Додаток 1
до Методичних рекомендацій щодо
здійснення базових заходів з кіберзахисту
(пункт 6 розділу I)

Характеристика базових заходів із кіберзахисту

1. УПРАВЛІННЯ (GV): визначення стратегій, політик, ролей та обов'язків, проведення моніторингу щодо управління ризиками у сфері кібербезпеки.

1.1. **Організаційний контекст (GV.OC)**: визначення місії, очікування заінтересованих сторін, залежності, нормативних та договірних вимог, яких має дотримуватися суб'єкт забезпечення кібербезпеки в своїй діяльності задля виконання прийнятих рішень щодо управління ризиками кібербезпеки.

1.1.1. **GV.OC-01**: забезпечити усвідомлення суб'єктами організації, які здійснюють управління ризиками кібербезпеки, місії організації.

Нормативні посилання:	COBIT 5: Control Objectives for Information and Related Technologies (ISACA, 2012) (далі – COBIT 5) – APO02.06, APO03.01; НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» (далі – НД ТЗІ 3.7-001-99) – п. 6.3; НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» (далі – НД ТЗІ 3.7-003-05) – п. 6.1.2; НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» (далі – НД ТЗІ 3.6-006-24) – PM-8, PM-11; Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (далі – Наказ-601) – ID.BE-2, ID.BE-3; NIST SP 800-221A «Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio» (далі – NIST SP 800-221A) – GV.CT-5, GV.CT-3; NIST SP 800-53 Rev. 5.1.1 «Security and Privacy Controlsfor Information Systems and Organizations» (далі – NIST SP 800-53 Rev. 5.1.1) – PM-08, PM-11.
Приклади заходів:	описано місію (мету функціонування) об'єкта кіберзахисту (наприклад, через бачення продуктів

	та послуг, які надаватиме суб’єкт забезпечення кібербезпеки, маркетинг та стратегії надання послуг), структуру та організаційні схеми забезпечення кібербезпеки для визначення ризиків, які можуть перешкодити функціонуванню об’єкта відповідно до його мети.

1.1.2. **GV.OC-02**: внутрішні та зовнішні заінтересовані сторони усвідомили, а їхні потреби та очікування від впровадження управління ризиками кібербезпеки визначені та впроваджені.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT) (далі – ДСТУ ISO/IEC 27001:2023) – A.15.1.3, A.15.2.1, A.15.2.2; Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджено постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 (далі – Загальні вимоги) – п. 7; НД ТЗІ 3.6-006-24 – PM-9, PM-18, PM-30, SA-12, SR-3, SR-5, SR-6, SR-8; Наказ-601 – ID.SC-2, ID.GV-2; COBIT 5 – APO08.04, APO08.05, APO10.03, APO10.04, APO10.05; NIST SP 800-218 «Secure Software Development Framework V1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities» (далі – NIST SP 800-218) – PO.2.1; NIST SP 800-221A – GV.OV-2, GV.CT-2, GV.CT3SP; NIST SP 800-53 Rev 5.1.1 – PM-09, PM-18, PM-30, SA-12, SR-03, SR-05, SR-06, SR-08.
Приклади заходів:	визначено підрозділи/посадові особи та їхні потреби/очікування від впровадження системи управління ризиками кібербезпеки (наприклад, очікування щодо підвищення ефективності контролю та управління посадових осіб об’єкта кіберзахисту, дотримання правил кібергігієни працівниками, оптимізація структури та бюджету організації тощо); визначено зовнішні заінтересовані сторони та їхні очікування щодо результатів впровадження суб’єктом забезпечення кібербезпеки системи управління ризиками кібербезпеки (наприклад, очікування клієнтів щодо дотримання конфіденційності, ділові очікування щодо партнерства, очікування відповідності законодавчих умов договірним умовам).

1.1.3. **GV.OC-03**: визначити та забезпечити виконання персоналом існуючих законодавчих, нормативних та договірних вимог, а також вимог організації щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав та свобод.

Нормативні посилання:	НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.7-003-05 – п. 6.1.3; НД ТЗІ 3.6-006-24 – AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1; Наказ-601 – ID.GV-3; COBIT 5 – APO02.01, APO02.06, APO03.01; NIST SP 800-218: PO.1.1, PO.1.2; NIST SP 800-53 Rev 5.1.1 – AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01.
Приклади заходів:	визначено процес відстеження та впровадження змін законодавства щодо кіберзахисту та захисту інформації (наприклад, щодо захисту персональних даних, захисту інформації в інформаційно-комунікаційних системах, хмарних обчислень, імплементації норм актів законодавства ЄС та НАТО у сфері кібербезпеки тощо); визначено процес щодо відстеження дотримання партнерами договірних вимог; визначено стратегію управління ризиками узгоджено з правовими, нормативними та договірними вимогами та їх змінами.

1.1.4. **GV.OC-04**: визначити ключові цілі, критичні послуги та спроможності, які очікуються постачальниками від організації, що доведені та усвідомлені її персоналом.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.11.2.2, A.11.2.3, A.12.1.3; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-24 – PM-8, PM-11, CP-2, PM-30, RA-9; НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.3; Наказ-601 – ID.BE-4, ID.BE-5; NIST SP 800-221A: MA.RI-1; NIST SP 800-53 Rev 5.1.1 – PM-08, PM-11, CP-02(08), PM-30(01), RA-09.
Приклади заходів:	встановлено критерії для визначення критичних спроможностей для послуг, які надаються внутрішніми і зовнішніми заінтересованими сторонами; визначено активи та операційні процеси, які безпосередньо впливають на досягнення цілей місії

	організації, і потенційний вплив від втрати (або часткової втрати) таких операційних процедур.

1.1.5. **GV.OC-05**: визначити наслідки, спроможності та послуги, від яких залежить діяльність організації, довести та забезпечити їх усвідомлення персоналом.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.15.1.3, A.15.2.1, A.15.2.2; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-24 – PM-11, PM-30, RA-7, SA-9, SR-5; Наказ-601 – ID.BE-1, ID.BE-4; COBIT 5 – APO08.04, APO08.05, APO10.03, APO10.04, APO10.05; NIST SP 800-221A – GV.CT-5, MA.RI-1; NIST SP 800-53 Rev 5.1.1– PM-11, PM-30, RA-07, SA-09, SR-05.
Приклади заходів:	створено зв’язки та визначено залежності об’єкта кіберзахисту від зовнішніх ресурсів (наприклад, інформаційно-комунікаційних систем, операторів електронних комунікацій, мереж електроживлення тощо) та їхні зв’язки із організаційними активами та послугами (сервісами); визначено та задокументовано зовнішні залежності, які є ключовими точками для втрати організацією критичних спроможностей та послуг, та їх доведено до відома до визначених посадових осіб.

1.2. **Стратегія управління ризиками (GV.RM)**: визначення пріоритетів, обмежень, рівнів ризику, втрат, які суб’єкт забезпечення кібербезпеки може понести, з урахуванням факторів ризику для кожного з видів діяльності, доведення їх до відома заінтересованих сторін для підтримки рішень щодо операційних ризику.

1.2.1. **GV.RM-01**: визначити та узгодити із заінтересованими сторонами організації цілі управління ризиками.

Нормативні посилання:	Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» (далі – НД ТЗІ 1.4-001-2000) – п. Д-4; НД ТЗІ 3.6-006-24 – PM-9, RA-7, SR-2; Наказ-601– ID.RM-1; COBIT 5 – APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02; NIST SP 800-221A – GV.RR-2; NIST SP 800-53 Rev 5.1.1 – PM-09, RA-07, SR-02.
Приклади заходів:	оновлено/переглянуто з визначеною частотою короткострокові та довгострокові цілі з управління

ризиками кібербезпеки, як частини річного стратегічного планування та в разі значних змін;
встановлено вимірювальні показники в рамках досягнення цілей управління ризиками кібербезпеки (наприклад, управління якістю навчання користувачів, забезпечення належного захисту від ризиків для кібербезпеки систем управління виробничими процесами, управління вразливостями та оновленнями програмного забезпечення засобів та обладнання, що використовуються на об’єкті кіберзахисту, антивірусним захистом, управління ризиками ланцюга постачання об’єкта кіберзахисту, його елементів та послуг, що ним або за допомогою його надаються);
погоджено з керівництвом цілі кібербезпеки і вони використовуються ним в повсякденній діяльності щодо заходів з управління ризиками.

1.2.2. **GV.RM-02**: визначити допустимий рівень ризику, який суб’єкт забезпечення кібербезпеки може прийняти, довести до відома всіх співробітників та заінтересованих сторін та підтримувати таку інформацію в актуальної стані.

Нормативні посилання:
Загальні вимоги – п. 4, 5;
НД ТЗІ 1.4-001-2000 – п. Д4;
НД ТЗІ 3.6-006-24 – PM-9;
Наказ-601 – ID.RM-2, ID.RM-3;
COBIT 5 – APO12.06;
NIST SP 800-221A – GV.BE-1, GV.BE-3;
NIST SP 800-53 Rev 5.1.1– PM-09.

Приклади заходів:
визначено допустимий рівень ризику об’єкта кіберзахисту, який відповідає очікуванням щодо належного рівня ризику для об’єкта кіберзахисту;
інформація про готовність організації приймати певний рівень ризику перенесена до розділу про допустимий рівень ризику;
інформація про готовність організації до прийняття ризиків та визначений допустимий рівень ризику доведена до відома співробітників та суб’єкта забезпечення кібербезпеки, інших заінтересованих сторін у конкретний, вимірюваний та широко зрозумілий спосіб;
встановлена періодичність уточнення інформації про допустимий рівень ризику.

1.2.3. **GV.RM-03**: додати до процесів управління ризиками організації діяльність з управління ризиками кібербезпеки та досягнення її цілей.

Нормативні посилання:
Загальні вимоги – п. 4, 5;
НД ТЗІ 1.4-001-2000 – п. Д4;

НД ТЗІ 3.6-006-24 – PM-3, PM-9, PM-30, RA-7, SR-2;
НД ТЗІ 3.7-001-99 – п. 6.8;
Наказ-601– ID.GV-4;
NIST SP 800-221A – GV.PO-2, GV.PO-3;
NIST SP 800-53 Rev 5.1.1 – PM-03, PM-09, PM-30, RA-07, SR-02.

