Съвет на
Европейския съюз

Брюксел, 13 май 2024 г.
(OR. en)

8500/24

LIMITE

CORLX 354
CFSP/PESC 510
CYBER 108
JAI 570
FIN 339

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) 2024/… 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) 2019/797[1].

(2) Решение (ОВППС) 2019/797 се прилага до 18 май 2025 г. Въз основа на преглед на въпросното решение срокът на валидност на посочените в него ограничителни мерки следва да бъде удължен до тази дата.

(3) С оглед на продължаващото и нарастващо злонамерено поведение в киберпространството, включително поведение, насочено срещу трети държави, основанията за включване на шест лица и две образувания в списъка на подлежащите на ограничителни мерки физически и юридически лица, образувания и органи, съдържащ се в приложението към Решение (ОВППС) 2019/797, следва да бъдат актуализирани.

(4) 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).

Член 1

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

1) Член 10 от се заменя със следното:

„*Член 10*

Настоящото решение се прилага до 18 май 2025 г. и подлежи на редовно преразглеждане.“;

2) Приложението се изменя в съответствие с приложението към настоящото решение.

Член 2

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

Съставено в … на

За Съвета
Председател

ПРИЛОЖЕНИЕ

Приложението към Решение (ОВППС) 2019/797 („Списък на физическите и юридическите лица, образуванията и органите, посочени в членове 4 и 5“) се изменя, както следва:

1) В списък „А. Физически лица“ вписвания 3—8 се заменят със следното:

	Име	Идентификационни данни	Основания	Дата на вписване
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Дата на раждане: 27.5.1972 г. Място на раждане: Пермска област, Руска СФСР (понастоящем Руска федерация) Паспорт №: 120017582 Издаден от: Министерството на външните работи на Руската федерация Валиден: от 17.4.2017 г. до 17.4.2022 г. Място: Москва, Руска федерация Гражданство: руско Пол: мъжки	Алексей Минин участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия и в кибератаки със значително въздействие срещу трети държави. Като оперативен офицер от агентурното разузнаване към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Алексей Минин е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО. Срещу Алексей Минин в качеството му на служител на руското Главно разузнавателно управление (ГРУ) е повдигнато обвинение от разширен съдебен състав в Западния окръг на Пенсилвания (Съединени американски щати) за компютърно хакерство, електронна измама, квалифицирана кражба на самоличност и изпиране на пари.	30.7.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Дата на раждане: 31.7.1977 г. Място на раждане: Мурманска област, Руска СФСР (понастоящем Руска федерация) Паспорт №: 100135556 Издаден от: Министерството на външните работи на Руската федерация Валиден: от 17.4.2017 г. до 17.4.2022 г. Място: Москва, Руска федерация Гражданство: руско Пол: мъжки	Алексей Моренец участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия и в кибератаки със значително въздействие срещу трети държави. Като кибероператор за Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Алексей Моренец е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО. Срещу Алексей Моренец в качеството му на служител на Военно подразделение 26165 е повдигнато обвинение от разширен съдебен състав в Западния окръг на Пенсилвания (Съединени американски щати) за компютърно хакерство, електронна измама, квалифицирана кражба на самоличност и изпиране на пари.	30.7.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Дата на раждане: 26.7.1981 г. Място на раждане: Курск, РСФСР (понастоящем Руска федерация) Паспорт №: 100135555 Издаден от: Министерството на външните работи на Руската федерация Валиден: от 17.4.2017 г. до 17.4.2022 г. Място: Москва, Руска федерация Гражданство: руско Пол: мъжки	Евгений Серебряков участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия и в кибератаки със значително въздействие срещу трети държави. Като кибероператор за Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Евгений Серебряков е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО. От пролетта на 2022 г. Евгений Серебряков е начело на „Sandworm“ (изв. още като „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ и „Telebots“) — извършител и хакерска група, свързана с Подразделение 74455 на руското Главно разузнавателно управление. От началото на агресивната война на Русия срещу Украйна „Sandworm“ извършва кибератаки срещу Украйна, включително срещу украински правителствени агенции.	30.7.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Дата на раждане: 24.8.1972 г. Място на раждане: Уляновск, Руска СФСР (понастоящем Руска федерация) Паспорт №: 120018866 Издаден от: Министерството на външните работи на Руската федерация Валиден: от 17.4.2017 г. до 17.4.2022 г. Място: Москва, Руска федерация Гражданство: руско Пол: мъжки	Олег Сотников участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия и в кибератаки със значително въздействие срещу трети държави. Като оперативен офицер от агентурното разузнаване към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Олег Сотников е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО. Срещу Олег Сотников в качеството му на служител на руското Главно разузнавателно управление (ГРУ) е повдигнато обвинение от разширен съдебен състав в Западния окръг на Пенсилвания за компютърно хакерство, електронна измама, квалифицирана кражба на самоличност и изпиране на пари.	30.7.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Дата на раждане: 15.11.1990 г. Място на раждане: Курск, РСФСР (понастоящем Руска федерация) Гражданство: руско Пол: мъжки	Дмитрий Бадин участва в кибератака със значително въздействие срещу Германския федерален парламент (Deutscher Bundestag) и в кибератаки със значително въздействие срещу трети държави. В качеството си на офицер от военното разузнаване от 85-и Главен център за специални услуги (ГЦСУ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Дмитрий Бадин е бил част от екипа на офицерите от руското военно разузнаване, които извършиха кибератаката срещу Германския федерален парламент през април и май 2015 г. Кибератаката беше насочена срещу информационната система на парламента и наруши нейното функциониране за няколко дни. Бяха откраднати значително количество данни и бяха засегнати електронните пощи на няколко членове на парламента, както и на бившия канцлер Ангела Меркел. Срещу Дмитрий Бадин в качеството му на служител на Военно подразделение 26165 е повдигнато обвинение от разширен съдебен състав в Западния окръг на Пенсилвания (Съединени американски щати) за компютърно хакерство, електронна измама, квалифицирана кражба на самоличност и изпиране на пари.	22.10.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Дата на раждане: 21.2.1961 г. Гражданство: руско Пол: мъжки	Игор Костюков е настоящият началник на Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ), където преди това е служил като първи заместник-началник. Една от единиците под негово командване е 85-и Главен център за специални услуги (ГЦСУ), (известен също като „Военно подразделение 26165“, „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ и „Strontium“). В това си качество Игор Костюков е отговорен за кибератаките, извършени от ГЦСУ, включително за тези със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки. По-специално офицерите от военното разузнаване от ГЦСУ са взели участие в кибератаките срещу Германския федерален парламент (Deutscher Bundestag през април и май 2015 г. и в опита за кибератака, която е имала за цел включване в безжичната мрежа на Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия през април 2018 г. Кибератаката срещу Германския федерален парламент беше насочена срещу информационната система на парламента и наруши нейното функциониране за няколко дни. Бяха откраднати значително количество данни и бяха засегнати електронните пощи на няколко членове на парламента, както и на бившия канцлер Ангела Меркел.	22.10.2020 г.“;

