*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*23.05.2025 №681*

#### *ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ*

#### *ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ*

#### *Загальні положення*

* 1. План реагування на інциденти кібербезпеки виконавчого комітету Криворізької міської ради (надалі – План реагування) є основою процесу управління інцидентами інформаційної безпеки у виконкомі Криворізької міської ради.
	2. План реагування передбачає процес керування інцидентами та подіями інформаційної безпеки й встановлює вказівки для посадових осіб і структурних підрозділів виконкому міської ради на інциденти, які вважають, що виявили інцидент безпеки або реагують на нього.
	3. Основними завданнями Плану реагування на інциденти є:

1.3.1 визначення можливих джерел інцидентів і їх впливу на інформаційні ресурси та системи виконкому Криворізької міської ради;

1.3.2 уточнення розміру можливих втрат і збитків;

1.3.3 визначення характеру та обсягів невідкладних дій і відновлювальних робіт, проведення розрахунків сил і засобів, необхідних для їх виконання;

1.3.4 визначення порядку та організації взаємодії, всебічного забезпечення дій та управління ними залежно від виду інциденту.

* 1. План реагування розроблено відповідно до:
		1. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги» (надалі – ISO 27001);
		2. ДСТУ EN ISO/IEC 27701:2022 (EN ISO/IEC 27701:2021, IDT; ISO/IEC 27701:2019, IDT) «Методи безпеки. Розширення до ISO/IEC 27001 і ISO/IEC 27002 для управління конфіденційною інформацією. Вимоги та вказівки» (надалі – ISO 27701);
		3. GDPR 2016/679 «Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/EC» (Загальний регламент про захист даних – GDPR).
	2. План реагування взаємопов’язаний із:
	3. Системою управління інформаційною безпекою «Сфера застосування СУІБ»;
	4. Системою управління інформаційною безпекою «Політика інформаційної безпеки»;
	5. Системою управління інформаційною безпекою «Політика захисту персональних даних»;
	6. Системою управління інформаційною безпекою «Політика класифікації інформації»;
	7. Системою управління інформаційною безпекою «Політика контролю доступу»;
	8. Системою управління інформаційною безпекою «Процедура управління інцидентами».

***2. Терміни, визначення та скорочення Плану реагування***

2.1. Для плану реагування застосовуються терміни та визначення згідно з переліком нормативних документів:

2.1.1 ДСТУ EN ISO/IEC 27000:2022 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд та словник термінів» (EN ISO/IEC 27000:2020, IDT; ISO/IEC 27000:2018, IDT)» (надалі – ДСТУ ISO/IEC 27000);

2.1.2 ISO 27701;

2.1.3 Загальний регламент про захист даних (GDPR);

2.1.4 ДСТУ EN ISO/IEC 29100:2022 (EN ISO/IEC 29100:2020, IDT; ISO/IEC 29100:2011, including Amd 1:2018, IDT) «Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя» (надалі – ДСТУ ISO/IEC 29100);

2.1.5 D4.1-СУІБ Політика інформаційної безпеки;

2.1.6 D00TD -СУІБ Основний перелік термінів, визначень і скорочень:

2.1.6.1 СУІБ – система управління інформаційною безпекою;

2.1.6.2 DPO – уповноважена особа із захисту персональних даних;

2.1.6.3 CSO – відповідальний за інформаційну безпеку, який відповідає за організацію процесу забезпечення безпеки у виконкомі Криворізької міської ради, включаючи фізичну безпеку, кібербезпеку та інші види безпеки в межах сфери застосування СУІБ;

2.1.6.4 СEO – власник і розпорядник СУІБ;

2.1.6.5 CISO – керівник підрозділу інформаційної безпеки виконкому Криворізької міської ради;

2.1.6.6 КЗІ (криптографічний захист інформації) – вид захисту інформації, що реалізується шляхом її перетворення з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

2.1.6.7 IRT (Incident Response Team) – група реагування на інциденти;

2.1.6.8 AdIRT – адміністратор управління інцидентами інформаційної безпеки;

2.1.6.9 Ad1 – адміністратор безпеки;

2.1.6.10 Ad2 – адміністратор системи;

2.1.6.11 Ad3 – адміністратор баз даних;

2.1.6.12 AdAvr – адміністратор антивірусного захисту;

2.1.6.13 ІБ – інформаційна безпека;

