СЛУЖБА БЕЗПЕКИ УКРАЇНИ

вул. Володимирська, 33, м. Київ, 01601, тел./факс: (044) 226-34-31, тел. 256-99-05
www.ssu.gov.ua, e-mail: sbu_cu@ssu.gov.ua Код ЄДРПОУ 00034074

06.10.2020 № 30/4/3-9891 На № _____ від _____

Прим. №___

Т.в.о. Голови Державної регуляторної служби України Олегу МІРОШНІЧЕНКУ

Щодо погодження проекту нормативно-правового акта

Шановний пане Олегу!

Відповідно до статей 10, 24 Закону України "Про Службу безпеки України" та статей 5, 10 та 11 Закону України "Про основні засади забезпечення кібербезпеки України", статті 19 Закону України "Про національну безпеку України", Ситуаційним центром забезпечення кібербезпеки Служби безпеки України розроблено та впроваджено платформу обміну інформацією щодо кіберінцидентів на базі адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA") між суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

З огляду на викладене, надсилаємо розроблений проект наказу Центрального управління Служби безпеки України "Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA")" для розгляду та погодження.

Відповідальні за опрацювання проекту в ДКІБ СБУ Кривко Олександр Васильович та Барабаш Сергій Дмитрович, тел. (044) 236-80-51.

Додатки: 1. Проект наказу ЦУ СБУ "Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage"

0.31

("MISP-UA")", реєстр. № 30/4/3-9889 від 06.10.2020, прим. № 1, на 5 арк., відкрита інформація, лише в адресу.

2. Пояснювальна записка до проекту наказу ЦУ СБУ "Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA")", реєстр. № 30/4/3-9890 від 06.102020, прим. № 1, на 3 арк., відкрита інформація, лише в адресу.

3. Аркуш погодження до проекту наказу ЦУ СБУ "Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA")", б/н, прим. № 1, на 1 арк., відкрита інформація, лише в адресу, підлягає поверненню.

З повагою

Заступник Голови Служби **Володимир ГОРБЕНКО**

Вик. Кравко О.В
т. Місцевий (044) 238-80-51

ПРОЕКТ

СЛУЖБА БЕЗПЕКИ УКРАЇНИ
ЦЕНТРАЛЬНЕ УПРАВЛІННЯ

НАКАЗ

_____ Київ № _____

Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing “Ukrainian Advantage” (“MISP-UA”)

Відповідно до статей 10, 24 Закону України “Про Службу безпеки України” та статей 5, 10 та 11 Закону України “Про основні засади забезпечення кібербезпеки України”, статті 19 Закону України “Про національну безпеку України”

НАКАЗУЮ:

1. Затвердити Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing “Ukrainian Advantage” (“MISP-UA”), що додається.

2. Начальникам Управління правового забезпечення та Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому законодавством порядку.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

Голова Служби **Іван БАКАНОВ**

Тематичні індекси: 1-1; 6-1; 14-1; 20-1.

ЗАТВЕРДЖЕНО
Наказ Центрального управління
Служби безпеки України
__._____.2020 року № ____

ПОЛОЖЕННЯ
про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA")

I. Загальні положення

1. Це Положення визначає порядок обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA") (далі – MISP-UA) між суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, визначені частиною четвертою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України" (далі – суб'єкти забезпечення кібербезпеки).

2. MISP-UA є системою збору, обробки та обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем між суб'єктами забезпечення кібербезпеки в режимі реального часу, яка побудована на базі

платформи з відкритим програмним кодом MISP (Malware Information Sharing Platform).

3. MISP-UA призначена для здійснення інформаційного обміну між суб'єктами забезпечення кібербезпеки щодо кібератак, кіберінцидентів, інших кіберзагроз, технічними даними про ідентифікатори компрометації інформаційних систем.

4. Розпорядником MISP-UA є Служба безпеки України (далі – СБУ).

5. Під час використання MISP-UA суб'єктам забезпечення кібербезпеки:

дозволяється оприлюднення та поширення інформації про зареєстровані кібератаки, кіберінциденти, внесені іншими суб'єктами забезпечення кібербезпеки до MISP-UA, за умови відсутності законодавчо визначених обмежень (зобов'язань), дотримання міжнародного стандарту Traffic Light Protocol (далі – TLP);

дозволяється використовувати дані MISP-UA, внесені іншими суб'єктами забезпечення кібербезпеки до MISP-UA, для організації та здійснення кіберзахисту власних інформаційно-телекомунікаційних систем;

забороняється надання (розголошення або поширення) розміщеної в MISP-UA інформації, що дозволяє ідентифікувати суб'єкт забезпечення кібербезпеки, який є власником (розпорядником) атакованої інформаційної системи, а також відомостей про наслідки або спричинені збитки стороні, яка не є користувачем MISP-UA;

забороняється внесення до MISP-UA інформації про кібератаки, кіберінциденти, інші кіберзагрози, технічні дані про ідентифікатори компрометації інформаційних систем у навмисно спотвореному чи перекрученому вигляді.

II. Особливості інформаційного обміну між суб'єктами забезпечення кібербезпеки з використанням MISP-UA та встановлення обмежень доступу до інформації, яка циркулює в MISP-UA

1. Обмін інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем між суб'єктами забезпечення кібербезпеки здійснюється на безоплатній основі на підставі спільних рішень, які оформлюються окремими публічними угодами між СБУ та іншими суб'єктами забезпечення кібербезпеки про організацію взаємодії з питань обміну інформацією з використанням MISP-UA.

