ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____ 2023 року № ____

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо підвищення рівня кіберзахисту систем електронного документообігу

І. Загальні положення

1. Методичні рекомендації щодо підвищення рівня кіберзахисту систем електронного документообігу (далі – Методичні рекомендації) розроблені з метою мінімізації ризиків несанкціонованого доступу до національних електронних інформаційних ресурсів, які обробляються та зберігаються з використанням програмних продуктів (сервісів) системи електронного документообігу органів державної влади, а також підвищення рівня кіберзахисту таких систем.

2. Методичні рекомендації розроблено відповідно до підпункту 1 частини другої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», абзаців другого та третього частини першої статті 3, пунктів 85, 86 та 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України», абзацу другого підпункту 1 та абзацу другого підпункту 2 пункту 3 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, та абзацу четвертого пункту 3, абзацу другого пункту 8, абзацу четвертого пункту 11, абзацу другого пункту 13 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, з метою забезпечення підвищення рівня кіберзахисту систем електронного документообігу та інформації під час надання та використання таких систем.

3. Методичні рекомендації розроблено з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity) та Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Держспецзв’язку від 06 жовтня 2021 року № 601.

4. Методичні рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання органами державної влади, підприємствами, установами, організаціями будь-якої форми власності, юридичними та/або фізичними особами, які відповідають за функціонування об'єктів критичної інфраструктури відповідно до чинного законодавства (далі – організація).

II. Терміни та визначення понять

1. У цих Методичних рекомендаціях терміни вживаються в такому значенні:

електронний документообіг (ЕДО) (Electronic Data Interchange, EDI) – спосіб організації роботи з документами, при якому основна маса документів використовується в електронному вигляді і зберігається централізовано, тобто структурована цифрова інформація між комп'ютерними системами бізнес-партнерів передається за допомогою серії стандартних угод та технічних правил і принципів, закладених у спеціальному програмному забезпеченні – СЕД;

система електронного документообігу (СЕД) (Document management system, DSM) – комп'ютерна програма (програмне забезпечення, система), яка дозволяє організувати роботу з електронними документами (створення, зміна, пошук), а також взаємодію між співробітниками (передачу документів, видачу завдань, відправлення повідомлень тощо);

управління корпоративним контентом (УКК) (Enterprise Content Management, ECM) – клас інтегрованих систем управління інформацією в організації. Це результат інтеграції функціональних і технологічних рішень, інтеграційних додатків та обмін даними (включаючи планування ресурсів організацій) системи управління процесами та робочими процесами, системи електронного керування даними та вебконтентом.

2. Інші терміни вживаються у значеннях, наведених у Законах України «Про основні засади кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації», «Про електронні довірчі послуги», «Про стандартизацію», постановах Кабінету Міністрів України від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту», від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інфраструктури», від 09 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інформаційної інфраструктури», від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

ІІІ. Мета та застосування Методичних рекомендацій

1. Методичні рекомендації запроваджують опис застосованих механізмів кіберзахисту до систем електронного документообігу, визначених національними та міжнародними стандартами, нормативними документами технічного захисту інформації, керівництвами та практиками, враховуючи підхід до класифікації заходів кіберзахисту, який описаний у Методичних рекомендаціях щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601.

2. Методичні рекомендації описують загальних підхід до аналізу поточного стану та опису цільового стану кіберзахисту СЕД, ідентифікації та визначення вразливостей та ризиків СЕД, встановлення пріоритетів щодо впровадження заходів із кіберзахисту для забезпечення безперервного та сталого функціонування СЕД.

3. Методичні рекомендації можуть використовуватися під час впровадження заходів кіберзахисту, які спрямовані на визначення, оцінки та управління ризиками кібербезпеки СЕД, визначення недоліків в існуючій діяльності із захисту СЕД, розроблення плану удосконалення та планування фінансування заходів для підвищення рівня кіберзахисту СЕД.

4. Методичні рекомендації описують систему заходів кіберзахисту до СЕД, яка базується на нормативних документах, національних та міжнародних стандартах, усталеній практиці забезпечення захисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем. Не слід розглядати зазначену систему заходів як вичерпний перелік заходів. Методичні рекомендації сформульовані у вигляді результатів, що очікуються у разі впровадження заходів кіберзахисту до СЕД.

