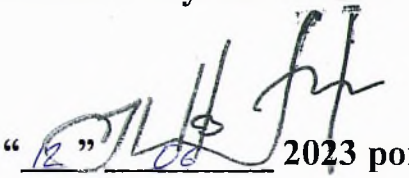
Прим№__

ЗАТВЕРДЖЕНО

Голова Служби безпеки України



Василь МАЛЮК

“ 12 ” 06 2023 року

ПЛАН
діяльності Служби безпеки України з підготовки проектів регуляторних актів на 2023 рік

№ з/п	Вид і назва проекту регуляторного акта	Ціль прийняття проекту регуляторного акта	Строк підготовки проекту регуляторного акта	Функціональні підрозділи, відповідальні за розроблення проекту регуляторного акта
	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)”	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	Протягом року	ДКІБ СБУ, УПЗ СБУ

№ з/п	Вид і назва проекту регуляторного акта	Ціль прийняття проекту регуляторного акта	Строк підготовки проекту регуляторного акта	Функціональні підрозділи, відповідальні за розроблення проекту регуляторного акта
		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. Для визначення механізму обміну інформацією щодо кіберінцидентів та врегулювання питань, які не врегульовані нормативно-правовими актами, розроблений згаданий проект		

Начальник Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України

Ілля ВІТЮК

Оприлюднено на сайті "__" _____ 2023 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 вебсайті 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 на електронну пошту 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 **Василь МАЛЮК**

"12" 06 2023 року

ПОЯСНЮВАЛЬНА ЗАПИСКА
до наказу Центрального управління Служби безпеки України від __.__.2023 №_____ "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 організації 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.

2. Обґрунтування необхідності прийняття акта

Видання наказу обумовлено 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 врегульовуються 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.

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, пунктом 14 Порядку проведення гендерно-правової експертизи, затвердженого постановою Кабінету Міністрів України від 28.11.2018 № 977, пунктом 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 Міністерством цифрової трансформації України, 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 містить ознаки регуляторного акта, а тому потребує погодження з Державною регуляторною службою України.

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

Голова Служби безпеки України **Василь МАЛЮК**

"12" 06 2023 року

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)"

I. 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. Цю небезпеку, що спричиняє 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)", розробленого Ситуаційним центром забезпечення кібербезпеки СБУ.

Визначення впливу:

Групи (підгрупи), на які наказ впливає	**Так**	**Ні**
Громадяни	-	+
Держава	+	-
Суб'єкти забезпечення кібербезпеки	+	-

II. Цілі державного регулювання

Розробка зазначеного проекту нормативно-правового акта 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".

III. 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 забезпечення кібербезпеки
2. Прийняття наказу ЦУ СБУ	Можливість на рівні нормативно-правового акта врегулювати відносини у сфері обміну

Вид альтернативи	Опис альтернативи
	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	Не вирішує проблемних питань	Відсутні можливості на рівні нормативно-правового акта врегулювати відносини щодо здійснення інформаційного обміну, що виникають у процесі залучення суб'єктів забезпечення кібербезпеки, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
2. Прийняття наказу ЦУ СБУ	Можливість 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	Утримання системи "MISP-UA" буде здійснюватися в межах бюджетних коштів СБУ. Витрати на виконання запланованого регулювання будуть здійснюватися в межах бюджетних коштів, виділених на фінансування СБУ, та складуть розрахунково 117,78 грн за 1 рік (розрахунки витрат наведені в додатку 4)

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання – власників об'єктів сервісу або інженерних комунікацій та мереж, що підпадають під дію регулювання, одиниць	-	-	1	-	1
Питома вага групи у загальній кількості, відсотків	-	-	100	-	100

