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

19.10.21 № 30/4/1-11094 На № _____ від _____

Прим. № 1

Голові Державної регуляторної служби України
Олексію КУЧЕРУ

Щодо погодження проекту нормативно-правового акта

Шановний пане Олексію!

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 здійснюються необхідні заходи з впровадження платформи 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.

Відповідно до процедури, передбаченої законодавством України, додатково направляємо повідомлення про оприлюднення проекту на

0.31

офіційному сайті СБУ та аналіз регуляторного впливу згаданого проекту. Повідомлення було опубліковано на офіційному сайті СБУ 05 серпня 2021 р. за посиланням – https://ssu.gov.ua/uploads/documents/2021/08/05/dlya-publikatsii-uzmig-nakaz-pro-zatv-polozhennya-misp-ua-poyasnyuvalbna-final-12-07-2021.pdf. Протягом місяця зауважень та пропозицій до проекту не отримано.

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" (MISP-UA)", реєстр. № 30/4/1-11090 від __.__.2021, 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. № 30/4/1-11091 від 08.10.2021, прим. № 1, на 4 арк., відкрита інформація, лише в адресу.

3. Повідомлення про оприлюднення 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), реєстр. № 30/4/1-11092 від 07.07.2021, прим. №1, на 1 арк., відкрита інформація, лише в адресу, підлягає поверненню.

4. Аналіз регуляторного впливу 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) реєстр. № 30/4/1-11093 від 08.10.2021, прим. №1, на 5 арк., відкрита інформація, лише в адресу.

З повагою

Заступник Голови Служби **Володимир ГОРБЕНКО**

Вих. 2 прим.
1 - на адресу
2 - до справи 147
Вик. - С. Винославський
0979424548
08.10.2021.

Прим. № 1

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 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**

Заступник Голови Служби **Володимир ГОРБЕНКО**

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

ЗАТВЕРДЖЕНО
Наказ Служби безпеки України
__._____.2021 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 програмного продукту 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, у разі згоди з публічною угодою 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 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".

~~Т.в.о~~ начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки **Ілля ВІТЮК**

3014/1-11090

ПОЯСНЮВАЛЬНА ЗАПИСКА

до наказу Центрального управління Служби безпеки України від __.__.2021 №_____ "Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" (MISP-UA)"

1. Мета

Метою видання 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)" є нормативно-правове врегулювання порядку та організаціїобміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних системміж суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

2. Обґрунтування необхідності прийняття акта

Необхідність видання наказу обумовлена необхідністю визначення механізму обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем між суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки та врегулювання питань, які не врегульовані нормативно-правовими актами.

3. Основні положення акта

Наказом врегульовується порядок та організація механізму обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем між суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

4. Правові аспекти

Наказ розроблений за власною ініціативою з метою нормативно-правового врегулювання процедури обміну інформацією щодо

кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем між суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки та визначені частиною четвертою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України": міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

5. Фінансово-економічне обґрунтування

Фінансово-економічні розрахунки впливу реалізації наказу на надходження та витрати державного та/або місцевого бюджетів не наводяться, оскільки його реалізація не потребує додаткового фінансування з державного чи місцевого бюджетів.

6. Позиція заінтересованих сторін

Наказ не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування та застосування української мови як державної, сфери наукової та науково-технічної діяльності, а тому не потребує проведення консультацій із заінтересованими сторонами.

Наказ потребує погодження із Адміністрацією Держспецзв'язку, Міністерством цифрової трансформації України, Державною регуляторною службою.

7. Оцінка відповідності

Наказ не стосується зобов'язань України у сфері європейської інтеграції.

У наказі 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 виникнути під час реалізації наказу.

Згідно з пунктом 10 Загального положення про юридичну службу міністерства, іншого органу виконавчої влади, державного підприємства, установи та організації, затвердженого постановою Кабінету Міністрів України від 26.11.2008 № 1040, пункту 14 Порядку проведення тендерно-правової експертизи, затвердженого постановою Кабінету Міністрів України від 28.11.2018 № 977,пункту 3 Порядку проведення органами виконавчої влади антидискримінаційної експертизи проектів нормативно-правових актів, затвердженого постановою Кабінету Міністрів України від 30.01.2013 № 61, Управлінням правового забезпечення СБУ проведено юридичну, гендерно-правову та антидискримінаційну експертизи наказу, за результатами яких визначено, що нормативно-правовий акт розроблений за необхідності правового регулювання управлінської діяльності та в межах повноважень СБУ, відповідає положенням Конституції України, актам законодавства, узгоджується з нормативно-правовими актами такої самої юридичної сили, у тому числі із зареєстрованими в Міністерстві юстиції України, а також не містить правових колізій та норм, що можуть сприяти вчиненню корупційних правопорушень; не містить положень, які не відповідають принципу забезпечення рівних прав та можливостей жінок та чоловіків; не містить положень, що містять ознаки дискримінації.