2.1.6.14 BYOD (Bring your own device) – це IT-політика, згідно з якою посадовим особам дозволено або рекомендується використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки) для доступу до даних і систем;

2.1.6.15 CVE — база даних загальновідомих вразливостей інформаційної безпеки;

2.1.6.16 Подія безпеки — це спостережувана подія, що стосується порушення доступності, цілісності або конфіденційності інформаційних активів, систем або мереж, що перебувають у користуванні виконкому Криворізької міської ради;

2.1.6.17 Інцидент безпеки – це подія безпеки, що призводить до втрати або пошкодження властивостей інформації: конфіденційності, доступності, цілісності або конфіденційності (приватності) контрольованих виконкомом Криворізької міської ради даних, систем або мереж;

* + - 1. Eлементи керування конфіденційністю (privacy) – заходи, що запобігають ризикам порушення конфіденційності персональних даних (надалі – PII) шляхом зменшення їх ймовірності або їх наслідків.

#### *3. Звітування про інциденти та документування*

**3.1. Звітність:**

* + 1. якщо посадовій особі виконкому Криворізької міської ради, користувачу Єдиної інформаційної системи або третій стороні, дотичній до області дії СУІБ, стає відомо про подію або інцидент у сфері інформаційної безпеки, можливий інцидент, неминучий інцидент, несанкціонований доступ, порушення політик СУІБ, слабкість безпеки або підозрілу активність, вони повинні негайно повідомити DPO, CSO, IRT за допомогою встановленого каналу зв'язку;
		2. звіти повинні містити конкретні подробиці про те, що було спостережено або виявлено.
	1. **Ступінь критичності інциденту:**
		1. Адміністратор IRT (або інша уповноважена особа за розпорядженням CEO), відповідальний за моніторинг звітів про інциденти або події безпеки, повинен стежити за заявками про інциденти та події і визначити серйозність заявок на основі наведених нижче категорій:
			1. S1 – Високий рівень критичності:
				1. скомпрометовано/пошкоджено критичні (суттєві) інформаційні або важливі системи виконкому Криворізької міської ради, у результаті чого вплив на інформаційну діяльність виконкому Криворізької міської ради може бути руйнівним;
				2. у разі виявлення порушень рівня S1 – негайно оповістити посадових осіб по каналах, визначених у п.3.1 Плану реагування, та вжити невідкладних заходів у межах виконання вимог Процедур управління інцидентами;
			2. S2 – Середній рівень критичності:
				1. скомпрометовано/пошкоджено середньої важливості некритичні інформаційні системи виконкому Криворізької міської ради, виявлено порушення Політики інформаційної безпеки, припинено важливі процеси виконкому Криворізької міської ради;
				2. у разі виявлення порушень рівня S2 – сповістити Адміністратора IRT через довірені канали зв'язку, що визначені в пункті 3.1 Плану реагування, та сумісно з Адміністратором IRT ужити заходів у межах виконання вимог Процедур управління інцидентами: створити заявку з початковими даними про подію безпеки або інцидент ІБ;
				3. упевнитися, що інцидент зареєстрований у адміністратора управління інцидентами інформаційної безпеки (надалі – AdIRT) і повідомити безпосереднього керівника структурного підрозділу з посиланням на номер заявки стосовно події безпеки або інциденту ІБ;
				4. AdIRT формує документ за формою, що наведена в додатку до Плану реагування – Типова форма збору даних про інциденти, надає пріоритет і призначає відповідний структурний підрозділ виконкому міської ради/посадову особу для обробки інциденту;
			3. S3 – Низький рівень критичності:
				1. проблеми такого рівня — це підозри або дивна поведінка користувача, Системи, які не перевірені та потребують додаткового дослідження. Немає чіткого показника того, що Системи мають відчутний ризик і не вимагають екстреного реагування. Це стосується втраченого/викраденого ноутбука з шифруванням диска, підозрілих електронних листів, збоїв, дивної активності на ноутбуці тощо;
				2. у разі виявлення порушень рівня S3 – створити заявку стосовно події або інциденту S3. Заявка повинна бути заповнена, а відповідна посадова особа має бути повідомлена через довірений канал, визначений у пункті 3.1 Плану реагування.
	2. **Документація:**
		1. усі зареєстровані події безпеки, інциденти та заходи реагування мають бути задокументовані у виконкомі Криворізької міської ради відповідно до вимог D14.20-СУІБ Процедур управління інцидентами;
		2. аналіз першопричин необхідно виконувати для всіх інцидентів безпеки, включаючи S3. Звіт про аналіз першопричини повинен бути задокументований відповідно до вимог D14.20-СУІБ Процедур управління інцидентами. Аналіз першопричин повинен бути переглянутий CSO, який визначає подальші дії з обробки інциденту, ризиків і визначення контрзаходів тощо.