Перелік заходів, зазначених в цих Методичних рекомендаціях, рекомендується наводити в технічному завданні на створення комплексної системи захисту інформації СЕД з урахуванням вимог НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем», а результати їх виконання – в окремому розділі матеріалів державної експертизи у сфері захисту інформації.

У таблиці наведено систему заходів кіберзахисту до СЕД. Повну класифікацію заходів кіберзахисту наведено у додатку до цих Методичних рекомендацій.

Таблиця

Система заходів кіберзахисту

Категорія заходів кіберзахисту	Опис	Заходи кіберзахисту
1	2	3
Клас заходів кіберзахисту «Ідентифікація ризиків кібербезпеки» (ID)		
ID.AM Управління активами	Описуються дані, персонал, пристрої та носії інформації, інформаційні системи, що дозволяють забезпечити стале функціонування СЕД, а також описується політика управління ризиками.	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 ID.AM-5 ID.AM-6
ID.BE Середовище надання життєво важливих послуг та функцій	Формування обов'язків персоналу щодо забезпечення кібербезпеки, а також рішень з управління ризиками у сфері кібербезпеки.	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5
ID.GV Управління безпекою	Формування правил, процедур і процесів для управління й моніторингу впроваджених нормативних, екологічних та експлуатаційних вимог, а також вимог щодо забезпечення кібербезпеки.	ID.GV-1 ID.GV-2 ID.GV-3 ID.GV-4
ID.RA Оцінка ризиків	Визначення ризиків у сфері кібербезпеки для СЕД.	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6
ID.RM Стратегія управління ризиками організації	Визначення пріоритетів, обмежень, допустимого рівня ризику для підтримки рішень щодо зниження ризиків кібербезпеки.	ID.RM-1 ID.RM-2 ID.RM-3
ID.SC Управління ризиками системи постачання	Визначення пріоритетів, обмежень, допустимого рівня ризику щодо системи постачання для підтримки рішень щодо ризиків, пов'язаних із системою постачання послуг третіми особами.	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5
Клас заходів кіберзахисту «Кіберзахист» (PR)		
PR.AC Управління ідентифікацією, автентифікацією та контроль доступу	Забезпечення доступу до фізичних і логічних ресурсів СЕД та пов'язаних з ними об'єктів тільки для авторизованих користувачів, адміністраторів або процесів. Управління здійснюється з урахуванням встановленого допустимого рівня ризику несанкціонованого доступу.	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7
PR.AT Обізнаність та навчання	Забезпечення інформування та обізнаності співробітників організації та партнерів організації щодо питань кіберзахисту СЕД. Співробітники мають освіту або пройшли спеціалізовану підготовку для покращення інформованості з питань кібербезпеки, пройшли належну підготовку для виконання своїх	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5

1	2	3
	обов'язків щодо забезпечення кіберзахисту СЕД відповідно до встановлених політик, правил, процедур та угод.	
PR.DS Безпека даних	Забезпечення управління інформацією та документацією з метою захисту конфіденційності, цілісності та доступності інформації.	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-4 PR.DS-5 PR.DS-6 PR.DS-7 PR.DS-8
PR.IP Процеси та процедури кіберзахисту	Забезпечення підтримання та управління політикою (правилами) безпеки, процесами та процедурами, які використовуються для управління захистом СЕД.	PR.IP-1 PR.IP-2 PR.IP-3 PR.IP-4 PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 PR.IP-10 PR.IP-11 PR.IP-12
PR.MA Технічне обслуговування	Технічне обслуговування та ремонт компонентів СЕД виконуються з дотриманням правил та процедур безпеки.	PR.MA-1 PR.MA-2
PR.PT Технології кіберзахисту	Управління технічними рішеннями (технологіями) кіберзахисту з метою забезпечення безпеки та стійкості СЕД з дотриманням правил, процедур з безпеки.	PR.PT-1 PR.PT-2 PR.PT-3 PR.PT-4 PR.PT-5
Клас заходів кіберзахисту «Виявлення кіберінцидентів» (DE)		
DE.AE Аномалії та кіберінциденти	Своєчасне виявлення аномальної активності та передбачення потенційного впливу кіберінцидентів.	DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5
DE.CM Безперервний моніторинг кібербезпеки	Відстеження безпеки СЕД через дискретні інтервали для виявлення кіберінцидентів та перевірки ефективності заходів кібербезпеки.	DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.CM-7 DE.CM-8
DE.DP Процеси виявлення кіберінцидентів	Підтримання і тестування процесів й процедур виявлення кіберінцидентів для забезпечення своєчасного та адекватного оповіщення про аномальні кіберінциденти.	DE.DP-1 DE.DP-2 DE.DP-3