Наказ не потребує проведення громадської гендерно-правової експертизи, а також громадських антикорупційної та антидискримінаційної експертиз.

Наказ потребує проведення цифрової експертизи (отримано висновок Міністерства цифрової трансформації про її проведення від 17.02.2021 № 1/04-2-1623), оскільки він стосується питань інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства, електронної демократії, надання адміністративних послуг або цифрового розвитку.

Наказ потребує погодження з Міністерством цифрової трансформації України, Державною регуляторною службою та Державною службою спеціального зв'язку та захисту інформації України.

8. Прогноз результатів

Реалізація наказу не матиме впливу на ринкове середовище, забезпечення захисту прав та інтересів суб'єктів господарювання, громадян і держави; розвиток регіонів, підвищення чи зниження спроможності територіальних громад; ринок праці, рівень зайнятості населення; громадське здоров'я, покращення чи погіршення стану здоров'я населення або його окремих груп; екологію та навколишнє природне середовище, обсяг природних ресурсів, рівень забруднення атмосферного повітря, води, земель, зокрема забруднення утвореними відходами, інші суспільні відносини.

Наказ дозволить унормувати порядок та організацію обміну інформацією про кіберінциденти між суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

Заступник Голови Служби безпеки України **Володимир ГОРБЕНКО**

"08" 10 2021 року

3014/1-11091

Оприлюднено на сайті "05" 08 2021 року

ПОВІДОМЛЕННЯ

про оприлюднення 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).

Службою безпеки України розроблений 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" (MISP-UA) (далі - Проект).

Проект необхідний для нормативно-правового 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". Він розміщений на офіційному Web-сайті СБУ (https://ssu.gov.ua/rehuliatorna-diialnist) у відповідному розділі ("Громадянам/ "Нормативно-правова база/ "Законодавство"/ "Регуляторна діяльність" документ).

Зауваження та пропозиції до проекту приймаються в письмовому вигляді або електронною поштою протягом календарного місяця за відповідними адресами:

Служба безпеки України,
вул. Володимирська, 33, м. Київ,
01601 (інформація для ДКІБ)

e-mail: support@dis.gov.ua
тел.: (063) 477-89-55

Голова Служби безпеки України **Іван БАКАНОВ**

"07" 07 2021 року

3094/1-11092

Аналіз регуляторного впливу
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)

І. Визначення проблеми

У зв'язку з невпинною автоматизацією виробничих і управлінських процесів з використанням мережі Інтернет, в Україні істотно зросли ризики ураження технологічних та комунікаційних систем шкідливим програмним забезпеченням. Його небезпеку, що втілюється у багатомільйонні фінансові та інфраструктурні збитки, відчули на собі десятки українських підприємств під час кібератак Petya/NonPetya, BlackEnergy тощо.

Підготовка регуляторного акта зумовлена необхідністю 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).

Визначення основних груп (підгруп), на які проблема справляє вплив:

Групи, на які наказ справляє вплив	**Так**	**Ні**
Громадяни		Ні
Держава	Так	
Суб'єкти забезпечення кібербезпеки	Так	

ІІ. Цілі державного регулювання

Розробка зазначеного проекту нормативно-правового акту спрямована на визначення порядку здійснення інформаційного обміну між суб'єктами забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції, заходи із забезпечення кібербезпеки, визначені частиною четвертою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України".

ІІІ. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	**Опис альтернативи**
1. Неприйняття наказу ЦУ СБУ	відсутність чіткого порядку здійснення інформаційного обміну між суб'єктами забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції суб'єкти забезпечення кібербезпеки.

Вид альтернативи	Опис альтернативи
2. Прийняття наказу ЦУ СБУ	дозволить на рівні нормативно-правового акта врегулювати відносини у сфері обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем з використанням MISP-UA. Зазначений спосіб на даний час є оптимальним для досягнення поставлених цілей та не вимагає додаткових витрат.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернатив	Вигоди	Витрати
1. Неприйняття наказу ЦУ СБУ	Зазначений спосіб не є доцільним, оскільки він не вирішує проблемних питань.	Немає
2. Прийняття наказу ЦУ СБУ	дозволить на рівні нормативно-правового акта врегулювати відносини, зокрема порядок здійснення інформаційного обміну, що виникають у процесі залучення суб'єктів забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції, заходи із забезпечення кібербезпеки	Немає

Оцінка впливу на сферу забезпечення кібербезпеки

Вид альтернативи	Вигоди	Витрати
1. Неприйняття наказу ЦУ СБУ	Відсутні	Відсутні
2. Прийняття наказу ЦУ СБУ	дозволяє встановити порядок здійснення інформаційного обміну між суб'єктами забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції, заходи із забезпечення кібербезпеки,	Відсутні

Вид альтернативи	Вигоди	Витрати
	визначені частиною четвертою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України"	

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
1. Неприйняття наказу ЦУ СБУ	Відсутні	Відсутні
2. Прийняття наказу ЦУ СБУ	Відсутні	Відсутні

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного балу
1. Неприйняття наказу СБУ	1	Проблема продовжить існувати
2. Прийняття наказу СБУ	4	При прийнятті регуляторного акту ціль буде досягнута повною мірою

Негативних результатів від прийняття регуляторного акта не очікується.