#### *4. Операційний план реагування на інциденти інформаційної безпеки*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***№******п\п*** | ***Перелік заходів реагування*** | ***Відповідальний*** | ***Термін******виконання*** | ***Необхідні*** ***ресурси*** |
| ***Інцидент: Несанкціонований доступ до Єдиної інформаційної системи та інформаційних Активів*** |
| 1 | Мережева ізоляція компонентів підсистем Єдиної інформаційної системи на час обробки інциденту | CSO | не більше30 хв. | наявні в користуванні адміністратора Єдиної інформаційної системи та адміністраторів підсистем |
| 2 | Припинення можливості внесення змін даних і створення копії | CSO | не більше30 хв. | наявні в користуванні |
| 3 | Зміна паролів доступу | CISO/Ad1 | не більше30 хв. | наявні в користуванні |
| 4 | Зміна конфігурації серверів | CISO/Ad2 | не більше12 год. | наявні в користуванні |
| 5 | Аналіз протоколів подій | CISO/посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3)  | не більше доби | наявні в користуванні |
| 6 | Проведення службового розслідування  | CSO, DPO | не більше 2 місяців | створення комісії, адміністраторів Єдиної інформаційної системи |
| ***Інцидент: Вірусні епідемії, атаки, шпигунське та інше зловмисне програмне забезпечення*** |
| 1 | Мережева ізоляція компонентів підсистем Єдиної інформаційної системи на час обробки інциденту | CSO | не більше30 хв. | наявні в користуванні |
| 2 | Повне антивірусне сканування компонентів підсистем Єдиної інформаційної системи | CIO, AdAvr (адміністратор антивірусного захисту) | не більше12 год. | наявні в користуванні |
| 3 | Пошук і видалення шкідливих програм, невідомих постачальникам антивірусів  | CISO/Ad1/Ad2/AdAvr | не більше доби | системні утиліти, сканери |
| 4 | Проведення навчання посадових осіб | CSO, CHRO | не більше доби | наявні в користуванні |
| ***Інцидент: Компрометація інформаційних систем, криптографічних ключів і автентифікаційних даних користувачів Єдиної інформаційної системи*** |
| 1 | Блокування доступу до Єдиної інформаційної системи та ресурсів | CSO/CISO/Ad1/група КЗІ | не більше30 хв. | штатні |
| 2 | Аналіз можливих протиправних/несанкціонованих змін | CSO/ група КЗІ/ посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3) | не більше2 год. | штатні |
| 3 | Повернення Єдиної інформаційної системи до стану останньої неушкодженої резервної копії або контрольної точки | CISO/Ad1/Ad2/ група КЗІ | не більше4 год. | наявні в користуванні |
| 4 | Заміна паролів доступу та/або криптографічних ключів користувачів | CISO/Ad1/ група КЗІ | не більше доби | наявні в користуванні |
| 5 | Проведення службового розслідування за фактом компрометації / втрати | CSO, DPO | не більше 2 місяців | створення комісії, залучення адміністраторів Єдиної інформаційної системи |
| ***Інцидент: Несанкціонована модифікація інформації, що обробляється в базах даних і інформаційних ресурсах виконкому Криворізької міської ради*** |
| 1 | Мережева ізоляція Єдиної інформаційної системи на час обробки інциденту | CSO/ Ad1, Ad3 (адміністратор баз даних) | не більше30 хв. | наявні в користуванні |
| 2 | Аналіз можливих протоколів щодо протиправних/ несанкціонованих змін | CISO/Ad3**/** посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3) | не більше2 год. | наявні в користуванні |