Приклади заходів:

об’єднано ризики кібербезпеки, які управляються разом з іншими ризиками (наприклад, відповідність вимогам, фінансові, операційні, регуляторні, репутаційні, безпека);
залучено менеджерів з управління ризиками кібербезпеки до планування управління ризиками об’єкта кіберзахисту;
встановлено критерії для передачі ризиків кібербезпеки на більш високий рівень управління в рамках управління ризиками об’єкта кіберзахисту.

1.2.4. **GV.RM-04**: визначити та довести до відома персоналу стратегічні напрями, які описують відповідні варіанти реагування на ризики.

Нормативні посилання:

НД ТЗІ 3.6-006-24 – PM-3;
Наказ-601– ID.RM-2;
NIST SP 800-221A – GV.BE-1;
NIST SP 800-53 Rev 5.1.1 – PM-09, PM-28, PM-30, SR-02.

Приклади заходів:

визначено варіанти реагування на ризик кібербезпеки, наприклад: зменшення ризику шляхом впровадження нових заходів захисту або посилення наявних заходів; прийняття ризику з відповідним обґрунтуванням; обмін, перенесення ризику або відхилення ризику;
визначено критерії прийняття та уникнення ризику кібербезпеки для даних різних класифікацій;
описано умови, за яких прийнятні моделі спільної відповідальності (наприклад, відповідно до договорів про передачу певних функцій кібербезпеки на аутсорсинг, виконання фінансових операцій третьою стороною від імені організації, використання публічних хмарних послуг);
ознайомлено персонал об’єкта кіберзахисту та заінтересовані сторони.

1.2.5. **GV.RM-05**: визначити та довести до відома персоналу способи обміну інформацією всередині організації щодо ризиків кібербезпеки, включаючи ризики, які несуть постачальники та інші треті сторони.

Нормативні посилання:

ДСТУ ISO/IEC 27001:2013 – A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1,A.15.2.2;
Загальні вимоги – п. 4, 5;
НД ТЗІ 1.4-001-2000 – п. Д7.1;

НД ТЗІ 3.6-006-24 – PM-9, PM-30;
Наказ-601 – ID.SC-1;
COBIT 5 – APO12.02;
NIST SP 800-53 Rev. 5 – SA-9, SA-12, PM-9;
NIST SP 800-221A – GV.PO-1;
NIST SP 800-53 Rev 5.1.1 – PM-09, PM-30.

Приклади заходів:

визначено та узгоджено проміжки часу інформування старших керівників, директорів і керівництво про стан кібербезпеки об'єкта кіберзахисту;
визначено механізми спілкування та інформування в рамках управління ризиками кібербезпеки на об'єкті кіберзахисту, наприклад, керівництво, служба безпеки об'єкта кіберзахисту, юридичний відділ, відділ закупівель, відділ фізичної безпеки та кадровий відділ спілкуватимуться між собою щодо ризиків кібербезпеки.

1.2.6. **GV.RM-06**: визначити та довести до відома персоналу стандартизовані методи розрахунку, документування, ідентифікації та визначення пріоритетності ризиків кібербезпеки.

Нормативні посилання:

Загальні вимоги – п. 4, 5;
НД ТЗІ 1.4-001-2000 – п. Д4;
НД ТЗІ 3.6-006-24 – PM-9, PM-18, PM-28, PM-30, RA-3;
Наказ-601 – ID.RM-1;
COBIT 5 – APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02;
NIST SP 800-221A – GV.RR-2;
NIST SP 800-53 Rev 5.1.1 – PM-09, PM-18, PM-28, PM-30, RA-03.

Приклади заходів:

встановлено критерії для використання кількісного підходу до аналізу ризиків кібербезпеки;
створено шаблони (наприклад, реєстр ризиків) для документування інформації про ризики кібербезпеки (включаючи опис ризику, контактні особу, відповідальну за ризик, загрозу);
встановлено критерії для визначення пріоритетів ризиків для організації;
використовується перелік категорій ризиків для їх збору, накопичення та порівняння.

1.2.7. **GV.RM-07**: визначити, охарактеризувати та забезпечувати обговорення зі співробітниками організації стратегічних можливостей щодо управління ризиками кібербезпеки.

Нормативні посилання:

НД ТЗІ 3.6-006-24 – PM-9, PM-18, PM-28, PM-30, RA-3;
NIST SP 800-53 Rev 5.1.1 – PM-09, PM-18, PM-28, PM-30, RA-03.

Приклади заходів:	визначено методи для виявлення можливостей і включення їх в обговорення ризиків (наприклад, аналіз сильних і слабких сторін, можливостей і загроз [SWOT]); визначено та затверджено додаткові цілі; розраховано та затверджено пріоритетність позитивних ризиків разом із негативними.

1.3. **Ролі, обов'язки та повноваження (GV.RR)**: визначення та доведення до відома співробітників суб'єкта забезпечення кібербезпеки ролей щодо кібербезпеки, відповідальності, уповноважених державних органів (підрозділів) для інформування, оцінки ефективності та постійного вдосконалення.

1.3.1. **GV.RR-01**: визначити із числа керівництва організації посадову особу, яка звітує про ризики кібербезпеки та підтримання культури поведінки щодо усвідомлення ризиків та етики, її постійне вдосконалення, а також відповідає за них.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – PM-2, PM-19, PM-23, PM-24, PM-29; NIST SP 800-218 – PO.2.3; NIST SP 800-53 Rev 5.1.1 – PM-02, PM-19, PM-23, PM-24, PM-29.
Приклади заходів:	керівництвом узгоджено власні ролі та обов'язки щодо розробки, впровадження та оцінювання виконання стратегії кібербезпеки; доведено до відома персоналу організації очікування керівників щодо безпечної та етичної культури, особливо коли поточні події надають можливість підкреслити позитивні або негативні приклади управління ризиками кібербезпеки; керівництвом визначено головного офіцера з інформаційної безпеки (CISO), якому доручено підтримувати комплексну стратегію управління ризиками кібербезпеки та переглядати й оновлювати її щонайменше раз на рік та після значних подій; проведено перевірки для забезпечення розуміння співробітниками своїх повноважень і налагодження координації між особами, відповідальними за управління ризиками кібербезпеки.

1.3.2. **GV.RR-02**: визначити ролі, відповідальність та державні органи (підрозділи), залучені до управління ризиками кібербезпеки, забезпечити їх розуміння персоналом і здійснювати контроль за їх дотриманням.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.6.1.1, A.7.2.1; Загальні вимоги – пп. 2, 5, 7, 8, 9; НД ТЗІ 1.4-001-2000 – п. 6, 7, 8, 9, 10; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-24 – PM-2, PM-13, PM-19, PM-23, PM-24, PM-29;

НД ТЗІ 3.7-001-99 – п. 6.3;
Наказ-601 – ID.AM-6, ID.GV-2, DE.DP-1;
COBIT 5 – APO01.02, DSS06.03;
NIST SP 800-218 – PO.2.1;
NIST SP 800-221A – GV.RR-1, RR-2, GV.OV-2;
NIST SP 800-53 Rev 5.1.1 – PM-02, PM-13, PM-19, PM-23, PM-24, PM-29.

Приклади заходів:

визначено в політиці та затверджено ролі та обов'язки з управління ризиками;
визначено відповідальних посадових осіб за діяльність з управління ризиками кібербезпеки, механізми проведення консультацій та механізми їх інформування;
до посадових обов'язків включено та до персоналу доведено обов'язковість виконання вимог з кібербезпеки;
затверджено показники продуктивності для персоналу, які виконують обов'язки з управління ризиками кібербезпеки; здійснюється періодичне вимірювання продуктивності, щоб визначити області для покращення;
визначено обов'язки з кібербезпеки в межах операцій, функцій управління ризиками та функцій внутрішнього аудиту.

1.3.3. **GV.RR-03**: визначити необхідні ресурси відповідно до стратегії управління ризиками кібербезпеки, ролей, відповідальності та політик.

Нормативні посилання:

Загальні вимоги – п. 4, 5;
НД ТЗІ 1.4-001-2000 – п. Д4;
НД ТЗІ 3.6-006-24 – PM-3;
Наказ-601– ID.RM-1;
COBIT 5 – APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02;
NIST SP 800-221A – GV.RR-2;
NIST SP 800-53 Rev 5.1.1 – PM-03.

Приклади заходів:

забезпечено періодичні перевірки керівництва, щоб переконатися, що ті, хто відповідає за управління ризиками кібербезпеки, мають необхідні повноваження;
забезпечено відповідність розподілу ресурсів та інвестиції ризику та заходам протидію йому;
забезпечено достатню кількість людей, процесів і технічних ресурсів для підтримки виконання заходів стратегії кібербезпеки.

1.3.4. **GV.RR-04**: додати кібербезпеку до практик управління людськими ресурсами.

Нормативні посилання:

ДСТУ ISO/IEC 27001:2013 – A.7.1.1; A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3; A.7.3.1, A.8.1.4;

НД ТЗІ 3.6-006-24 – PM-13, PS-1, PS-7, PS-9;
Наказ-601 – PR.IP-11;
CIS Critical Security Controls – 5, 16;
COBIT 5 – APO07.01, APO07.02; APO07.03, APO07.04, APO07.05;
NIST SP 800-53 Rev 5.1.1 – PM-13, PS-01, PS-07, PS-09.

Приклади заходів:

у кадрову політику включено управління ризиками кібербезпеки (наприклад, перевірка персоналу перед прийняттям на роботу, адаптація, сповіщення про зміни, звільнення);
при підборі кадрів знання та навички кандидатів з кібербезпеки визначено як позитивний фактор;
проводиться перевірка біографії перед прийомом на роботу нового персоналу на чутливі посади;
у подальшому періодично повторюються перевірки біографії для персоналу на таких посадах;
забезпечено перевірку дотримання персоналом зобов’язань щодо знання, дотримання та підтримки політики безпеки відповідно до їхніх ролей та посадових інструкцій.

