



Брюксел, 7 юли 2026 г.
(OR. en)

8643/26

LIMITE

CORLX 388
CFSP/PESC 584
CYBER 192
JAI 505
FIN 592

ЗАКОНОДАТЕЛНИ АКТОВЕ И ДРУГИ ПРАВНИ ИНСТРУМЕНТИ

Относно:	РЕШЕНИЕ НА СЪВЕТА за изменение на Решение (ОВППС) 2019/797 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки
----------	---

РЕШЕНИЕ (ОВППС) 2026/... НА СЪВЕТА

от ...

**за изменение на Решение (ОВППС) 2019/797 относно ограничителни мерки
срещу кибератаки, застрашаващи Съюза или неговите държави членки**

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за Европейския съюз, и по-специално член 29 от него,

като взе предвид предложението на върховния представител на Съюза по въпросите на
външните работи и политиката на сигурност,

като има предвид, че:

- (1) На 17 май 2019 г. Съветът прие Решение (ОВППС) 2019/797¹.
- (2) Като част от непрекъснатите, целенасочени и координирани действия на Съюза срещу извършителите на непрекъснати киберзаплахи, в съдържащия се в приложението към Решение (ОВППС) 2019/797 списък на физическите и юридическите лица, образуванията и органите, спрямо които се прилагат ограничителни мерки, следва да бъдат добавени осем физически лица и четири образувания. Тези лица и образувания са отговорни, подкрепят или участват в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки.
- (3) Поради това Решение (ОВППС) 2019/797 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

¹ Решение (ОВППС) 2019/797 на Съвета от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 129I, 17.5.2019 г., стр. 13, ELI: <http://data.europa.eu/eli/dec/2019/797/oj>).

Член 1

Приложението към Решение (ОВППС) 2019/797 се изменя в съответствие с приложението към настоящото решение.

Член 2

Настоящото решение влиза в сила в деня на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в ... на

За Съвета

Председател

ПРИЛОЖЕНИЕ

Приложението към Решение (ОВППС) 2019/797 се изменя, както следва:

1) В раздел „А. Физически лица“ се добавят следните вписвания:

	Име	Идентификационни данни	Основания	Дата на вписване
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Изв. още като: „Bentley“, „Bergen“, „Alex Konor“, „Benny“, „Ben“, „Stern“ Дата на раждане: 23.6.1988 г. Адрес: Serebristy Bulvar 34 (Serebristy Bul'var); krp 1; flt 528; 197341; Санкт Петербург, Руска федерация Гражданство: руско Пол: мъжки Свързани образувания: TrickBot, Wizard Spider, Conti	Виталий Ковальов е със значителен опит в сферата на зловредните софтуерни програми „Trickbot“ и „Conti“. Той е известен и с онлайн псевдонимите „Bentley“, „Bergen“, „Alex Konor“, „Benny“, „Ben“ и „Stern“. Първоначално Conti и Trickbot са създадени и разработени от Wizard Spider. Wizard Spider провежда кампании със софтуер за изнудване в различни сектори, включително основни услуги като здравеопазването и банковото дело, заразява компютри в световен мащаб, а нейният зловреден софтуер е разработен в силно модулен зловреден софтуерен пакет. Кампаниите на Wizard Spider с използване на зловреден софтуер като Conti и TrickBot, са причина за значителни икономически щети в Европейския съюз. Следователно Виталий Ковальов е отговорен и участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.	+