| 3 | Повернення Єдиної інформаційної системи до стану останньої неушкодженої резервної копії або контрольної точки | CISO/Ad2/Ad3 | не більше4 год. | наявні в користуванні |
| 4 | Заміна паролів доступу та/або криптографічних ключів користувачів | CISO/Ad1 | не більше доби | наявні в користуванні |
| 5 | Проведення службового розслідування за фактом компрометації / втрати | CSO, DPO | не більше 7 днів | створення комісії, залучення адміністраторів Єдиної інформаційної системи |
| ***Інцидент: Витік інформації з обмеженим доступом каналами передачі даних у електронному вигляді*** |
| 1 | Мережева ізоляція Єдиної інформаційної системи на час обробки інциденту | CSO | не більше30 хв. | наявні в користуванні |
| 2 | Встановлення обсягу інформації та її власника | CSO/ посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3) | не більше4 год. | наявні в користуванні |
| 3 | Заміна паролів доступу/ криптографічних ключів користувачів | CISO/Ad1, група КЗІ | не більше доби | наявні в користуванні |
| 4 | Проведення навчання посадових осіб | CSO, CHRO | не більше 3 днів | наявні в користуванні |
| 5 | Проведення службового розслідування | CSO, DPO | не більше 2 місяців | створення комісії,залучення адміністраторів Єдиної інформаційної системи |
| ***Інцидент: Викрадення або втрата обладнання*** |
| 1 | Ідентифікація повного переліку втраченого активу | CISO/власники активу/ посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3) | не більше доби | наявні в користуванні |
| 2 | Проведення аналізу можливого витоку інформації з обмеженим доступом | CISO/Ad1/ посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3) | не більше доби | наявні в користуванні |
| 3 | Проведення навчання посадових осіб | CSO, CHRO | не більше 3 днів | наявні в користуванні |
| 4 | Проведення службового розслідування за фактом втрати обладнання | CSO, DPO | не більше 2 місяців | створення комісії, залучення матеріально-відповідальних осіб, звернення до правоохоронних органів |
| ***Інцидент: Вимкнення або перешкоджання роботі засобів забезпечення безпеки: антивірусних програм, міжмережевих екранів тощо*** |
| 1 | Локалізація активів, для яких може виникнути загроза  | CSO, CISO | не більше 30 хв. | наявні в користуванні |
| 2 | Відновлення роботи засобів забезпечення безпеки, у тому числі шляхом використання резервних | CISO/ Ad1, Ad2, AdAvr | не більше 2 год. | наявні в користуванні |
| 3 | Зміна паролів доступу до засобів забезпечення безпеки | CISO/Ad1 | не більше 2 год. | наявні в користуванні |
| 4 | Аналіз можливих протоколів щодо протиправних/ несанкціонованих змін | CISO/Ad2/ посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3) | не більше доби | наявні в користуванні |
| ***Інцидент: Порушення правил використання Єдиної інформаційної системи виконкому Криворізької міської ради*** |
| 1 | Локалізація можливих наслідків | CSO | не більше 2 год. | наявні в користуванні |
| 2 | Встановлення обставин виникнення порушення | CSO/ посадові особи IRT у межах повноважень (IRTL1, IRTL2, IRTL3) | не більше 4 год. | наявні в користуванні |
| 3 | Проведення навчання посадових осіб | CSO, CHRO | не більше 3 днів | наявні в користуванні |
| 4 | Проведення службового розслідування | CSO, DPO | не більше 2 місяців | залучення адміністраторів Єдиної інформаційної системи, юристів |

***В.о. керуючої справами виконкому –***

***заступник міського голови Надія ПОДОПЛЄЛОВА***