2) В списък „Б. Юридически лица, образувания и органи“ вписвания 3 и 4 се заменят със следното:

	Име	Идентификационни данни	Основания	Дата на вписване
„3.	Главен център за специални технологии (ГЦСТ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ)	Адрес: Ул. „Кирова“ № 22, Москва, Руска федерация	Главният център за специални технологии (ГЦСТ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ), известен още като „Подразделение 74455“, участва в кибератаките със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или за неговите държави членки, и в кибератаки със значително въздействие върху трети държави, в т.ч. кибератаките от юни 2017 г., известни в публичното пространство като „NotPetya“ или „EternalPetya“, и кибератаките срещу електроенергийната мрежа на Украйна през зимата на 2015/2016 г. „NotPetya“ или „EternalPetya“ прекъсват достъпа до данните на редица дружества в Съюза, в Европа като цяло и по света, като заразяват компютрите със софтуер за изнудване и блокират достъпа до данните, което освен всичко друго води до значителни икономически загуби. Кибератаката срещу електроенергийна мрежа на Украйна води до частичното ѝ изключване през зимата.	30.7.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
			„NotPetya“ или „EternalPetya“ е дело на извършител, известен в публичното пространство като „Sandworm“ (изв. още като „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ и „Telebots“). Той стои и зад атаката срещу електроенергийната мрежа на Украйна. От началото на агресивната война на Русия срещу Украйна „Sandworm“ извършва кибератаки срещу Украйна, включително срещу украински правителствени агенции и критична инфраструктура на Украйна. Тези кибератаки включват кампании за насочен фишинг, атаки със зловреден софтуер и софтуер за изнудване. Главният център за специални технологии към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация играе активна роля в действията в киберпространството, дело на Sandworm, и може да бъде свързан с него.	

	Име	Идентификационни данни	Основания	Дата на вписване
4.	85-и Главен център за специални услуги (ГЦСУ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ)	Адрес: Комсомольский пр., 20, Москва, 119146, Руска федерация	85-и Главен център за специални услуги (ГЦСУ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ), (известен също като „Военно подразделение 26165“, „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“, „Strontium“), участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки и в кибератаки със значително въздействие срещу трети държави. По-специално офицерите от военното разузнаване от ГЦСУ са взели участие в кибератаките срещу Германския федерален парламент (Deutscher Bundestag) през април и май 2015 г., и в опита за кибератака, която е имала за цел включване в безжичната мрежа на Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия през април 2018 г. Кибератаката срещу Германския федерален парламент беше насочена срещу информационната система на парламента и наруши нейното функциониране за няколко дни. Бяха откраднати значително количество данни и бяха засегнати електронните пощи на няколко членове на парламента, както и на бившия канцлер Ангела Меркел. От началото на агресивната война на Русия срещу Украйна страната е обект на кибератаки от ГЦСУ (насочен фишинг и атаки, базирани на зловреден софтуер).	22.10.2020 г.“.