Оскільки кількість суб'єктів господарювання, що виявлять бажання підключитися до системи на даному етапі, встановити неможливо, розрахунки витрат здійснені на одного умовного суб'єкта господарювання малого підприємництва.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Вид альтернативи	Вигоди	Витрати
1. Неприйняття наказу ЦУ СБУ	Відсутні	Відсутня можливість встановлення чіткого порядку здійснення інформаційного обміну між суб'єктами забезпечення кібербезпеки, які безпосередньо здійснюють у межах своєї компетенції заходи, визначені частиною четвертою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України"
2. Прийняття наказу ЦУ СБУ	Встановлення 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	Для суб'єктів господарювання, які виявили бажання долучитися до системи "MISP-UA", витрати на авторизацію та реєстрацію на офіційному сайті системи "MISP-UA" розрахунково складуть 78,52 грн одноразово (згідно з додатком 4 до Методики). Отримання та обмін інформацією в системі "MISP-UA" буде

Вид альтернативи	Вигоди	Витрати
	Закону України "Про основні засади забезпечення кібербезпеки України"	здійснюватися на безоплатній основі.

Оцінка впливу на сферу інтересів громадян

Проект регуляторного акта не має прямого впливу на сферу інтересів громадян.

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	**Держава:** відсутні	**Держава:** відсутня можливість встановити 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"	Продовження існування проблеми

	Громадяни: відсутня	**Громадяни:** витрати коштів на відновлення комп'ютерної техніки та подолання інших наслідків, пов'язаних із кібератаками	
	Суб'єкти господарювання: відсутні	**Суб'єкти господарювання:** відсутня можливість обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем з використанням	
Альтернатива 2	**Держава:** відсутня можливість встановити 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	**Держава:** відсутні	Досягнення цілей державного регулювання та вирішення існуючої проблеми

	Закону України “Про основні засади забезпечення кібербезпеки України” **Громадяни:** витрати коштів на відновлення комп’ютерної техніки та інших наслідків, пов’язаних із кібератаками **Суб’єкти господарювання:** відсутня можливість обміну інформацією щодо кібератак, кіберінцидентів, інших кіберзагроз та технічними даними про ідентифікатори компрометації інформаційних систем з використанням MISP-UA	**Громадяни:** відсутні **Суб’єкти господарювання:** відсутні	

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	**Бал результативності (за чотирибальною системою оцінки)**	**Коментарі щодо присвоєння відповідного бала**
1. Неприйняття наказу СБУ	1	Проблема продовжить існувати
2. Прийняття наказу СБУ	3	При прийнятті регуляторного акта основні цілі будуть досягнуті

Негативних результатів від прийняття регуляторного акта не очікується.

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

Для розв'язання визначеної проблеми пропонується 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.

Користування MISP-UA здійснюється на безоплатній основі.

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.

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".

Витрати суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки на виконання вимог регулювання, наведені у додатку 4 до Методики проведення аналізу впливу регуляторного акта (оскільки кількість суб'єктів господарювання, які виявлять бажання підключитися до системи, на даному етапі встановити неможливо, розрахунки витрат здійснені на одного умовного суб'єкта господарювання малого підприємництва).

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:

розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта, не зміниться;

кількість суб'єктів господарювання та/або фізичних осіб, на яких поширюватиметься дія акта;

розмір коштів і кількість часу, що витрачатимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта;

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта – високий.

Проект регуляторного акта розміщений на офіційному вебсайті Служби

Додаткові показники:

кількість суб'єктів господарювання, яким наданий доступ до системи "MISP-UA";

кількість суб'єктів господарювання, яким припинений доступ у системі "MISP-UA" внаслідок порушень ними умов безпеки (користування);

кількість скарг/звернень від суб'єктів господарювання, пов'язаних із дією 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)";

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.

Василь МАЛЮК

12 06 2023 року

Додаток 4
до Методики проведення аналізу впливу
регуляторного акта

ТЕСТ
малого підприємництва (М-Тест)

1. Консультації з представниками мікро- та малого підприємництва щодо оцінки впливу регулювання

Консультації щодо визначення впливу запропонованого регулювання на суб'єктів малого підприємництва та визначення детального переліку процедур, виконання яких необхідно для здійснення регулювання, розробником не проводилися у зв'язку з відсутністю звернень від суб'єктів господарювання.