1.4. **Політика (GV.PO)**: затвердження, доведення та сприяння реалізації політики кібербезпеки організації.

1.4.1. **GV.PO-01**: розробити та довести до відома персоналу організації політику управління ризиками кібербезпеки, яка визначена з урахуванням структури організації, стратегії кібербезпеки та пріоритетів.

Нормативні посилання:

ДСТУ ISO/IEC 27001:2013 – A.5.1.1;
Загальні вимоги – пп. 1, 2, 4, 7, 8;
НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» (далі – НД ТЗІ 1.1-002-99) – п. 6.2;
НД ТЗІ 1.4-001-2000 – п. Д5;
НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» (далі – НД ТЗІ 2.5-004-99) – п. 6, 7, 8, 9;
НД ТЗІ 3.6-006-24 – AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1;
НД ТЗІ 3.7-001-99 – п. 6.4.1;
НД ТЗІ 3.7-003-05 – п. 6.2;
Наказ-601 – ID.GV-1;
COBIT 5 – APO01.03, EDM01.01, EDM01.02;
NIST SP 800-221A – GV.PO-1;
NIST SP 800-53 Rev 5.1.1 – AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-

	01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01.
Приклади заходів:	створено, поширено та підтримується політика управління ризиками, яка зрозуміла та враховує цілі, очікування та спрямування керівництва суб'єкта забезпечення кібербезпеки; проводиться періодичний перегляд політики та допоміжних послуг (сервісів) кібербезпеки, для їх узгодження із цілями та пріоритетами стратегії управління ризиками, а також з керівництвом політики кібербезпеки на високому рівні; затверджено політику керівництвом вищого рівня та доведено її до відома всіх співробітників; персоналом отримано та вивчено політики під час першого прийому на роботу, щорічно та у разі внесення оновлень до неї.

1.4.2. **GV.PO-02**: забезпечити періодичний перегляд, оновлення, доведення та виконання політики управління ризиками кібербезпеки з урахуванням змін нормативних вимог, загроз, технологій та місії організації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.5.1.1; Загальні вимоги – пп. 1, 2, 4, 7, 8; НД ТЗІ 1.1-002-99 – п. 6.2; НД ТЗІ 1.4-001-2000 – п. Д5; НД ТЗІ 2.5-004-99 – п. 6, 7, 8, 9; НД ТЗІ 3.6-006-24 – AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.7-003-05 – п. 6.2; Наказ-601– ID.GV-1; COBIT 5 – APO01.03, EDM01.01, EDM01.02; NIST SP 800-53 Rev 5.1.1– AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01.
Приклади заходів:	оновлено політику управління ризиками кібербезпеки на основі періодичних перевірок результатів управління ризиками кібербезпеки, щоб гарантувати, що політика та допоміжні послуги (сервіси з кібербезпеки) адекватно підтримують ризик на прийнятному рівні, зміни в правових і нормативних вимогах, в технологіях (наприклад, впровадження штучного інтелекту); встановлено графік для перегляду змін у середовищі ризиків організації (наприклад, зміни в ризиках або в цілях місії організації) та визначено рекомендації з оновлення політики; оновлено політику, щоб відобразити зміни в юридичних та нормативних вимогах;

	оновлено політику, щоб відобразити зміни в технологіях (наприклад, впровадження штучного інтелекту) та організаційній діяльності (наприклад, придбання нових активів, нові вимоги до контрактів).

1.5. **Контроль (GV.OV)**: використання результатів комплексної діяльності з управління ризиками кібербезпеки здійснюється для інформування, покращення ефективності та коригування стратегії управління ризиками.

1.5.1. **GV.OV-01**: забезпечити врахування результатів стратегії управління ризиками кібербезпеки для вдосконалення та коригування її напрямів.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1 ,IR-1, MA-1,MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, PM-9, PM-18, PM-30, PM-31, RA-7, SR-6 NIST SP 800-221A – GV.AD-3; NIST SP 800-53 Rev 5.1.1 – AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01 ,IR-01, MA-01,MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01, PM-09, PM-18, PM-30, PM-31, RA-07, SR-06.
Приклади заходів:	проаналізовано, наскільки стратегія управління ризиками та результати перевірки чи аудиту системи управління ризиками допомогли керівникам приймати рішення та досягати цілей організації; проаналізовано чи чинна стратегія управління ризиками кібербезпеки потребує корегування з метою усунення чинників, які перешкоджають ефективному функціонуванню організації та впровадження інновацій в ній.

1.5.2. **GV.OV-02**: забезпечити перегляд та коригування стратегії управління ризиками кібербезпеки для забезпечення охоплення нею вимог організації та ризиків.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – PM-9, PM-19, PM-30, PM-31, RA-7, SR-6; NIST SP 800-221A – GV.AD-2, GV.AD-3, RM-8; NIST SP 800-53 Rev 5.1.1 – PM-09, PM-19, PM-30, PM-31, RA-07, SR-06.
Приклади заходів:	переглянуто результати аудиту, щоб підтвердити, чи забезпечила існуюча стратегія кібербезпеки відповідність внутрішнім і зовнішнім вимогам; переглянуто ефективність виконання функцій, пов’язаних з кібербезпекою, щоб визначити, чи потрібні зміни в політиці управління ризиками кібербезпеки; переглянуто стратегію управління ризиками кібербезпеки з огляду на інциденти кібербезпеки.

Продовження додатка 1

1.5.3. **GV.OV-03**: забезпечити оцінювання продуктивності управління ризиками кібербезпеки для перегляду, внесення необхідних коригувань відповідно до поточних потреб.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – PM-4, PM-6, RA-7, SR-6; NIST SP 800-221A – GV.OV-2, MA.RM-2; SP 800-53 Rev 5.1.1 – PM-04, PM-06, RA-07, SR-06**.**
Приклади заходів:	переглянуто ключові індикатори виконання (KPI) для переконання, що розроблена політика та впроваджені процедури на об’єкті кіберзахисту допомагають досягти постановленої мети; переглянуто ключові індикатори ризику (KRI), в тому числі ймовірність їх виникнення та потенційний вплив з метою визначення ризиків, які можуть виникнути на об’єкті кіберзахисту; зібрати та доповісти керівництву показники з управління ризиками кібербезпеки.

1.6. **Управління ризиками ланцюга постачання у сфері кібербезпеки (GV.SC)**: ідентифікація, визначення, управління, моніторинг виконання процесів управління ризиками кібербезпеки, пов’язаних з ланцюгами постачання, та їх покращення постачальниками організації.

1.6.1. **GV.SC-01**: розробити програму, стратегію, цілі, політики та процеси управління ризиками кібербезпеки, пов’язаними з ланцюгами постачання, погодити їх із заінтересованими сторонами організації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1,A.15.2.2; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – PM-30, SR-2, SR-3; Наказ-601: ID.SC-1; COBIT 5 – APO12.02; NIST SP 800-221A – GV.PO-1; NIST SP 800-53 Rev 5.1.1 – PM-30, SR-02, SR-03.
Приклади заходів:	створено стратегію, яка відображає цілі програми управління ризиками кібербезпеки ланцюга постачання; розроблено програму управління ризиками в ланцюжку постачання в кібербезпеці, включаючи план (з основними показниками), політики та процедури, які керують впровадженням і вдосконаленням цієї програми; політики та процедури доведені до відома заінтересованих сторін суб’єкта забезпечення кібербезпеки; створено міжорганізаційний механізм, який забезпечує узгодженість між функціями, які сприяють управлінню ризиками кібербезпеки ланцюга постачання, наприклад: кібербезпека,

безпека ІТ, функціонування, юридичний, кадровий та інженерний аспекти.

1.6.2. **GV.SC-02**: розробити, довести, здійснювати внутрішню та зовнішню координацію ролей з кібербезпеки при їх виконанні постачальниками, користувачами та партнерами організації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.6.1.1; Загальні вимоги – пп. 5, 7, 8, 9; НД ТЗІ 1.4-001-2000 – п. 6, 7, 8, 9, 10; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-24 – SR-2, SR-3, SR-5; НД ТЗІ 3.7-001-99 – п. 6.3; Наказ-601 – ID.AM-6. COBIT 5 – APO01.02, DSS06.03; NIST SP 800-218 – PO.2.1; NIST SP 800-221A – GV.RR-1, GV.RR-2; NIST SP 800-53 Rev 5.1.1 – SR-02, SR-03, SR-05.
Приклади заходів:	визначено одну (або кілька) роль/посадову особу, яка відповідає за планування, забезпечення ресурсами та виконання діяльності з управління ризиками кібербезпеки ланцюга постачання; затвердити в політиці ролі управління ризиками кібербезпеки ланцюга постачання та відповідальність за ними; створити матрицю відповідальності для визначення посадової особи (групи посадових осіб), відповідальної за виконання заходів з управління ризиками кібербезпеки ланцюга постачання, а також встановлено механізми проведення консультацій та інформування такої посадової особи (груп посадових осіб); у посадових обов’язках визначено обов’язки та показники результативності щодо управління ризиками кібербезпеки ланцюга постачання, проводиться їх періодичне вимірювання, щоб визначити та покращити продуктивність; розроблено завдання та встановлено відповідальність до постачальників, користувачів та партнерів щодо допустимих ризиків кібербезпеки ланцюга постачання, які впроваджені в політику суб’єкта забезпечення кібербезпеки та застосовуються у відповідних договорах з постачальниками; повідомлено про ролі та обов’язки з управління ризиками кібербезпеки в ланцюгу постачання для третіх сторін; встановлено правила та протоколи обміну інформацією та звітування між суб’єктом забезпечення кібербезпеки та постачальником.