+ ОВ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Дата на раждане: 30.1.1983 г. Място на раждане: СССР Гражданство: руско Паспорт №: 762988138 Пол: мъжки Свързани образувания: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Александър Волосовик е собственик на Media Land LLC. От 2016 г. Bullet Proof Hosting service Media Land LLC подпомага широк спектър от атаки със зловреден софтуер както срещу Съюза, така и в световен мащаб, като предлага хостинг услуги, които прикриват самоличността на потребителите и не могат да бъдат премахнати като съдържание от правоприлагащите органи. Media Land LLC е създала възможности за широкомащабни операции със софтуер за изнудване, услуги за управление и контрол и фишинг операции, насочени към критична инфраструктура и основни услуги в държавите членки, което води до значителни финансови загуби. Операциите, подпомагани от Media Land LLC, включват, наред с другото, LockBit, EvilCorp и BlackBasta. Следователно Media Land LLC участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки. Като собственик на Media Land LLC Александър Волосовик е отговорен за тези кибератаки и участва в тях. Той е свързан и с Media Land LLC.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Изв. още като: „Dena“ Дата на раждане: 9.10.1989 г. Място на раждане: СССР Гражданство: руско Пол: мъжки Адрес: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Руска федерация	Денис Дегтяренко, изв. още като Dena, е руски хакер от CARR (Cyber Army of Russia Reborn или „Киберармия за възраждане на Русия“). CARR носи отговорност за кибератаки срещу услуги, необходими за поддържането на основни икономически дейности и критични държавни функции в държавите членки, както и срещу инфраструктура в Украйна и други трети държави. CARR е свързана с Главния център за специални технологии (ГЦСТ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГРУ). ГЦСТ продължава да извършва кибератаки срещу Съюза и неговите държави членки. Сред целите на CARR са включени правителствени агенции, финансови институции, медии и критична инфраструктура в държавите членки и САЩ. CARR извършва разпределени атаки от типа „отказ от обслужване“ в Украйна и срещу правителства и дружества, намиращи се в държави, които подкрепят Украйна. Следователно Денис Дегтяренко, основен хакер на CARR, участва в кибератаки със значително въздействие, включително опити за кибератаки с потенциално значително въздействие, които представляват външна заплаха за държавите членки и за трети държави. Като член на CARR той е свързан и с ГЦСТ.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Изв. още като: „YULIYA“ Дата на раждане: 6.4.1984 г. Място на раждане: СССР Гражданство: руско Пол: женски Адрес: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Руска федерация	Юлия Панкратова е руски хакер, който работи за CARR (Cyber Army of Russia Reborn), а след това основава и работи за Z-Pentest. CARR носи отговорност за кибератаки срещу услуги, необходими за поддържането на основни икономически дейности и критични държавни функции в държавите членки, както и срещу инфраструктура в Украйна и други трети държави. CARR е подкрепяна от Главния център за специални технологии (ГЦСТ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГРУ). ГЦСТ продължава да извършва кибератаки срещу Съюза и неговите държави членки. Сред целите на CARR са правителствени агенции, финансови институции, медии и критична инфраструктура в държавите членки и САЩ. CARR извършва разпределени атаки от типа „отказ от обслужване“ в Украйна и срещу правителства и дружества, намиращи се в държави, които подкрепят Украйна.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
			Z-Pentest носи отговорност за кибератаки със значително въздействие, наред с другото, срещу услуги, необходими за поддържането на основни дейности в държавите членки. Следователно Юлия Панкратова, основен хакер на CARR и Z-Pentest, участва в кибератаки със значително въздействие, включително опити за кибератаки с потенциално значително въздействие, които представляват външна заплаха за държавите членки и за трети държави. Тя е свързана и със Z-Pentest.	

