексна устойчива заплаха: Атака, при която неупълномощен потребител осъществява достъп до система или мрежа с цел кражба на чувствителни данни и остава там за продължителен период от време.

Проверка за проникване: Метод за оценка на сигурността на дадена ИТ система, при който се правят опити за пробив в нейните механизми за защита чрез използването на същите инструменти и техники, които обикновено се използват от враждебно настроените действащи лица.

Социално инженерство: В информационната сигурност — психологическа манипулация за заблуда на потребителите да направят нещо или да споделят поверителна информация.

Тестова кибератака с цел подобряване на сигурността: Реалистична симулация на кибератаки, включваща елементи на изненада и техники, актуално използвани в реалната практика, с фокус върху специфични цели чрез множество линии на атака.

Фишинг: Практиката да се изпращат електронни съобщения, претендиращи, че идват от надежден източник, за да се заблудят получателите да последват зловредни връзки или да споделят лична информация.

Отговори на Комисията

https://www.eca.europa.eu/bg/Pages/DocItem.aspx?did=60922

Отговори на CERT-EU и ENISA

https://www.eca.europa.eu/bg/Pages/DocItem.aspx?did=60922

Хронология

https://www.eca.europa.eu/bg/Pages/DocItem.aspx?did=60922

АВТОРСКИ ПРАВА

© Европейски съюз, 2022 г.

Политиката на ЕСП относно повторната употреба е определена в Решение № 6-2019 на Европейската сметна палата относно политиката за свободно достъпни данни и повторната употреба на документи.

Освен ако не е посочено друго (напр. в отделни известия за авторските права), създаденото от ЕСП съдържание, притежавано от ЕС, е лицензирано по Creative Commons Attribution 4.0 International (CC BY 4.0). Това означава, че като правило повторната употреба е позволена, при условие че са посочени първоначалните източници и всички извършени промени. Лицето, което използва информацията на ЕСП повторно, следва да не изменя първоначалния смисъл или послание на документите. ЕСП не носи отговорност за последствия, възникнали в резултат на повторната употреба.

Необходимо е да се получи допълнително разрешение в случаите, когато дадено съдържание изобразява разпознаваеми частни лица, например на снимки на персонала на ЕСП, или когато е включено съдържание на трети страни.

В случаите, когато е получено такова разрешение, то отменя и заменя горепосоченото общо разрешение и ясно посочва всички ограничения при използването.

За използването или възпроизвеждането на съдържание, което не е собственост на ЕС, може да е необходимо да се потърси разрешение директно от носителите на авторските права.

Софтуер или документи, обхванати от правата на индустриална собственост, като патенти, търговски марки, регистрирани дизайни, лого и наименования, са изключени от политиката на ЕСП за повторно използване.

Уебсайтовете на всички институции на Европейския съюз, включени в домейна europa.eu, съдържат препратки към сайтове на трети страни. Тъй като ЕСП не контролира съдържанието им, моля, запознайте се с тяхната политика за поверителност на данните и с политиката за авторските права.

Използване на логото на ЕСП
Логото на ЕСП не може да бъде използвано без предварително разрешение.

PDF	ISBN 978-92-847-7569-9	1977-5814	doi:10.2865/482568	QJ-AB-22-003-BG-N
HTML	ISBN 978-92-847-7605-4	1977-5814	doi:10.2865/68332	QJ-AB-22-003-BG-Q

Броят на кибератаките срещу институциите, органите и агенциите на ЕС (EUIBA) се увеличава рязко. Тъй като тези институции са тясно свързани, слабостите в една от тях могат да изложат останалите на заплахи за сигурността. Европейската сметна палата (ЕСП) разгледа дали EUIBA разполагат с подходящи механизми за защита срещу киберзаплахи. Установихме, че като цяло тяхната подготвеност не отговаря на заплахите, както и че различните организации имат различно ниво на зрялост в областта на киберсигурността. ЕСП препоръчва на Комисията да предприеме действия за подобряване на подготвеността на EUIBA, като предложи въвеждането на задължителни правила за киберсигурност и увеличаването на ресурсите, заделени за Екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU). Комисията следва също така да насърчава полезните взаимодействия между EUIBA, а CERT-EU и Агенцията на Европейския съюз за киберсигурност следва да фокусират подкрепата си за по-малко подготвените организации.

Специален доклад на ЕСП съгласно член 287, параграф 4, втора алинея от ДФЕС.

ЕВРОПЕЙСКА СМЕТНА ПАЛАТА

Служба за публикации на Европейския съюз

ЕВРОПЕЙСКА СМЕТНА ПАЛАТА
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Тел. +352 4398-1

За запитвания: eca.europa.eu/bg/Pages/ContactForm.aspx
Уебсайт: eca.europa.eu
Туитър: @EUAuditors