1.6.3. **GV.SC-03**: забезпечити інтеграцію управління ризиками ланцюга постачання у сфері кібербезпеки в процеси управління ризиками кібербезпеки організації, оцінку ризиків і їх вдосконалення.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, PM-9, PM-18, PM-30, PM-31, SR-2, SR-3, RA-3, RA-7; Наказ-601 – ID.SC-2; COBIT 5 – APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03; NIST SP 800-218 – PW.4.1; NIST SP 800-221A – GV.CT-2, GV.CT-3; NIST SP 800-53 Rev 5.1.1 – AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01, PM-09, PM-18, PM-30, PM-31, SR-02, SR-03, RA-03, RA-07.
Приклади заходів:	ідентифіковано та узгоджено питання кібербезпеки з управлінням ризиками суб’єкта забезпечення кібербезпеки; створено зведені набори заходів управління ризиками кібербезпеки та управління ризиками кібербезпеки ланцюга постачання; управління ризиками кібербезпеки ланцюга постачання інтегровано в процеси вдосконалення; важлива інформація про ризики кібербезпеки ланцюга постачання доводиться до відома керівництва суб’єкта забезпечення кібербезпеки та враховується на рівні управління ризиками організації.

1.6.4. **GV.SC-04**: визначити та пріоритизувати постачальників за ступенем критичності.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – RA-9, SA-9, SR-6; Наказ-601 – ID.SC-2. COBIT 5 – APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03; NIST SP 800-221A – GV.CT-2, GV.CT-3; NIST SP 800-53 Rev 5.1.1 – RA-09, SA-09, SR-06.

Приклади заходів:	розроблено критерії критичності постачальників на основі чутливості даних, які обробляються або зберігаються постачальниками, ступеня доступу до систем організації та важливості продуктів або послуг для місії організації; ведеться облік усіх постачальників та здійснено їх пріоритизацію на основі критеріїв їх критичності.

1.6.5. **GV.SC-05**: встановити вимоги, пов’язані з ризиками кібербезпеки в ланцюгах постачання, та впровадити їх в договори/контракти або інші типи договорів з постачальниками та відповідними третіми сторонами.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.1.1, A.15.1.2, A.15.1.3; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – SA-4, SA-9, SR-3, SR-5, SR-6, R-10; COBIT 5 – APO10.01, APO10.02, APO10.03, APO10.04, APO10.05; Наказ-601 – ID.SC-3; NIST SP 800-218 – PO.1.3; NIST SP 800-53 Rev 5.1.1 – SA-04, SA-09, SR-03, SR-05, SR-06, SR-10.
Приклади заходів:	визначено вимоги безпеки для постачальників, продуктів і послуг (зокрема, щодо тестування та доведення безпеки продуктів і послуг, що постачаються, протягом їх всього життєвого циклу) відповідно до рівня критичності та потенційного впливу компрометації продуктів та послуг, які ними постачаються; включити до договору всі вимоги до кібербезпеки та ланцюга постачання, обов’язкові для виконання третіми сторонами, а також встановити механізми перевірки дотримання цих вимог; визначено правила та протоколи обміну інформацією між організацією та її постачальником та субпідрядником; передбачено, що управління ризиками щодо включення вимог з безпеки в договорі базується на критичності потенційних наслідків у випадку компрометації поставок; визначено вимоги до безпеки в договорах про рівень обслуговування (SLA) для моніторингу постачальників на предмет прийнятної продуктивності безпеки протягом усього життєвого циклу відносин з постачальниками; у контрактах від постачальників вимагається: розкривати функції, функціональні можливості та вразливості їхніх продуктів і послуг протягом усього

	терміну служби продукту або терміну обслуговування; надавати та підтримувати актуальний інвентар компонентів (наприклад, перелік програмного або апаратного забезпечення) для критичних продуктів; перевіряти своїх співробітників і захищатися від внутрішніх загроз; надавати докази виконання прийнятних практик безпеки, наприклад, через самостійне підтвердження, відповідність чинним стандартам, сертифікації або інспекції; вказано у контрактах та інших договорах права та обов'язки організації, її постачальників та їхніх ланцюгів постачання щодо потенційних ризиків кібербезпеки.

1.6.6. **GV.SC-06**: забезпечити планування та комплексну перевірку постачальників або інших третіх сторін для зменшення ризиків перед початком юридичних відносин з ними.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2; Загальні вимоги – п. 4, 5, 7; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – RA-9, SA-4, SA-9, SR-3, SR-6; Наказ-601 – ID.SC-1; COBIT 5 – APO10.01, APO10.02, APO10.03, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, MEA01.02, MEA01.03, MEA01.04, MEA01.05; NIST SP 800-218 – PW.4.1, PW.4.4; NIST SP 800-221A – GV.CT-2, GV.CT-3, MA.RM-2, MA.RM-3; NIST SP 800-53 Rev 5.1.1 – RA-09, SA-04, SA-09, SR-03, SR-06.
Приклади заходів:	проведено ретельну перевірку потенційних постачальників, яка відповідає рівню ризику, критичності та складності відносин з кожним потенційним постачальником; оцінено застосовність технологій та їх кібербезпекові властивості, а також практики потенційних постачальників щодо управління ризиками; проведено оцінку ризиків постачальників щодо застосовності вимог з кібербезпеки; проводиться оцінювання автентичності, цілісності та безпеки критичних продуктів перед їх придбанням.

1.6.7. **GV.SC-07**: визначити ризики, пов'язані з постачальником, його продукцією та послугами, які він надає, з іншими третіми сторонами, усвідомити їх, зареєструвати, пріоритизувати та забезпечити реагування на них і контроль протягом всієї співпраці.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2; Загальні вимоги – п. 4, 5, 7; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – RA-9, SA-4, SA-9, SR-3, SR-6; Наказ-601 – ID.SC-2, ID.SC-4; COBIT 5 – APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03; NIST SP 800-218 – PW.4.1, PW.4.4; NIST SP 800-221A – GV.CT-2, GV.CT-3, MA.RM-2, MA.RM-3; NIST SP 800-53 Rev 5.1.1 – RA-09, SA-04, SA-09, SR-03, SR-06.
Приклади заходів:	скориговано формати та частоту оцінювання на основі репутації третьої сторони та критичності продуктів чи послуг, які вона надає; оцінено докази відповідності третіх сторін вимогам щодо кібербезпеки за контрактом, як-от самоатестації, гарантії, сертифікати та інші артефакти; забезпечено контроль критично важливих постачальників таким чином, що його результати (перевірки, аудити, випробування чи інші форми оцінювання) підтверджують виконання постачальниками своїх зобов’язань щодо безпеки протягом життєвого циклу відносин із постачальниками; проводиться моніторинг критичних постачальників, послуг та продуктів на предмет змін у їхніх профілях ризику та переоцінюється критичність постачальників і вплив ризиків; заплановано дії на випадок несподіваних перебоїв, пов’язаних з постачальниками та ланцюгами постачання, щоб забезпечити безперервність функціонування організації.

1.6.8. **GV.SC-08**: забезпечити залучення відповідних постачальників та інших третіх сторін до діяльності щодо планування, реагування та відновлення після інцидентів.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.17.1.3; Загальні вимоги – п. 4,5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – SA-4, SA-9, SR-2, SR-3, SR-8, CP-1, IR-1; Наказ-601 – ID.SC-5; COBIT 5 – DSS04.04; NIST SP 800-221A – GV.CT-3; NIST SP 800-53 Rev 5.1.1 – SA-04, SA-09, SR-02, SR-03, SR-08, CP-01, IR-01.

Приклади заходів:	визначено та використовуються правила та протоколи звітування про заходи реагування на інциденти та відновлення, а також статус між об’єктом кіберзахисту та його постачальниками; визначено та затверджено ролі та відповідальність суб’єкта забезпечення кібербезпеки та його постачальників щодо реагування на інциденти; залучено критичних постачальників до тренувань та симуляцій; визначено та скоординовано методи комунікацій та протоколи взаємодії, проведено спільний розгляд отриманого досвіду; визначити та забезпечувати координацію способів кризових комунікацій та протоколів між організацією та її критичними постачальниками; проводяться спільні дослідження отриманих результатів навчань з критичними постачальниками.

1.6.9. **GV.SC-09**: інтегрувати практичні заходи щодо забезпечення безпеки ланцюга постачання в програми організації щодо кібербезпеки та управління ризиками, контролювати їх ефективність протягом всього життєвого циклу користування продуктами та послугами, які суб’єкт отримує від постачальника чи інших третіх сторін.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1,A.15.2.2; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – PM-9, PM-19, PM-28, PM-30, PM-31, RA-3, RA-7, SA-4, SA-9, SR-2, SR-3, SR-5, SR-6; Наказ-601– ID.SC-1; COBIT 5 – APO12.02; NIST SP 800-221A – GV.PO-1; NIST SP 800-53 Rev 5.1.1 – PM-09, PM-19, PM-28, PM-30, PM-31, RA-03, RA-07, SA-04, SA-09, SR-02, SR-03, SR-05, SR-06.
Приклади заходів:	політики та процедури вимагають документування походження всіх придбаних технологічних продуктів і послуг; періодично готувати та подавати керівництву звіти про ідентифіковані ризики, а також про заходи, що підтверджують автентичність і відсутність підробок у придбаних компонентах; впроваджено періодичну комунікацію з відповідальним особами за управління ризиками кібербезпеки та персоналом, що експлуатує об’єкт кіберзахисту, про потреби в придбанні програмних патчів, оновлень та модернізації виключно від автентифікованих та надійних постачальників програмного забезпечення; переглянуто правила, щоб переконатися, що вони вимагають взаємодії з визначеним персоналом

	постачальника виконувати технічне обслуговування його продуктів; політиками встановлено вимоги та процедури щодо виявлення на дозволеної модернізації апаратного забезпечення об’єкта кіберзахисту.

1.6.10. **GV.SC-10**: передбачити в планах управління ризиками кібербезпеки, пов’язаними з ланцюгами постачання, порядок дій, які необхідно виконати після прийняття рішення щодо партнерства або укладання договору про надання послуг.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – А.15.1.1, А.15.1.2, А.15.1.3, А.15.2.1,А.15.2.2; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – PM-31, RA-3, RA-5, RA-7, SA-4, SA-9, SR-2, SR-3, SR-5, SR-6; Наказ-601 – ID.SC-1; COBIT 5 – APO12.02; NIST SP 800-221A – GV.PO-1; NIST SP 800-53 Rev 5.1.1 – PM-31, RA-03, RA-05, RA-07, SA-04, SA-09, SR-02, SR-03, SR-05, SR-06.
Приклади заходів:	встановлено процеси для припинення критичних відносин як за нормальних, так і за несприятливих обставин; визначено та впроваджено плани підтримки та обслуговування компонентів після закінчення їхнього життєвого циклу та їх фізичного зношення; своєчасно деактивується доступ постачальників до ресурсів організації, коли він більше не потрібен; перевіряється, що активи, які містять дані організації, повертаються або належним чином утилізуються вчасно, контрольовано та безпечно; розроблено та виконується план припинення відносин або зміни постачальників, враховуючи ризики безпеки ланцюга постачання та стійкість; передбачено впровадження компенсаційних заходів для мінімізації рівнів ризиків, пов’язаних із припиненням співпраці або зміною постачальників, які можуть вплинути на безпеку даних та систем; здійснюється управління ризиками витоку даних, пов’язаних з припиненням відносин з постачальниками.