Порядковий номер	**Вид консультації (публічні консультації прямі (круглі столи, наради, робочі зустрічі тощо), інтернет-консультації прямі (інтернет-форуми, соціальні мережі тощо), запити (до підприємців, експертів, науковців тощо)**	**Кількість учасників консультацій, осіб**	**Основні результати консультацій (опис)**
1	Пропозиції та зауваження до проекту акта за результатами громадського обговорення будуть розглянуті у разі їх надходження	Не визначено	

2. Вимірювання впливу регулювання на суб'єктів малого підприємництва (мікро- та малі):

кількість суб'єктів малого підприємництва – оскільки кількість суб'єктів господарювання, які виявлять бажання підключитися до системи, на даному етапі встановити неможливо, розрахунки витрат здійснені на одного умовного суб'єкта господарювання малого підприємництва.

3. Розрахунок витрат суб'єктів малого підприємництва на виконання вимог регулювання

Порядковий номер	Найменування оцінки	У перший рік (стартовий рік впровадження регулювання)	Періодичні (за наступний рік), грн	Витрати за п'ять років
Оцінка "прямих" витрат суб'єктів малого підприємництва на виконання регулювання				
1	Придбання необхідного обладнання (пристроїв, машин, механізмів)	-	-	-

2	Процедури повірки та/або постановки на відповідний облік у визначеному органі державної влади чи місцевого самоврядування	-	-	-
3	Процедури експлуатації обладнання (експлуатаційні витрати - витратні матеріали)	-	-	-
4	Процедури обслуговування обладнання (технічне обслуговування)	-	-	-
5	Інші процедури (уточнити):	-		
6	Разом (сума рядків 1+2+3+4), грн	0	0	0
7	Кількість суб'єктів господарювання, що повинні виконати вимоги регулювання в частині отримання дозволів, одиниць	1		
8	Сумарно (рядок 6 х рядок 7), гривень	0	0	0
Оцінка вартості адміністративних процедур суб'єктів малого підприємництва щодо виконання регулювання та звітування				
9	Процедури отримання первинної інформації про вимоги регулювання	1 год. х 39,26* грн = 39, 26 грн	0	39, 26
10	Процедури організації виконання вимог регулювання (авторизація та реєстрація на сайті, направлення заявки про приєднання до системи тощо)	1 год. х 39,26 грн = 39, 26 грн	0	39, 26
11	Процедури офіційного звітування	-	-	-
12	Процедури щодо забезпечення процесу перевірок	-	-	-
13	Інші процедури (уточнити)	X	X	X
14	Разом, гривень (сума рядків 9+10+11+12+13а)	78, 52	-	39, 26

15	Кількість суб'єктів малого підприємництва, що повинні виконати вимоги регулювання в частині отримання дозволів на влаштування заїзду/виїзду та перехідно-швидкісних смуг до об'єкта дорожнього сервісу, одиниць	1		
16	Сумарно, гривень (рядок 14 х рядок 15)	78, 52	-	78, 52

*Відповідно до Закону України про Державний Бюджет України на 2022 рік мінімальна оплата праці за 1 годину складає 39, 26 грн.

БЮДЖЕТНІ ВИТРАТИ
на адміністрування регулювання для суб'єктів малого і мікропідприємництва

Розрахунок витрат на адміністрування регулювання здійснюється окремо для кожного відповідного органу державної влади чи органу місцевого самоврядування, що залучений до процесу регулювання.