V. Механізм та заходи, які забезпечать розв'язання визначеної проблеми

Для розв'язання визначеної проблеми пропонується такий механізм, який спрямований на запровадження порядку обміну інформацією з використанням MISP-UA між суб'єктами забезпечення кібербезпеки щодо кібератак, кіберінцидентів, інших кіберзагроз, технічними даними про ідентифікатори компрометації інформаційних систем.

Для суб'єктів забезпечення кібербезпеки, які виявили бажання здійснювати обмін інформацією з використанням MISP-UA необхідно:

ознайомитися з положеннями проекту регуляторного акта;

повідомити ДКІБ СБ України про намір здійснювати обмін інформацією з використанням MISP-UA та направити відповідну заявку на підключення, яка розміщена на офіційному ресурсі Служби безпеки України.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Державне регулювання не передбачає утворення нового державного органу або нового структурного підрозділу діючого органу.

Витрати органів державної влади на виконання вимог регулювання не передбачаються, у зв'язку із чим додаток 3 до Методики проведення аналізу впливу регуляторного акта не розроблявся.

Прийняття запропонованого проекту акта сприятиме здійсненню інформаційного обміну між суб'єктами забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції, заходи із забезпечення кібербезпеки, визначені частиною четвертою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України".

Прийняття та оприлюднення акта в установленому порядку забезпечить доведення його до відома суб'єктів забезпечення кібербезпеки. Вимоги регуляторного акта є обов'язковими для виконання суб'єктами забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції, заходи із забезпечення кібербезпеки та використовують MISP-UA.

Прийняття проекту акта не призведе до неочікуваних результатів і не потребуватиме додаткових витрат з державного бюджету.

Можлива шкода в разі очікуваних наслідків дії акта не прогнозується. До зовнішніх чинників, які потенційно можуть впливати на дію запропонованого регуляторного акта, можна віднести зміни в законодавчих актах України.

Нагляд за додержанням вимог цього акта здійснюватиметься Службою безпеки України.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії 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) не встановлюється, оскільки його застосування пропонується здійснювати на постійній основі.

Він може бути змінений у разі внесення відповідних змін до законодавства.

Строк набрання чинності регуляторним актом: відповідно до законодавства – з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Основні показники результативності дії регуляторного акта:

кількість суб'єктів забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції, заходи із забезпечення кібербезпеки з використанням адаптованого програмного продукту Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" (MISP-UA);

рівень поінформованості суб'єктів забезпечення кібербезпеки щодо основних положень акта.

Запропоновані зміни дозволять забезпечити досягнення визначених цілей. Перешкод для реалізації норм цього регуляторного акту у разі його прийняття немає.

Прийняття запропонованого регуляторного акта визначить порядок здійснення інформаційного обміну між суб'єктами забезпечення кібербезпеки, які безпосередньо здійснюють, у межах своєї компетенції, заходи із забезпечення кібербезпеки, визначені частиною четвертою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України".

Проект регуляторного акта розміщений на офіційному Web-сайті Служби безпеки України (https://ssu.gov.ua/rehuliatorna-diialnist) 07.08.2021.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Стосовно регуляторного акта буде здійснюватися базове, повторне та періодичне відстеження його результативності у строки, установлені статтею 10 Закону України "Про засади державної регуляторної політики у сфері господарської діяльності".

Базове відстеження результативності регуляторного акта буде здійснено через 1 рік після набрання ним чинності шляхом аналізу та підрахунку статистичних даних.

Повторне відстеження буде здійснюватися через 2 роки після набрання чинності цим регуляторним актом, під час якого проводитиметься моніторинг інформації щодо кількості зареєстрованих користувачів MISP-UA.

У результаті повторного відстеження відбудеться порівняння показників базового та повторного відстеження.

Вид даних, за допомогою яких здійснюватиметься відстеження результативності, – статистичні.

Цільові групи, які будуть залучатися для проведення відстеження – Служба безпеки України та її регіональні органи, суб'єкти забезпечення кібербезпеки, які безпосередньо користуються MISP-UA.

Заступник Голови Служби безпеки України **Володимир ГОРБЕНКО**

08 10 2021 року

30/4/1-11093