2. ІДЕНТИФІКАЦІЯ (ID): оцінка реальних та потенційних ризиків у сфері кібербезпеки для запобігання та нейтралізації кіберзагроз.

2.1. **Управління активами (ID.AM)**: ідентифікація активів (у т.ч. даних, програмного забезпечення, систем, засобів, послуг, осіб), які необхідні

організації для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі організації та стратегії управління ризиками.

2.1.1. **ID.AM-01**: забезпечити періодичне проведення інвентаризації обладнання, яким керує організація.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 - A.8.1.1, A.8.1.2; Загальні вимоги – пп. 3, 5, 6, 10; НД ТЗІ 1.4-001-2000 – п. Д3.1; НД ТЗІ 2.5-004-99 – п. 10.1; НД ТЗІ 3.6-006-24 – CM-8, PM-5; НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.2; Наказ-601 – ID.AM-1; COBIT 5 – BAI09.01, BAI09.02; NIST SP 800-221A – MA.RI-1; NIST SP 800-53 Rev 5.1.1 – CM-08, PM-05.
Приклади заходів:	проведено інвентаризацію для всіх типів обладнання об’єкта кіберзахисту, включаючи IT, IoT, OT та мобільні пристрої; запроваджено постійний моніторинг об’єкта кіберзахисту, щоб виявляти нове обладнання, проводиться автоматична реєстрація здійснених оновлень.

2.1.2. **ID.AM-02**: забезпечити періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує організація.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 A.8.1.1, A.8.1.2; Загальні вимоги – пп. 3, 5, 6, 10; НД ТЗІ 1.4-001-2000 – п. Д3.1; НД ТЗІ 2.5-004-99 – п. 10.1; НД ТЗІ 3.6-006-24 – AC-20, CM-8, PM-5, SA-5, SA-9; НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.2; Наказ-601 – ID.AM-2; COBIT 5 – BAI09.01, BAI09.02, BAI09.05; NIST SP 800-221A – MA.RI-1; NIST SP 800-53 Rev 5.1.1 – AC-20, CM-08, PM-05, SA-05, SA-09.
Приклади заходів:	всі типи програмного забезпечення та послуг, у тому числі із відкритим вихідним кодом, користувацьких програм, служб API та хмарних послуг ідентифіковано та задокументовано; запроваджено постійний моніторинг всіх платформ, включаючи віртуальні машини, на наявність змін для інвентаризації оновлень для них; всі ІКС організації інвентаризацію та описано.

2.1.3. **ID.AM-03**: забезпечити підтримку використання авторизованих мережевих з’єднань та визначити внутрішні і зовнішні мережеві потоки

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.13.2.1; Загальні вимоги – пп. 5, 6, 53; НД ТЗІ 1.4-001-2000 – п. Д 3.2; НД ТЗІ 2.5-004-99 – п. 6.1, 6.2, 9.3; НД ТЗІ 3.6-006-24 – AC-4, CA-3, CA-9, PL-2, PL-8, PM-7; НД ТЗІ 3.7-001-99 – п. 6.3, 6.4.1; НД ТЗІ 3.7-003-05 – п. 6.1.2; Наказ-601 – ID.AM-3, DE.AE-1; COBIT 5 – DSS03.01, DSS05.02; NIST SP 800-53 Rev 5.1.1 – AC-04, CA-03, CA-09, PL-02, PL-08, PM-07.
Приклади заходів:	підтримувати базові лінії зв'язку та потоки даних у дротових та бездротових мережах об’єкта кіберзахисту; проведено інвентаризацію електронних комунікацій, потоків даних, які їх використовують, між організацією та зовнішніми організаціями; розроблено структурну схему інформаційних потоків, яка відображає інфраструктуру взаємодії між основним компонентами (завданнями, об’єктами); визначено в документації з прив’язкою до кожного порта мережі, протоколу та служби, що вони типово використовуються для авторизованих систем.

2.1.4. **ID.AM-04**: забезпечити періодичне проведення інвентаризації послуг, що надаються постачальниками.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.11.2.6; Загальні вимоги – пп. 5, 7, 52; НД ТЗІ 2.5-004-99 – п. 9.7; НД ТЗІ 3.6-006-24 – AC-20, SA-9, SR-2; НД ТЗІ 3.7-001-99 – пп. 6.3, 6.4.1; НД ТЗІ 3.7-003-05 – п.6.1.2; Наказ-601– ID.AM-4; COBIT 5 – APO02.02; NIST SP 800-53 Rev 5.1.1 – AC-20, SA-09, SR-02.
Приклади заходів:	усі зовнішні служби та послуги, які використовуються організацією, включаючи послуги IaaS, PaaS SaaS; API; та інші зовнішні служби додатків ідентифіковано та задокументовано; оновлюються інвентаризаційні дані при використанні нової зовнішньої служби або

	послуги, щоб забезпечити адекватний моніторинг управління ризиками кібербезпеки.

2.1.5. **ID.AM-05**: здійснити пріоритизацію активів за їх класифікацією, критичністю, ресурсами, впливом на місію організації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.8.2.1; Загальні вимоги – пп. 3, 5, 7; НД ТЗІ 1.4-001-2000 – п. Д5.6.2, 5.6.2.1; НД ТЗІ 3.6-006-24 – RA-3, RA-9, RA-2; НД ТЗІ 3.7-001-99 – п. 5.2; НД ТЗІ 3.7-003-05 – п. 6.1.3; Наказ-601 – ID.AM-5; COBIT 5 – APO03.03, APO03.04, BAI09.02; NIST SP 800-221A – MA.RI-1; NIST SP 800-53 Rev 5.1.1 – RA-03, RA-09, RA-02.
Приклади заходів:	встановлено критерії пріоритизації активів для кожного їх класу; застосовано критерії пріоритизації для кожного активу; критерії активів переглядаються періодично або у разі значних змін в організації.

2.1.6. **ID.AM-06**: вилучено, впроваджено в GV.RR-02, GV.SC-02.

2.1.7. **ID.AM-07**: забезпечити інвентаризацію даних і пов’язаних з ними метаданих відповідно до визначених типів даних.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CM-12, CM-13, SI-12; NIST SP 800-221A – MA.RI-1; SP 800-53 Rev 5.1.1 – CM-12, CM-13, SI-12.
Приклади заходів:	затверджено перелік типів даних (ідентифікаційна інформація, захищена інформація про здоров’я, номери фінансових рахунків, інтелектуальна власність організації, дані про операційні технології тощо); за результатами постійного аналізу даних здійснюється оновлення (за потребою) їх типів; встановлено індикатори віднесення інформації за встановленими типами даних; організацією здійснюється відстеження походження, власника та геолокації інформації за кожним типом даних.

2.1.8. **ID.AM-08**: забезпечити управління системами, апаратним та програмним забезпеченням, послугами та даними протягом усього їх життєвого циклу.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.6.1.5, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.1.2, A.11.2.4, A.11.2.5A.11.2.7, A.14.1.1, A.14.2.1, A.14.2.5, A.15.1.1, A.15.2.1; Загальні вимоги – п. 5, 10, 19, 20, 36, 39;

	НД ТЗІ 1.4-001-2000 – п. Д5.6.5; НД ТЗІ 2.5-004-99 – 7.3, 7.4, 8.1, 10.3; НД ТЗІ 3.7-001-99 – п. 6.4; НД ТЗІ 3.6-006-24 – CM-9, CM-13, MA-2, MA-6, PL-2 , PM-22, PM-23, SA-3, SA–4, SA-8, SA-22, SI-12, SI-18, SR-5, SR-12; Наказ-601 – PR.DS-3, PR.IP-2, PR.MA-1, PR.MA-2, PR.IP-6, PR.DS; COBIT 5 – APO13.01, BAI09.03, DSS05.04; NIST SP 800-218 – PW.4.1, PW.4.4; NIST SP 800-221A – MA.RI-1; NIST SP 800-53 Rev 5.1.1 – CM-09, CM-13, MA-02, MA-06, PL-02, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12.
Приклади заходів:	питання кібербезпеки розглядаються протягом усього життєвого циклу систем, апаратного забезпечення, програмного забезпечення та послуг; питання кібербезпеки розглядаються протягом життєвого циклу продуктів; виявляються неофіційні використання технологій для досягнення цілей місії (тобто, тіньові ІТ); періодично виявляються надлишкові системи, апаратне забезпечення, програмне забезпечення та послуги, які непотрібно збільшують поверхню атаки організації; налаштовано належним чином та захищаються системи, апаратне забезпечення, програмне забезпечення та послуги перед їх впровадженням у виробництво; здійснюється оновлення даних інвентаризації, коли системи, апаратне забезпечення, програмне забезпечення та послуги переміщуються або передаються в межах організації; безпечно знищувати збережені дані відповідно до політики збереження даних організації, використовуючи передбачений метод знищення, ведеться та здійснюється управління записами про знищення; безпечно очищуються сховища даних, коли апаратне забезпечення виводиться з експлуатації, списується, замінюється або відправляється на ремонт чи заміну; визначено методи знищення паперу, носіїв зберігання та інших фізичних форм зберігання даних.

2.2. **Оцінка ризиків (ID.RA)**: усвідомлення всією організацією ризиків кібербезпеки для неї, її активів і ризиків, які пов’язані з людським фактором.