	Име	Идентификационни данни	Основания	Дата на вписване
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Изв. още като: „Daugn0“ Гражданство: предполагаемо руско Пол: мъжки	Максим Воронин, изв. още като Daugn0, участва в разработването, разпространението и продажбата на зловредния софтуер за кражба на информация LummaC2 (изв. още като Lumma infostealer, Lumma Stealer). LummaC2 е платформа от типа „зловреден софтуер като услуга“ (MaaS), използвана за кражба на чувствителни данни, данни за идентификация в браузър, криптографски портфейли или системна информация, за инсталиране на допълнителен зловреден софтуер на заразени устройства, за кражба на криптовалути и за кампании за шпионаж. Кибератаките със зловредния софтуер LummaC2 се използват и от финансово мотивирани участници в киберзаплахи като Storm-113, Storm-1607, Storm-1674, Octo Tempest и др. Зловредният софтуер LummaC2 се използва за кибератаки срещу критични държавни функции и услуги, необходими за поддържането на основни социални и икономически дейности на държавите членки. През 2024 и 2025 г. LummaC2 е един от най-използваните в световен мащаб инструменти за кражба на информация. Следователно Максим Воронин като разработчик, дистрибутор и продавач на LummaC2 участва в кибератаки и подпомага такива със значително въздействие, които представляват външна заплаха за държавите членки.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
25.	Maksim Aleksandrovich GORDIENKO Изв. още като Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Изв. още като: „Lummaseller“ Гражданство: предполагаемо руско Пол: мъжки	Максим Гордиенко, изв. още като Lummaseller, участва в разработването и разпространението на зловредния софтуер за кражба на информация LummaC2 (известен още като Lumma infostealer, Lumma Stealer). LummaC2 е платформа от типа „зловреден софтуер като услуга“ (MaaS), използвана за кражба на чувствителни данни, данни за идентификация в браузър, криптографски портфейли или системна информация, за инсталиране на допълнителен зловреден софтуер на заразени устройства, за кражба на криптовалути и за кампании за шпионаж. Кибератаките със зловредния софтуер LummaC2 се използват и от финансово мотивирани участници в киберзаплахи като Storm-113, Storm-1607, Storm-1674, Octo Tempest и др. Зловредният софтуер LummaC2 се използва за кибератаки срещу критични държавни функции и услуги, необходими за поддържането на основни социални и икономически дейности на държавите членки. През 2024 и 2025 г. LummaC2 е един от най-използваните в световен мащаб инструменти за кражба на информация. Следователно Максим Гордиенко като разработчик, дистрибутор и продавач на LummaC2 участва в кибератаки и подпомага такива със значително въздействие, които представляват външна заплаха за държавите членки .	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Дата на раждане: 25.1.1980 г. Място на раждане: СССР Гражданство: руско Пол: мъжки Свързани лица: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Свързани образувания: отдел 29155 на ГРУ, „Impuls“ LLC	Евгений Башев е член на руската агенция за военно разузнаване ГРУ, отдел 29155. В рамките на отдела той подкрепя и подпомага кибератаки със значително въздействие срещу държави членки, наред с другото чрез контрол върху сървъра Aegon, използван за хакерски операции. По-специално той предоставя техническа и материална подкрепа за кибератаките на отдел 29155 на ГРУ чрез своето дружество „Impuls“ LLC, което подпомага оперативното прикриване, инфраструктурата и плащанията, както и управяването технически активи, включително сървъри, които се използват за кибератаки. Той също така координира сътрудничеството между структурите на ГРУ и външните хакерски мрежи. Кибератаките, които той подпомага, са насочени към системи и услуги с критични държавни функции, необходими за поддържането на основни социални или икономически дейности в държавите членки, по-специално в транспортния сектор. Чрез кампанията WhisperGate отдел 29155 на ГРУ атакува и критичната инфраструктура на Украйна.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
			Следователно Евгений Башев предоставя техническа и материална подкрепа или по друг начин участва в кибератаки и опити за кибератаки със значително въздействие, представляващи външна заплаха за държавите членки, както и кибератаки със значително въздействие срещу трета държава. В качеството си на собственик и генерален директор той е свързан с дружеството "Impuls" LLC. Като член на отдел 29155 на ГРУ той е свързан и с това образувание.	

	Име	Идентификационни данни	Основания	Дата на вписване
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Място на раждане: Руска федерация Гражданство: руско Пол: мъжки Свързани лица: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Свързани образувания: отдел 29155 на ГРУ	Роман Пунтус е член на руската агенция за военно разузнаване ГРУ, отдел 29155. В рамките на отдела той има водеща функция в организирането и координирането на кибератаки със значително въздействие срещу държави членки. Той също така подкрепя развитието на вътрешния киберкапацитет на отдела, включително набирането и ръководството на персонал като хакери и програмисти. Като създава фиктивното дружество Aegeon-Impulse, той подпомага логистичните и финансовите аспекти на кибероперациите. Под негово ръководство отделът извършва кибератаки, насочени към системи и услуги, свързани с критични държавни функции, необходими за поддържането на основни социални или икономически дейности в държавите членки, по-специално в транспортния сектор. Чрез кампанията WhisperGate отдел 29155 на ГРУ атакува и критичната инфраструктура на Украйна.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
			Следователно Роман Пунтус носи отговорност или по друг начин участва в кибератаки със значително въздействие, които представляват външна заплаха за държавите членки, както и в кибератаки със значително въздействие срещу трета държава. Като член на отдел 29155 на ГРУ той е свързан и с това образувание.	

2) В раздел „Б. Юридически лица, образувания и органи“ се добавят следните вписвания:

	Име	Идентификационни данни	Основания	Дата на вписване
„8.	Media Land LLC	Адрес: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District Санкт Петербург, 196006, Руска федерация Вид на образуванието: дружество с ограничена отговорност Място на регистрация: Санкт Петербург Дата на регистрация: 19.10.2015 г. Регистрационен номер: 1152536009900 Основно място на стопанска дейност: Санкт Петербург, Руска федерация Свързано образувание: ML.Cloud	От 2016 г. Bullet Proof Hosting service Media Land LLC подпомага широк спектър от атаки със зловреден софтуер както срещу държави членки, така и в световен мащаб, като предлага хостинг услуги, които прикриват самоличността на потребителите и не могат да бъдат премахнати като съдържание от правоприлагащите органи, което води до значителни финансови загуби. Media Land LLC е създадо възможности за широкомащабни операции със софтуер за изнудване, услуги за управление и контрол, и фишинг операции, насочени към критична инфраструктура и основни услуги в редица държави членки. Операциите, подпомагани от Media Land LLC, включват, наред с другото, LockBit, EvilCorp и BlackBasta. Следователно Media Land LLC участва в кибератаки със значително въздействие, които представляват външна заплаха за държавите членки.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
9.	ML.Cloud	Адрес: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Място на регистрация: Рига Свързано лице: Alexander Volosovik Други свързани образувания: Media Land LLC	ML.Cloud е свързано с Media Land LLC дружество и осигурява техническата инфраструктура на Media Land LLC. От 2016 г. Bullet Proof Hosting service Media Land LLC подпомага широк спектър от атаки със зловреден софтуер както срещу държави членки, така и в световен мащаб, като предлага хостинг услуги, които прикриват самоличността на потребителите и не могат да бъдат премахнати като съдържание от правоприлагащите органи, което води до значителни финансови загуби. Media Land LLC е създадо възможности за широкомащабни операции със софтуер за изнудване, услуги за управление и контрол и фишинг операции, насочени към критична инфраструктура и основни услуги в държави членки . Операциите, подпомагани от Media Land LLC, включват, наред с другото, LockBit, EvilCorp и BlackBasta. Следователно Media Land LLC участва в кибератаки, които представляват външна заплаха със значително въздействие върху държавите – членки на ЕС. Следователно ML. Cloud предоставя техническа подкрепа за кибератаки със значително въздействие, които представляват външна заплаха за държавите членки.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
10.	„Impuls“ LLC	Общество с ограниченной ответственностью „Импульс“ Адрес: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Вид на образуването: дружество с ограничена отговорност Място на регистрация: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Руска федерация Дата на регистрация: 27.9.2010 г.	“Impuls” LLC е руско дружество, притежавано от Евгений Викторович Башев, член на Руската агенция за военно разузнаване ГРУ, отдел 29155. Дружеството предоставя техническа и материална подкрепа за кибератаки и опити за кибератаки, извършвани от отдел 29155 на ГРУ. По-специално “Impuls” LLC служи като оперативен посредник, който осигурява възможности за извършването на дейности, свързани с хакерство, чрез дружество, което формално не е свързано с руската държава. То подпомага оперативното прикриване, инфраструктурата и плащанията за кибератаки и е свързано с технически активи, включително сървъри, използвани в подкрепа на хакерски дейности. По-специално “Impuls” LLC е създавало възможност за сътрудничество между структурите на ГРУ и външните хакерски мрежи. Кибероперациите, подпомагани от “Impuls” LLC, са насочени към критични държавни функции и услуги, необходими за поддържането на основни социални и икономически дейности в държавите членки, по-специално в транспортния сектор. Чрез кампанията WhisperGate отдел 29155 на ГРУ атакува и критичната инфраструктура на Украйна.	+

+ ОБ: Моля, въведете датата на публикуване на настоящото решение.

	Име	Идентификационни данни	Основания	Дата на вписване
		Регистрационен номер: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Основно място на стопанска дейност: Руска федерация Свързани лица: Evgeniy Bashev Свързани образувания: отдел 29155 на ГРУ	Следователно “Impuls” LLC предоставя техническа и материална подкрепа или участва по друг начин в кибератаки със значително въздействие, представляващи външна заплаха за държавите членки, както и кибератаки със значително въздействие срещу трета държава.	

	Име	Идентификационни данни	Основания	Дата на вписване
11.	Z-Pentest	Изв. още като: „Z-Pentest Alliance“, „Z-Alliance“ Основно място на стопанска дейност: Руска федерация Свързани лица: Yuliya Pankratova Свързани образувания: Cyber Army of Russia/CARR Профил в X.com: ZPentest (профилът е блокиран) Профил в Telegram: Zpentestalliance	Z-Pentest е проруска хакерска група, съставена от членове на CARR (Cyber Army of Russia Reborn) и NoName057, чиято дейност е насочена в световен мащаб към критичната инфраструктура, по-специално в секторите на енергетиката и водоснабдяването. По-конкретно през декември 2024 г. групата извършва атака срещу датско водоснабдително дружество. Следователно Z-Pentest носи отговорност за кибератаки със значително въздействие, които представляват външна заплаха за държавите членки.	+

+ ОВ: Моля, въведете датата на публикуване на настоящото решение.