Додаток
до Плану реагування на кіберінциденти
у Баштанській районній державній
(військовій) адміністрації

Картка інформування про кіберінцидент/кібератаку

Примітка: *1. Для позначення потрібних варіантів підкреслити (обвести, виділити кольором) обраний варіант.* *2. Намагатися вказати якомога більше інформації, заповнивши відповідні поля.*

TLP				
RED	AMBER	AMBER + STRICT	GREEN	CLEAR
Дата та час виявлення кіберінциденту/кібератаки:	____.____.____ ___:___:___ GMT _____			

Заявник			
П. І. Б.:		Електронна адреса:	
Посада:		Номер телефону:	
Суб'єкт забезпечення кібербезпеки:			

Джерело виявлення кіберінциденту/кібератаки			
Адміністратор	Користувач	Антивірусне ПЗ	EDR
IDS/IPS	Інше (вказати): _____		

Запропонована категорія (рівень) критичності кіберінциденту/кібератаки	
0, некритичний (білий)	1, низький (зелений)
2, середній (жовтий)	3, високий (помаранчевий)
4, критичний (червоний)	5, надзвичайний (чорний)
Не вдалося визначити	

Отримана інформація
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Постраждалий суб'єкт забезпечення кібербезпеки			
Юридична назва:			
Адреса:			
Електронна адреса:		Номер телефону:	
Контактна особа 1			
П. І. Б.:		Електронна адреса:	
Посада:		Номер телефону:	
Контактна особа 2			
П. І. Б.:		Електронна адреса:	
Посада:		Номер телефону:	

Сектор (галузь) атакованого об'єкта			
Сектор безпеки і оборони	Органи державної влади	Органи місцевого самоврядування	Енергетичний сектор
Сфера електронних комунікаційних послуг	ІТ сектор	Транспортна галузь	Фінансовий сектор
Підприємства та організації відповідної форми власності	Засоби масової інформації	Інші критичні організації	Інше (вказати): _____ _____

Доменна зона			
UAGOV Український державний	UACOM Український недержавний	FGOV Закордонний державний	FCOM Закордонний недержавний
Відношення України до кіберінциденту/кібератаки			
Україна - об'єкт атаки	Україна - джерело атаки	Україна - елемент механізму атаки	не стосується території України
Інше (вказати): _____			

Категорія та тип кіберінциденту (відповідно до Переліку категорій та типів кіберінцидентів)

Код	*Категорія кіберінциденту*	*Код*	*Тип кіберінциденту*
01	Шкідливий (образливий) вміст (Abusive content)	01	Спам
02	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (ШПЗ)
		02	Розповсюдження ШПЗ
		03	Командно-контрольний центр (С2)
		04	Шкідливе підключення

03	Збір інформації зловмисником (Information Gathering)	01	Сканування
		02	Сніфінг
		03	Фішинг
04	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості
		02	Спроби авторизації / входу в систему
05	Втручання (Intrusion)	01	Компрометація облікового запису
		02	Компрометація системи
06	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні
		02	Саботаж / шкідливі дії
		03	Збій
07	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації
		02	Несанкціонована модифікація
08	Шахрайство (Fraud)	01	Шахрайський сайт
09	Відома вразливість (Vulnerable)	01	Вразливість
		03	Некоректна конфігурація
10	Інше (Other)	01	Невизначений інцидент

Дата та час початку кіберінциденту/кібератаки:	___.___._____ ___:___:___ GMT ____

Чи пов'язаний цей (ця) кіберінцидент/кібератака з попередніми?

ТАК	НІ	ID пов'язаного кіберінциденту/ кібератаки: _____	Невідомо

Короткий опис кіберінциденту/кібератаки

_____

_____

_____

_____

_____

_____

Вплив на функціонування систем/мереж, сервіси (послуги)

Немає впливу взагалі	Немає впливу на сервіси (послуги)
Мінімальний вплив на некритичні сервіси (послуги)	Мінімальний вплив на критичні сервіси (послуги)
Значний вплив на некритичні сервіси (послуги)	Значний вплив на некритичні сервіси (послуги)
Втрата доступності некритичних сервісів (послуг)	Втрата доступності критичних сервісів (послуг)

Кількість скомпрометованих систем/мереж (ЕОМ)

1 - 10	10 - 50	Інше (вказати): _____	Невідомо

Тип скомпрометованої системи/мережі за функціоналом			
Робочі станції	Сервер(и) додатків	Сервер(и) баз даних	Вебсервер(и)
Сервери доменних імен	Поштовий сервер	Брандмауер(и)	Мережеве обладнання
Інше (вказати): _____			
Об'єкт кібератаки			
Тип (модель):			
Ім'я:			
Операційна система:			
Дата встановлення ОС:			
Часова зона:			
Мережеві налаштування:			
Облікові записи:			
CVE:	CVE-____-____	CVE-____-____	CVE-____-____
Висновок: _____ _____ _____			
Тип (модель):			
Ім'я:			
Операційна система:			
Дата встановлення ОС:			
Часова зона:			
Мережеві налаштування:			
Облікові записи:			
CVE:	CVE-____-____	CVE-____-____	CVE-____-____
Висновок: _____ _____ _____ _____			
Тип (модель):			
Ім'я:			
Операційна система:			
Дата встановлення ОС:			
Часова зона:			
Мережеві налаштування:			
Облікові записи:			

CVE:	CVE-____-____	CVE-____-____	CVE-____-____
Висновок: _____ _____ _____			

Чи вирішено кіберінцидент/кібератаку?		**Чи потрібна допомога CERT-UA?**	
Так	Ні	Так	Ні

Чи повідомлялося про кіберінцидент/кібератаку іншим основним суб'єктам забезпечення кібербезпеки? Яким саме?

Так		Ні	
Служба безпеки України		Міністерство оборони України та Генеральний штаб Збройних Сил України	Розвідувальні органи
Національний банк України		Національна поліція України	Національний координаційний центр кібербезпеки при РНБО України
Департамент кіберполіції Національної поліції України		Коментар: _____ _____	

Чи залучалися сторонні організації до вирішення кіберінциденту/кібератаки?

Так		Ні	
Інший CERT, CSIRT, SOC	Антивірусні компанії	Обслуговуюча компанія, інтегратор, представник вендора	Інше (вказати): _____ _____

Коментар:_____
_____
_____
_____
_____

Результат впливу

Витік даних	Злам (компрометація) системи	Втрата функціональності систем/сервісів	Інше (вказати): _____ _____

Від потенційного впливу кіберінциденту/кібератаки на державному рівні під загрозою

Національна безпека	Сталість економіки	Національний імідж	Функціонування Уряду
Безпека персональних даних громадян	Інше: _____		

Індикатори компрометації		
Мережеві:		
IP/домен/URI./User Agent	Коментар	
Хостові:		
Шлях / команда / сервіс / заплановане завдання / гілка реєстру	Коментар	
Файлові:		
Хешсума файлу	Назва файлу	Коментар
MD5 (приклад): [хешсума]		
Перелік отриманих даних		
Хешсума файлу	Назва файлу	Коментар
MD5 (приклад): [хешсума]		