2.2.1. **ID.RA-01**: ідентифікувати, підтверджувати та вести записи щодо вразливих місць активів.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3; Загальні вимоги – п. 4, 5, 24; НД ТЗІ 1.1-002-99 – п. 6.1, 6.5, 9; НД ТЗІ 1.4-001-2000 – п. Д1.1, Д1.2, Д4, Д5.6.2.4; НД ТЗІ 2.5-004-99 – п.9; НД ТЗІ 3.6-006-24 – CA-2, CA-7, CA-8, RA-3, RA-5, SA-11, SA-15, SA-15, SI-4, SI-5; Наказ-601 – ID.RA-1, PR.IP-12, DE.CM-8; CIS CSC – 4, 18, 20; COBIT 5 – APO12.01, APO12.02, APO12.03, APO12.04, BAI03.10, DSS05.01, DSS05.02; NIST SP 800-218 – PO.5.2; NIST SP 800-221A – MA.RI-3; NIST SP 800-53 Rev 5.1.1 – CA-02, CA-07, CA-08, RA-03, RA-05, SA-11(02), SA-15(07), SA-15(08), SI-04, SI-05.
Приклади заходів:	запроваджено використання технології управління вразливостями для виявлення не налаштованого та неправильно налаштованого програмного забезпечення; здійснюється оцінювання архітектури мережі та системи на предмет слабких місць у проектуванні та під час впровадження, які впливають на кібербезпеку; переглянуто, проаналізовано або протестовано програмне забезпечення, розроблене організацією, щоб виявити вразливості в проектуванні, кодуванні та налаштуваннях за замовчуванням; оцінено об’єкти, що містять критичні обчислювальні активи, на предмет фізичних вразливостей та питань стійкості; проводиться моніторинг джерел розвідки кіберзагроз для отримання інформації про нові вразливості в продуктах і послугах; переглянуто процеси та процедури на предмет слабких місць, які можуть бути використані для впливу на кібербезпеку.

2.2.2. **ID.RA-02**: організувати отримання інформації про загрози безпеки та вразливості з форумів обміну інформацією та офіційних джерел.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.6.1.4; Загальні вимоги – п. 5, 6; НД ТЗІ 3.6-006-24 – SI-5, PM-15, PM-16; Наказ-601 – ID.RA-2; NIST SP 800-221A – GV.BE-4; NIST SP 800-53 Rev 5.1.1 – SI-05, PM-15, PM-16.
Приклади заходів:	налаштувати інструменти та технології кібербезпеки з можливостями виявлення або реагування для безпечного надання та отримання зворотнього зв’язку про кіберзагрози; отримувати та аналізувати консультації від авторитетних третіх сторін щодо поточних суб'єктів загроз та їхньої тактики, методів і процедур (ТМП); проводити моніторинг джерела інформації про кіберзагрози для отримання інформації про типи вразливостей, які можуть мати новітні технології.

2.2.3. **ID.RA-03**: визначити та задокументувати внутрішні та зовнішні загрози.

Нормативні посилання:	Загальні вимоги – п. 4, 5; НД ТЗІ 1.1-002-99 – п. 6.1, 6.4, 6.5; НД ТЗІ 1.4-001-2000 – п. Д4.2.3, Д4.3, Д4.4; НД ТЗІ 3.6-006-24 – PM-12, PM-16, RA-3, SI-5; НД ТЗІ 3.7-003-05 – п. 6.1.2.9; Наказ-601 – ID.RA-3; COBIT 5 – APO12.01, APO12.02, APO12.03, APO12.04; NIST SP 800-221A – MA.RI-2; NIST SP 800-53 Rev 5.1.1 – PM-12, PM-16, RA-03, SI-05.
Приклади заходів:	використовувати кіберрозвідку для підтримки обізнаності про типи загрозливих акторів, які можуть націлюватися на організацію, та їх тактику, методи і процедури (ТМП); виконуйте пошук загроз для виявлення ознак загрозливих акторів у середовищі; реалізувати процеси для ідентифікації внутрішніх суб’єктів загроз.

2.2.4. **ID.RA-04**: визначити та задокументувати потенційні наслідки та вірогідні загрози, пов’язані з експлуатацією вразливостей.

Нормативні посилання:	Загальні вимоги – п. 4, 5; НД ТЗІ 1.1-002-99 – п. 6.1, 6.5; НД ТЗІ 1.4-001-2000 – п. Д5.6.2.4; НД ТЗІ 3.6-006-24 – PM-9, PM-11, RA-2, RA-3, RA-8, RA-9;

	НД ТЗІ 3.7-003-05 – п. 6.1.2.9; Наказ-601 – ID.RA-4; COBIT 5 – DSS04.02; NIST SP 800-221A – MA.RI-4; NIST SP 800-53 Rev 5.1.1 – PM-09, PM-11, RA-02, RA-03, RA-08, RA-09.
Приклади заходів:	керівники об’єкта кіберзахисту та фахівці з управління ризиками кібербезпеки працюють разом, щоб оцінити ймовірність та вплив сценаріїв ризиків і зареєструвати їх у реєстрах ризиків; визначити та обрахувати потенційний вплив несанкціонованого доступу до комунікацій організації, систем і даних, які обробляються цими системами; розглянути потенційний вплив каскадних відмов у взаємопов’язаних системах, враховувати потенційний вплив каскадних збоїв для операційних систем.

2.2.5. **ID.RA-05**: забезпечити використання інформації про вірогідні загрози, вразливості та можливі наслідки від їх настання для розуміння невід’ємного ризику та інформування про пріоритетність реагування на ризики.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.12.6.1; Загальні вимоги – п. 4, 5; НД ТЗІ 1.1-002-99 – п. 6.1 6.5; НД ТЗІ 1.4-001-2000 – п. Д5.6.2; НД ТЗІ 3.6-006-24 – PM-16, RA-2, RA-3, RA-7; НД ТЗІ 3.7-003-05 – п. 6.1.2.9; Наказ-601 – ID.RA-5; COBIT 5 – APO12.02; NIST SP 800-218 – PW.1.1; NIST SP 800-221A – MA.RA-2; NIST SP 800-53 Rev 5.1.1 – PM-16, RA-02 , RA-03, RA-07.
Приклади заходів:	здійснювати розвиток модель загроз для більшого розуміння ризиків для даних та визначити відповідні заходи реагування; здійснювати пріоритизацію ресурсів, що виділяються, та інвестицій у кібербезпеку на основі оцінених ймовірностей та наслідків.

2.2.6. **ID.RA-06**: визначити заходи реагування на ризики кібербезпеки та встановити їх пріоритетність, забезпечити їх відслідковування та комунікацію щодо них.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.12.6.1; Загальні вимоги – п. 4,5, 4.7;

	НД ТЗІ 1.4-001-2000 – п. 8.1, 8.2, Д4, Д5.6.3; НД ТЗІ 3.6-006-24 – PM-9, PM-18, PM-30, RA-7. Наказ-601 – ID.RA-6, RS.MI-3; COBIT 5 – APO12.05, APO13.02; NIST SP 800-218 – PO.5.2; NIST SP 800-221A – MA.RP; NIST SP 800-53 Rev 5.1.1 – PM-09, PM-18, PM-30, RA-07.
Приклади заходів:	критерії плану управління вразливостями застосовуються для прийняття, передачі, пом’якшення або уникнення ризику, або вибору компенсаційних заходів для пом’якшення ризику; здійснювати відстеження удосконалення процесів реагування на ризики (наприклад: за затвердженим планом, який містить основні етапи реагування на ризики; ведеться реєстр ризиків, надається детальний звіт про реагування); використовувати результати оцінки ризиків для прийняття рішення про реагування на ризик та виконання відповідних дій; про заплановані заходи реагування на ризик в пріоритетному порядку інформуються заінтересовані сторони.

2.2.7. **ID.RA-07**: забезпечити управління, оцінювання на предмет ризику, реєстрацію та відстеження змін та винятків до затвердженої документації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4; Загальні вимоги – п. 10; НД ТЗІ 1.1-002-99 – п. 7.4; НД ТЗІ 2.5-004-99 – п. 10.3, 10.6; НД ТЗІ 3.7-001-99 – п. 6.7; НД ТЗІ 3.6-006-24 – CA-7, CM-3, CM-4; Наказ-601 – PR.IP-3; COBIT 5 – BAI06.01, BAI01.06; NIST SP 800-218 – PO.5.2; NIST SP 800-221A – MA.RI-3; NIST SP 800-53 Rev 5.1.1 – CA-07, CM-03, CM-04.
Приклади заходів:	запроваджено та контролюється дотримання визначених документацією процедур перегляду, оцінювання та затвердження запропонованих змін до неї; здійснюється документування внесення/невнесення кожної запропонованої зміни щодо кожного можливого ризику; здійснюється документування кожної пов’язаної

	з ризиком пропозиції та планування реагування на такий ризик; проводиться періодичний перегляд ризиків, прийнятих на основі запланованих майбутніх дій або етапів.

2.2.8. **ID.RA-08**: визначити процеси отримання, аналізу та реагування на опубліковані повідомлення про виявлені вразливості.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.4; НД ТЗІ 3.6-006-24 – RA-5; Наказ-601 – RS.AN-5; COBIT 5 – APO12.06, DSS03.02, DSS05.07; NIST SP 800-221A – MA.RI-3; NIST SP 800-53 Rev 5.1.1 – RA-05.
Приклади заходів:	здійснювати обмін інформацією про вразливості між організацією та її постачальниками відповідно до правил та протоколів, визначених у контрактах; встановлено обов’язки щодо перевірки виконання процедур обробки, аналізу впливу та реагування на загрози кібербезпеці, уразливості або розкриття інцидентів постачальниками, клієнтами, партнерами та Держспецзв'язку, іншими уповноваженими державними організаціями з кібербезпеки.