2. У MISP-UA не допускається здійснення обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем, які містять відомості з обмеженим доступом.

3. У MISP-UA реалізовано обмеження доступу до інформації та її поширення відповідно до міжнародного стандарту Traffic Light Protocol (далі – TLP) у таких значеннях:

TLP:RED – суб'єкти забезпечення кібербезпеки не мають права розголошувати розміщену в MISP-UA інформацію;

TLP:AMBER – суб'єкти забезпечення кібербезпеки мають право надавати розміщену в MISP-UA інформацію виключно співробітникам;

TLP:GREEN – суб'єкти забезпечення кібербезпеки мають право надавати розміщену в MISP-UA інформацію своїм співробітникам, а також партнерським органам, організаціям, установам у сфері кібербезпеки, але без використання загальнодоступних каналів;

TLP:WHITE – суб'єкти забезпечення кібербезпеки мають право надавати розміщену в MISP-UA інформацію без обмежень.

4. Припинення доступу суб'єктів забезпечення кібербезпеки до MISP-UA здійснюється СБУ за їх ініціативою або в разі порушення ними умов, визначених у пункті 5 розділу I цього Положення.

III. Зберігання та використання інформації, розміщеної у MISP-UA

1. Інформація щодо кібератак, кіберінцидентів, інших кіберзагроз та технічні дані про ідентифікатори компрометації інформаційних систем зберігаються в MISP-UA безстроково.

2. Інформація з MISP-UA використовується з додержанням вимог Закону України "Про інформацію" виключно для потреб, визначених статтями 8, 11 Закону України "Про основні засади забезпечення кібербезпеки України".

Начальник Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки **Олексій КОРНІЙЧУК**

30/4/3-9889

Прим. № 1

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту наказу Центрального управління Служби безпеки України "Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA")"

1. Резюме

Проект наказу спрямований на нормативно-правове врегулювання порядку та організації обміну інформацією про кіберінциденти між суб'єктами забезпечення кібербезпеки, які визначені статтею 5 Закону України "Про основні засади забезпечення кібербезпеки України.

2. Проблема, яка потребує розв'язання

Видання проекту наказу обумовлене необхідністю визначення механізму обміну інформацією про кіберінциденти між суб'єктами забезпечення кібербезпеки та врегулювання питань, які раніше не були чітко врегульовані нормативно-правовими актами.

3. Суть проекту акта

Проектом наказу врегульовується порядок та організація механізму обміну інформацією про кіберінциденти між суб'єктами забезпечення кібербезпеки.

4. Вплив на бюджет

Реалізація положень проекту не потребує виділення додаткових коштів з Державного бюджету України.

5. Позиція заінтересованих органів

Проект наказу не потребує проведення консультацій із заінтересованими сторонами, не стосується питання функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку. Соціально-трудової сфери, прав та осіб з інвалідністю.

Проект накауз не стосується сфери наукової та науково-технічної діяльності, у зв'язку з чим він не надсилається на розгляд Наукового комітету Національної ради з питань розвитку науки і технологій.

Проект акта не вноситься на громадське обговорення.

6. Прогноз впливу

Видання проекту наказу не має негативного впливу на ринкове середовище, забезпечення прав і інтересів суб'єктів господарювання, громадян та держави.

Реалізація проекту наказу не має впливу на окремі регіони.

Реалізація проекту наказу не має впливу на ринок праці, рівень зайнятості населення; громадського здоров'я, покращення чи погіршення стану здоров'я його окремих груп; екологію та навколишнє середовище, обсяг природних ресурсів, рівень забруднення атмосферного повітря, води, земель, зокрема забруднення утвореними відходами.

7. Позиція заінтересованих органів

Проект наказу потребує погодження з Міністерством цифрової трансформації України, Державною регуляторною службою України та Держспецзв'язку України.

8. Ризики та обмеження

Проект наказу не стосується питань інформатизації, електронного урядування, формування і використання національних інформаційних ресурсів, розвитку інформаційного суспільства, електронної демократії, надання адміністративних послуг або цифрового розвитку та не потребує проведення цифрової експертизи Мінцифри і отримання відповідного висновку.

В проекті наказу відсутні положення, що стосуються прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод, впливають на забезпечення рівних прав та можливостей жінок і чоловіків, містять ризики вчинення корупційних правопорушень та правопорушень, пов'язаних з корупцією, створюють підстави для дискримінації, стосуються інших ризиків та обмежень, які можуть викинути під час реалізації акта.

Громадська антикорупційна та громадська антидискримінаційна експертиза проекту наказу не проводилася.

9. Підстава розроблення проекту акта

Проект наказу розроблено за власною ініціативою з метою нормативно-правового врегулювання процедури обміну інформацією про кіберінциденти між суб'єктами забезпечення кібербезпеки.

Начальник ДКІБ СБ України **Олексій КОРНІЙЧУК**

«06» жовтня 2020 року

30/4/3-9890

Додаток 10
до Інструкції про нормотворчу діяльність Служби безпеки України

А Р К У Ш П О Г О Д Ж Е Н Н Я

до проекту наказу ЦУ СБУ "Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" ("MISP-UA")"

(найменування підрозділу, з яким погоджується проект акта)	(підпис керівника підрозділу, або особи, яка його заміщує, ініціал його імені та прізвище)

Погодження здійснив: консультант-експерт 3 відділу 4 управління (СЦЗК) ДКІБ СБУ Кривко О.В.

02. жовтня 2020.