1	2	3
		DE.DP-4 DE.DP-5
Клас заходів кіберзахисту «Реагування на кіберінциденти» (RS)		
RS.RP Планування реагування	Процеси та процедури в СЕД реагування на кіберінциденти виконуються та підтримуються з метою забезпечення своєчасного реагування на виявлені кіберінциденти.	RS.RP-1
RS.CO Комунікації	Координація заходів з реагування між внутрішніми та зовнішніми партнерами організації (у разі доцільності).	RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5
RS.AN Аналіз	Проведення аналізу кіберінцидентів для забезпечення адекватних заходів реагування та підтримки відновлення.	RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.AN-5
RS.MI Мінімізація наслідків	Виконання заходів з метою запобігання поширенню кіберінциденту, мінімізації його наслідків та унеможливлення його повторення.	RS.MI-1 RS.MI-2 RS.MI-3
RS.IM Удосконалення	Удосконалення заходів з реагування шляхом врахування досвіду з поточних або виконаних заходів виявлення/реагування.	RS.IM-1 RS.IM-2
Функція кібербезпеки «Відновлення стану кібербезпеки» (RC)		
RC.RP Планування відновлення	Процеси та процедури відновлення в СЕД виконуються та підтримуються з метою своєчасного відновлення.	RC.RP-1
RC.IM Удосконалення	Планування відновлення та процеси відновлення удосконалюються шляхом урахування отриманого досвіду.	RC.IM-1 RC.IM-2
RC.CO Комунікації	Заходи з відновлення координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, постачальники електронних комунікаційних мереж та/або послуг, власники атакуючих систем, інші групи реагування на інциденти, пов’язані з інформаційною та/або кібербезпекою (CSIRT).	RC.CO-1 RC.CO-2 RC.CO-3

IV. Призначення та види систем електронного документообігу

1. СЕД призначена для створення, реєстрації, зберігання, пошуку, класифікації та маршрутизації документів.

2. СЕД підтримує можливості створення картки та маршруту документів, відстеження руху документів та відповідальних осіб за виконання документів, ведення обліку змін до документів, здійснення контролю над виконанням

документів, за підготовку резолюцій.

3. Використання СЕД забезпечує безпеку та конфіденційність інформації, контроль та розмежування доступу, використання електронної ідентифікації.

4. Розрізняються зовнішній і внутрішній електронний документообіг. Зовнішній документообіг призначений для обміну вхідними та вихідними документами з іншими організаціями. Внутрішній документообіг дозволяє обмінюватися документами тільки в межах структурних підрозділів організації.

5. До окремого виду СЕД належить ECM система, що функціонує як стратегічна інфраструктура та технічна архітектура для підтримання єдиного життєвого циклу неструктурованої інформації (контенту) різних типів та форматів.

6. Сучасні ECM системи виступають як програмні рішення, що реалізують такі ключові компоненти:

документоорієнтована взаємодія (англ. collaboration) – спільне використання документів користувачами та підтримка проєктних команд;

управління вебконтентом (WCM) – автоматизація ролі вебмайстра, управління динамічним контентом та взаємодією користувачів;

управління документами – експорт, імпорт, контроль версій, безпека та служби бібліотек для ділових документів;

управління записами – довгострокове архівування, автоматизація політик зберігання та відповідності нормам регулюючих органів, забезпечення відповідності законодавчим та галузевим вимогам;

управління знаннями (англ. knowledge management) – підтримка систем для накопичення та доставки релевантної для бізнесу інформації;

управління мультимедіаконтентом (англ. DAM) – управління графічними, відео та аудіофайлами, різними маркетинговими матеріалами, наприклад, флеш-банерами, рекламними роликами;

управління образами документів (англ. document imaging) – захоплення, перетворення та управління паперовими документами;

управління потоками робіт (англ. workflow) – підтримка бізнес-процесів, передача контенту за маршрутами, призначення робочих завдань і станів, створення журналів аудиту.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку Данило МЯЛКОВСЬКИЙ