2.2.9. **ID.RA-09**: проводити перевірку автентичності і цілісності обладнання та програмного забезпечення перед його придбанням і використанням.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.11.2.4; НД ТЗІ 2.5-004-99 – п. 5, п. 7, А.2; НД ТЗІ 3.6-006-24 – SA-4, SA-5, SA-10, SA-11, SA-15, SA-17, SI-7, SR-5, SR-6, SR-10, SR-11; НД ТЗІ 3.7-001-99 – п. 6.1, п. 10; Наказ-601 – PR.DS-8; COBIT 5 – BAI03.05; NIST SP 800-218 – PO.5.2; NIST SP 800-221A – MA.RI-3; NIST SP 800-53 Rev 5.1.1 – SA-04, SA-05, SA-10, SA-11, SA-15, SA-17, SI-07, SR-05, SR-06, SR-10, SR-11.
Приклади заходів:	оцінка автентичності та кібербезпеки критично важливих технологічних продуктів і послуг здійснюється до їх придбання та використання.

2.2.10. **ID.RA-10**: забезпечити проведення оцінювання постачальників перед придбанням у них критично важливих для організації продуктів і послуг.

Продовження додатка 1

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2; Загальні вимоги – п. 4, 5, 7; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-24 – SR-6; Наказ-601 – ID.SC-2, ID.SC-4; COBIT 5 – APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03; NIST SP 800-221A – GV.CT-2, GV.CT-3, MA.RM-2, MA.RM-3; NIST SP 800-53 Rev 5.1.1 – SR-06.
Приклади заходів:	оцінка автентичності та кібербезпеки критично важливих технологічних продуктів і послуг здійснюється до їх придбання та використання.

2.3. **Удосконалення (ID.IM)**: удосконалення організаційних процесів, процедур і діяльності з управління ризиками кібербезпеки, які визначено у класах заходів кіберзахисту.

2.3.1. **ID.IM-01**: визначити напрями удосконалення за результатами проведеного оцінювання стану кіберзахисту.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, CA-2, CA-5, CA-7, CA-8, CP-2, IR-04, IR-08, PL-02, RA-03, RA-05, RA-07, SA-08, SA-11, SA-17(06), SI-02, SI-04, SR-05; NIST SP 800-53 Rev 5.1.1 – AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01, CA-02, CA-05, CA-07, CA-08, CP-02, IR-04, IR-08, PL-02, RA-03, RA-05, RA-07, SA-08, SA-11, SA-17(06), SI-02, SI-04, SR-05.
Приклади заходів:	проведено самооцінку критично важливих служб, враховуючи поточні загрози та відомі техніки, тактики та процедури; проведено зовнішнє оцінювання/незалежний аудит ефективності програми кібербезпеки організації, за результатами якого визначено сфери, які потребують покращення; оцінювання відповідності суб’єкта забезпечення кібербезпеки встановленим для нього/обраних ним вимог з кібербезпеки здійснюється за допомогою автоматизованих засобів.

2.3.2. **ID.IM-02**: визначити напрями удосконалення за результатами тестування безпеки та навчальних вправ, включаючи їх виконання у взаємодії з постачальниками та відповідними третіми сторонами.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.17.1.3, A.14.2.8; Загальні вимоги – п. 4, 5, 39; НД ТЗІ 1.4-001-2000 – п. Д1.1, Д7.1; НД ТЗІ 3.7-001-99 – п. 6.8; НД ТЗІ 3.6-006-24 – AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, CA-2, CA-5, CA-7, CA-8, CP-2, CP-4, IR-3, IR-4, IR-8, PL-2, PM-4, PM-31, RA-3, RA-5, RA-7, SA-8, SA-11, SI-2, SI-4, SR-5; Наказ-601– ID.SC-5, PR.IP-10, DE.DP-3; COBIT 5 – DSS04.04; NIST SP 800-221A – GV.CT-3; NIST SP 800-53 Rev 5.1.1 – AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01, CA-02, CA-05, CA-07, CA-08, CP-02, CP-04, IR-03, IR-04, IR-08, PL-02, PM-04, PM-31, RA-03, RA-05, RA-07, SA-08, SA-11, SI-02, SI-04, SR-05.
Приклади заходів:	за результатами аналізу процедур реагування на кіберінциденти (у тому числі ТТХ, симуляцій, тестувань, внутрішніх оглядів та незалежного аудиту) визначено, які з них і як потребують удосконалення для покращення реагування на інциденти кібербезпеки у майбутньому; визначаються покращення для майбутніх заходів із забезпечення безперервної діяльності організації, аварійного відновлення та реагування на інциденти на основі навчань, проведених у координації з постачальниками критично важливих послуг та продуктів; керівництво суб’єкта забезпечення кібербезпеки та його внутрішні заінтересовані сторони (юридичний відділ, відділ кадрів тощо) за потреби залучаються до перевірок безпеки та навчань (вправ); керівництвом суб’єкта забезпечення кібербезпеки затверджено проведення тестування на проникнення у найбільш критичні системи об’єктів кіберзахисту; впроваджено план дій у надзвичайних ситуаціях для реагування та відновлення після виявлення того, що продукти або послуги не походять від постачальника або партнера, з яким укладено контракт, або були змінені до їх отримання; проведено збір та аналіз показників ефективності за допомогою інструментів та сервісів безпеки з метою підвищення ефективності програми кібербезпеки.

2.3.3. **ID.IM-03**: визначати покращення під час виконання операційних процесів, процедур і дій.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.6; Загальні вимоги – п. 4; НД ТЗІ 1.4-001-2000 – п. 8.2, п. Д1.1, Д5.6.5; НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» (далі – НД ТЗІ 3.6-004-21) – п. 6 – 8; НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації» (далі – НД ТЗІ 3.6-005-21) – п. 5; НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» (далі – НД ТЗІ 3.6-007-21) – п. 5; НД ТЗІ 3.6-008-21 «Порядок моніторингу безпеки інформаційних систем» (далі – НД ТЗІ 3.6-008-21) – п. 5; Наказ-601 – PR.IP-7, PR.IP-8, DE.DP-5, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2; COBIT 5 – APO11.06, BAI01.13, BAI08.04, DSS03.04, DSS04.05; NIST SP 800-221A – GV.AD-1, MA.RM-6, MA.IM1, AC01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01, CA-02, CA-05, CA-07, CA-08, CP-02, IR-04, IR-08, PL-02, PM-04, PM-31, RA-03, RA-05, RA-07, SA-04, SA08, SA-11, SI-02, SI-04, SR-05.
Приклади заходів:	проводиться спільне з постачальниками вивчення отриманого досвіду з минулих кіберінцидентів та управління вразливостями; щороку здійснюється перегляд політики, процесів та процедур виконання заходів кіберзахисту, які у разі потреби враховують отриманий досвід; визначені та періодично застосовуються показники оцінки ефективності процесів та процедур виконання заходів кіберзахисту.

2.3.4. **ID.IM-04**: розробити, затвердити, довести до відома персоналу, переглядати та удосконалювати Плани реагування на інциденти та інші плани кібербезпеки, які впливають на діяльність організації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3; Загальні вимоги – п. 74; НД ТЗІ 1.4-001-2000 – п. Д5.8, Д.5.6.2; НД ТЗІ 3.6-006-24 – CP-2, IR-8, PL-2, SR-2; Наказ-601 – PR.IP-9, RS.IM-1, RC.IM-1, PR.IP-10; COBIT 5 – DSS04.03; NIST SP 800-221A – MA.RR-4, MA.IM-1; NIST SP 800-53 Rev 5.1.1 – CP-02, IR-08, PL-02, SR-02.
Приклади заходів:	розроблено плани дій у надзвичайних ситуаціях (наприклад, реагування на інциденти, безперервність діяльності об’єкта кіберзахисту, відновлення після катастроф) для реагування та відновлення після несприятливих подій, які можуть перешкоджати діяльності, викривати конфіденційну інформацію або іншим чином загрожувати місії та функціонуванню об’єкта кіберзахисту; внесено інформацію щодо контактних осіб та комунікаційних схем, процесів обробки загальних сценаріїв, а також критеріїв для визначення пріоритетів, ескалації та підвищення рівня до усіх планів дій у надзвичайних ситуаціях; створено плани управління вразливостями для визначення та оцінювання всіх типів вразливостей для їх пріоритизації, тестування та внесення до плану реагування на ризики; плани кіберзахисту (включаючи внесені до них зміни) доведені до відома відповідальних за їх виконання посадових осіб та заінтересованих сторін; перегляд всіх планів кіберзахисту здійснюється щорічно або у разі визначеної потреби у їх значному покращенні.

2.4. **Середовище надання життєво важливих послуг та функцій (ID.BE)** – заходи перенесено у клас Організаційний контекст (GV.OC).

2.4.1. **ID.BE-01**: впроваджено у GV.OC-05.

2.4.2. **ID.BE-02**: впроваджено у GV.OC-01.

2.4.3. **ID.BE-03**: впроваджено у GV.OC-01.

2.4.4. **ID.BE-04**: впроваджено у GV.OC-04, GV.OC-05.

2.4.5. **ID.BE-05**: впроваджено у GV.OC-04.

2.5. **Управління** (**ID.GV**) перенесено в категорію GV.

2.5.1. **ID.GV-01**: впроваджено у GV.PO, GV.PO-01, GV.PO-02.

2.5.2. **ID.GV-02**: впроваджено у GV.OC-02, GV.RR, GV.RR-02.

2.5.3. **ID.GV-03**: перенесено у GV.OC-03.

2.5.4. **ID.GV-04**: перенесено у GV.RM-04.

2.6. **Стратегія управління ризиками (ID.RM)** перенесено в категорію GV.RM.

2.6.1. **ID.RM-01**: впроваджено у GV.RM-01, GV.RM-06, GV.RR-03.

2.6.2. **ID.RM-03**: перенесено у GV.RM-02.

2.6.3. **ID.RM-02**: впроваджено у GV.RM-02, GV.RM-04.

2.7. Управління ризиками в ланцюгу поставок **(ID.SC)** перенесено в категорію GV.SC.

2.7.1. **ID.SC-01**: впроваджено у GV.RM-05, GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10.

2.7.2. **ID.SC-02**: впроваджено у GV.OC-02, GV.SC-03, GV.SC-04, GV.SC-07, ID.RA-10.

2.7.3. **ID.SC-03**: перенесено у GV.SC-05.

2.7.4. **ID.SC-04**: впроваджено у GV.SC-07, ID.RA-10.