Державний орган, для якого здійснюється розрахунок адміністрування регулювання:

Служба безпеки України

Процедура регулювання суб'єктів малого підприємництва (розрахунок на одного типового суб'єкта господарювання малого підприємництва – за потреби окремо для суб'єктів малого та мікропідприємництва)	**Планові витрати часу на процедуру, год.**	**Вартість часу співробітника органу державної влади відповідної категорії (заробітна плата), грн**	**Оцінка кількості процедур за рік, що припадають на одного суб'єкта**	**Оцінка кількості суб'єктів, що підпадають під дію процедури регулювання**	**Витрати на адміністрування регулювання * (за рік), гривень**
1. Облік суб'єкта господарювання, що перебуває у сфері регулювання	1	39, 26	1	1	39, 26
2. Поточний контроль за суб'єктом господарювання, що перебуває у сфері регулювання, у тому числі:	1	39, 26	1	1	39, 26
камеральні	1	39, 26	1	1	39, 26
виїзні	-	-	-	-	-

3. Підготовка, затвердження та опрацювання одного окремого акта про порушення вимог регулювання	-	-	-	-	-
4. Реалізація одного окремого рішення щодо порушення вимог регулювання (припинення доступу до системи)	1	39, 26	1	1	39, 26
5. Оскарження одного окремого рішення суб'єктами господарювання	-	-	-	-	-
6. Підготовка звітності за результатами регулювання	-	-	-	-	-
7. Інші адміністративні процедури (уточнити)	-	-	-	-	-
Разом за рік	3	39, 26	1	1	117, 78
Сумарно за п'ять років	3	39, 26	1	1	221, 70

* Вартість витрат, пов'язаних з адмініструванням процесу регулювання державними органами, визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації та на кількість суб'єктів, що підпадають під дію процедури регулювання, та на кількість процедур за рік.

Державне регулювання не передбачає утворення нового державного органу (або нового структурного підрозділу діючих органів).

4. Розрахунок сумарних витрат суб'єктів малого підприємництва, що виникають на виконання вимог регулювання

Порядковий номер	**Показник**	**Перший рік регулювання (стартовий)**	**За п'ять років**
1	Оцінка "прямих" витрат суб'єктів малого підприємництва на виконання регулювання в частині отримання дозволів	0	0
1	Оцінка "прямих" витрат суб'єктів малого підприємництва на виконання регулювання	0	0

2	Оцінка вартості адміністративних процедур для суб'єктів малого підприємництва щодо виконання регулювання	78, 52	78, 52
3	Сумарні витрати малого підприємництва на виконання запланованого регулювання	78, 52	78, 52
4	Бюджетні витрати на адміністрування регулювання суб'єктів малого підприємництва	117, 78	221, 70
5	Сумарні витрати на виконання запланованого регулювання	196, 30	300, 22

5. Розроблення коригуючих (пом'якшувальних) заходів для малого підприємництва щодо запропонованого регулювання не передбачено.

Прим. № —

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 **Василь МАЛЮК**

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

ЗАТВЕРДЖЕНО
Наказ Служби безпеки України
__ _____ 2023 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 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.

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, які безпосередньо здійснюють у межах своєї компетенції заходи із 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, які безпосередньо здійснюють у межах своєї компетенції заходи із 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, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, до MISP-UA, за умови відсутності законодавчо визначених обмежень (зобов'язань), дотримання міжнародного стандарту TRAFFIC LIGHT PROTOCOL (далі – TLP) згідно витягу із протоколу № 21 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 9 лютого 2023 року;

дозволяється використовувати дані MISP-UA, внесені іншими суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із 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, який безпосередньо

здійснює в межах своєї компетенції заходи із забезпечення кібербезпеки та 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, які безпосередньо здійснюють у межах своєї компетенції заходи із 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, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, виконується на безоплатній основі на підставі спільного рішення, у разі згоди з публічною угодою про організацію взаємодії з питань обміну інформацією з використанням MISP-UA між СБУ та згаданими суб'єктами.

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, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, до MISP-UA застосовується 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 СБ України

Ілля ВІТЮК