2025/173

27.1.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/173 НА СЪВЕТА

от 27 януари 2025 година

за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2019/796 на Съвета от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки ([1]), и по-специално член 13, параграф 1 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 Регламент (ЕС) 2019/796.

(2) Целенасочените ограничителни мерки срещу кибератаки със значително въздействие, представляващи външна заплаха за Съюза или неговите държави членки, са една от мерките, включени в рамката на Съюза за съвместен дипломатически отговор на злонамерени действия в киберпространството, а именно „инструментариум за кибердипломация“, и са жизненоважен инструмент за предотвратяването, възпирането, разколебаването и реагирането на такива действия.

(3) Броят, честотата и изобретателността на злонамерените действия в киберпространството срещу критична инфраструктура или основни услуги, включително чрез използването на софтуер за изнудване и за заличаване на съдържание, вземането на прицел на веригите на доставки и кибершпионажът, включително дейностите за кражба на интелектуална собственост, се увеличават. Със смущенията и разрушителните си последици тези дейности представляват системна заплаха за сигурността, икономиката, и демокрацията и обществото като цяло в Съюза.

(4) През 2020 г. бяха извършени кибератаки със значително въздействие срещу Естония. Бяха извършени кибератаки срещу компютърни системи на множество институции с цел използване на данните за заплаха за сигурността на Естония. Тези кибератаки се отнасяха до съхранението на класифицирана информация.

(5) Като част от непрекъснатите, целенасочени и координирани действия на Съюза срещу упорстващите извършители на киберзаплахи, в списъка на подложените на ограничителни мерки физически и юридически лица, образувания и органи, съдържащ се в приложение I към Регламент (ЕС) 2019/796, следва да бъдат включени три физически лица. Тези лица са отговорни или участват в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки.

(6) Поради това приложение I към Регламент (ЕС) 2019/796 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Приложение I към Регламент (ЕС) 2019/796 се изменя в съответствие с приложението към настоящия регламент.

Член 2

Настоящият регламент влиза в сила в деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 27 януари 2025 година.

За Съвета

Председател

K. KALLAS

([1]) ОВ L 129 I, 17.5.2019 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ПРИЛОЖЕНИЕ

В приложение I към Регламент (ЕС) 2019/796 се добавят следните вписвания в раздел „A. Физически лица“:

	Име	Идентификационни данни	Основания	Дата на вписване
„15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Дата на раждане: 16.9.1997 г. Гражданство: руско Пол: мъжки Свързано образувание: Главно управление на Генералния щаб на въоръжените сили на Руската федерация	Николай Корчагин участва и носи отговорност за кибератаки със значително въздействие чрез извършване на разузнавателни дейности срещу Естония и незаконно получаване на достъп до компютърна система. Николай Корчагин е офицер във военно поделение 29155 на Главното управление на Генералния щаб на въоръжените сили на Руската федерация. В това си качество той участва и носи отговорност за кибератаки срещу компютърни системи с цел събиране на данни от системите за данни на множество институции, които самостоятелно или в комбинация дават представа за политиката на Естония в областта на киберсигурността, кибернетичните способности на държавата, на чувствителни лични данни и други чувствителни данни с цел да бъдат използвани за заплаха за сигурността на Естония. Атаките следователно се отнасят до съхранението на класифицирана информация. Атаките засягат съюзници и партньори на Естония. Следователно Николай Корчагин участва и носи отговорност за кибератаки със значително въздействие, които представляват външна заплаха за държава членка.	27.1.2025 г.
16.	Vitaly SHEVCHENKO	Виталий Шевченко Дата на раждане: 1.9.1997 г. Гражданство: руско Пол: мъжки Свързано образувание: Главно управление на Генералния щаб на въоръжените сили на Руската федерация	Виталий Шевченко участва и носи отговорност за кибератаки със значително въздействие чрез извършване на разузнавателни дейности срещу Естония и незаконно получаване на достъп до компютърна система. Виталий Шевченко е офицер във военно поделение 29155 на Главното управление на Генералния щаб на въоръжените сили на Руската федерация. В това си качество той участва и носи отговорност за кибератаки срещу компютърни системи с цел събиране на данни от системите за данни на множество институции, които самостоятелно или в комбинация дават представа за политиката на Република Естония в областта на киберсигурността, кибернетичните способности на държавата, на чувствителни лични данни и други чувствителни данни с цел да бъдат използвани за заплаха за сигурността на Естония. Атаките следователно се отнасят до съхранението на класифицирана информация. Атаките засягат съюзници и партньори на Естония. Следователно Виталий Шевченко участва и носи отговорност за кибератаки със значително въздействие, които представляват външна заплаха за държава членка.	27.1.2025 г.

ELI: http://data.europa.eu/eli/reg_impl/2025/173/oj

	Име	Идентификационни данни	Основания	Дата на вписване
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Дата на раждане: 17.6.1980 г. Гражданство: руско Пол: мъжки Свързано образувание: Главно управление на Генералния щаб на въоръжените сили на Руската федерация	Юрий Денисов участва и носи отговорност за кибератаки със значително въздействие чрез извършване на разузнавателни дейности срещу Естония и незаконно получаване на достъп до компютърна система. Юрий Денисов е офицер във военно поделение 29155 на Главното управление на Генералния щаб на въоръжените сили на Руската федерация. В това си качество той участва и носи отговорност за кибератаки срещу компютърни системи с цел събиране на данни от системите за данни на множество институции, които самостоятелно или в комбинация дават представа за политиката на Естония в областта на киберсигурността, кибернетичните способности на държавата, на чувствителни лични данни и други чувствителни данни с цел да бъдат използвани за заплаха за сигурността на Естония. Атаките следователно се отнасят до съхранението на класифицирана информация. Атаките засягат съюзници и партньори на Естония. Следователно Юрий Денисов участва и носи отговорност за кибератаки със значително въздействие, които представляват външна заплаха за държава членка.	27.1.2025 г.“