2.7.5. **ID.SC-05**: впроваджено у GV.SC-08, ID.IM-02.

3. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ (PR): розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення удосконалення систем реагування на кіберінциденти та кібератаки з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам.

3.1. **Управління ідентифікацією, автентифікація та контроль доступу (PR.AA)**: доступ до фізичних і логічних активів надається лише авторизованим користувачам, службам та обладнанню та управляється відповідно до оціненого ризику неавторизованого доступу.

3.1.1. **PR.AA-01:** забезпечити на рівні організації керування суб’єктами та їх обліковими даними для авторизованих користувачів, служб і апаратного забезпечення.

Нормативні посилання: ДСТУ ISO/IEC 27001:2013 –A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3;
Загальні вимоги – п. 11, 12, 13, 14, 15, 16, 17;
НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2;

	НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п.8.1; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.6-006-24 – AC-1, AC-0, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5,IA-6, IA-7, IA-8, IA-9, IA-10, IA-11; Наказ-601 – PR.AC-1; COBIT 5 – DSS05.04, DSS06.03; NIST SP 800-53 Rev 5.1.1 – AC-01, AC-02, AC-14, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11.
Приклади заходів:	ініціація запитів на отримання або на розширення існуючих прав доступу для співробітників, підрядників та інших осіб відстежується, переглядається та надається за потреби і погодженням з власниками системи або даних; видавати, управляти та відкликати криптографічні сертифікати та ідентифікаційні токени, криптографічні ключі (тобто управління ключами) та інші облікові дані; унікальний ідентифікатор для кожного пристрою обирається з незмінних характеристик апаратного забезпечення або з наданого у захищений спосіб ідентифікатора пристрою; забезпечується фізичне маркування авторизованого обладнання ідентифікатором для цілей інвентаризації та обслуговування.

3.1.2. **PR.AA-02**: забезпечити підтвердження ідентичності користувачів та їх відповідність обліковим записам на основі умов взаємодії.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.7.1.1, A.9.2.1; Загальні вимоги – п. 13 -18; НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» (далі – НД ТЗІ 2.5-010-03) – п. 7.2.9, 7.2.10; НД ТЗІ 2.5-004-99 – п. 9.2, 9.7, A.2.2, A.2.7; НД ТЗІ 2.5-008-2002 «Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2» (далі – НД ТЗІ 2.5-008-2002) – п. 6.5.3, 6.5.4, 6.5.12, 7.4.5; НД ТЗІ 3.6-006-24 – IA-12; Наказ-601 – PR.AC-6; CIS CSC 16; COBIT 5 – DSS05.04, DSS05.05, DSS05.07, DSS06.03;

	ANSI/ISA-62443-2-1-2024 «Security for industrial automation and control systems, Part 2-1: Security program requirements for IACS asset owners» (далі – ISA 62443-2-1:2009) – 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4; ANSI/ISA-62443-3-3-2013, Security for industrial automation and control systems Part 3-3: System security requirements and security levels (далі – ISA 62443-3-3:2013) – SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1; NIST SP 800-53 Rev 5.1.1 – IA-12.
Приклади заходів:	правилами організації визначено, що реєстрація та перевірка особи проводяться на підставі офіційних документів, що її засвідчують (паспорт, водійські права тощо); в організації проводиться перевірка унікальності облікових даних для кожної особи і використання облікових даних однієї особи іншими не допускається.

3.1.3. **PR.AA-03:** забезпечити автентифікацію користувачів, служб та апаратного забезпечення.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.6.2.1, A.6.2.2, A.9.2.1., A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.2.6, A.13.1.1, A.13.2.1, A.18.1.4; Загальні вимоги – п. 15, 18; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3; НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п. 8.1, 9.7, 9.8, 9.9; НД ТЗІ 3.7-001-99 – п. 6.4.1; Наказ-601 – PR.AC-3, PR.AC-7; COBIT 5 – APO13.01, DSS01.04, DSS05.03, DSS05.10, DSS06.10; NIST SP 800-218 – PO.5.2, AC-07, AC-12, IA-02, IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11.
Приклади заходів:	в організації впроваджено та використовується багатофакторна автентифікація; в організації передбачено обмеження на мінімальну довжину паролів, PIN-кодів і подібних автентифікаторів; в організації періодична повторна автентифікація користувачів, служб і апаратного забезпечення проводиться на основі ризику (наприклад, в архітектурах нульової довіри); в організації підтверджується, що уповноважений персонал має можливість доступу до облікових даних під час надзвичайних ситуацій.

3.1.4. **PR.AA-04**: забезпечити перевіряння, захист та передавання інформації про запити на ідентифікацію.

Нормативні посилання:	NIST SP 800-53 Rev 5.1.1 – IA-13.
Приклади заходів:	надійність ідентифікації підтверджена тим, що передача даних автентифікації та інформації користувача здійснюється через системи єдиного входу або між державними системами; впроваджено підходи на основі стандартів надійної ідентифікації в усіх контекстах, дотримуються усі інструкції щодо створення (наприклад, моделі даних, метаданих), захисту (наприклад, цифровий підпис, шифрування) та перевірки (наприклад, підтвердження підпису) надійності ідентифікації.

3.1.5. **PR.AA-05**: визначити в політиці, дотримуючись принципів найменших привілеїв і розподілу обов’язків, дозволи доступу, повноваження та авторизації, керувати ними, застосовувати та переглядати.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5; Загальні вимоги – п. 11, 12; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3; НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п. 8.1; Наказ-601 – PR.AC-1, PR.AC-3, PR.AC-4; COBIT 5 – DSS05.04; NIST SP 800-218 – PO.5.2, PS.1.1, AC-01, AC-02, AC-03, AC-05, AC-06, AC-10, AC-16, AC-17, AC-18, AC-19, AC-24, IA-13.
Приклади заходів:	перегляд привілеїв логічного та фізичного доступу здійснюється періодично та щоразу, коли змінюється роль або відбувається звільнення співробітника, або привілеї, які більше не потрібні, скасовуються; для прийняття рішення щодо надання доступу до запитуваного ресурсу враховуються атрибути запитувача (наприклад, геолокація, день/час, стан захищеності обладнання, з якого здійснюється доступ (кінцева точки); доступ і привілеї зменшені до необхідного мінімуму (наприклад, архітектура нульової довіри); здійснюється періодичний перегляд привілеїв, пов’язаних з критично важливими функціями діяльності організації, щоб підтвердити належний розподіл обов’язків.

3.1.6. **PR.AA-06**: здійснювати управління та моніторинг фізичного доступу до активів відповідно до ризику.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8; Загальні вимоги – п. 27, 28, 31, 49, 50, 51; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3; НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.6-006-24 – PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-18, PE-19, PE-20; Наказ-601 – PR.AC-2, PR.PT-4; COBIT 5 – DSS01.04, DSS05.05; NIST SP 800-53 Rev 5.1.1 – PE-02, PE-03, PE-04, PE-05, PE-06, PE-08, PE-18, PE-19, PE-20.
Приклади заходів:	в організації залучено персонал охорони, застосовуються камери спостереження, замки на вході, системи сигналізації та інші технічні засоби контролю перебування та обмеження доступу; в організації впроваджено додаткові заходи фізичної безпеки для просторів (приміщень), в яких розміщуються активи високого рівня критичності; в організації здійснюється супроводження відвідувачів у приміщеннях з активами, критичними для її функціонування.

3.2. **Обізнаність і навчання (PR.AT)**: персонал організації має обізнаність у кібербезпеці, проходить навчання з кібербезпеки таким чином, що може виконувати свої завдання, пов’язані із забезпеченням кібербезпеки.

3.2.1. **PR.AT-01**: забезпечити обізнаність та навченість персоналу таким чином, що він має знання та навички для виконання основних завдань щодо ризиків кібербезпеки.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.6.1.1, A.7.2.2, A.16.1.1; Загальні вимоги – п. 1, 2, 7, 8, 9; НД ТЗІ 1.1-002-99 – п. 7.2.4; НД ТЗІ 3.6-006-24 – AT-2, AT-3. Наказ-601 – PR.AT-1, PR.AT-3, RS.CO-1; COBIT 5 – APO07.03, APO10.04, APO10.05, BAI05.07; NIST SP 800-218 – PO.2.2; NIST SP 800-221A – GV.CT-3, GV.RR-2; NIST SP 800-53 Rev 5.1.1 – AT-02, AT-03.
Приклади заходів:	проводяться навчання та тренінги для працівників, підрядників, партнерів,

	постачальників та інших визначених користувачів непублічних ресурсів організації для їх обізнаності щодо базових принципів кібербезпеки; запроваджено навчання щодо розпізнавання та протидії спробам застосування методів соціальної інженерії, поширеним атакам, дотримання прийнятних політик безпеки, дотримання базових принципів кібергігієни (наприклад, виправлення програмного забезпечення, вибір паролів, захист облікових даних), а також інформування про атаки та підозрілу активність; співробітникам організації доводиться інформації про наслідки порушення політики кібербезпеки як для окремих користувачів, так і для організації в цілому; здійснюється періодичне оцінювання або перевірка розуміння користувачами основних практик кібербезпеки; встановлено вимоги щодо щорічного підвищення кваліфікації для покращення існуючих та впровадження нових практик з кібербезпеки.

3.2.2. **PR.AT-02**: забезпечити обізнаність та навченість співробітників, які безпосередньо виконують завдання із забезпечення кібербезпеки, кіберзахисту, таким чином, що вони мають знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.6.1.1, A.7.2.2; Загальні вимоги – п. 1, 2; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-24 – АТ-3; Наказ-601 – PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5; COBIT 5 – APO07.02, DSS06.03; NIST SP 800-218 – PO.2.2; NIST SP 800-221A – GV.CT-3, GV.CT-4, GV.RR-2; NIST SP 800-53 Rev 5.1.1 – AT-03.
Приклади заходів:	визначено посади, які мають доступ до важливих для даних організації, обіймання яких вимагає проходження додаткового навчання з питань кібербезпеки (персонал із фізичної та кібербезпеки, фінансовий персонал, вище керівництво); проводяться тренінги навчання та перевіряється рольова обізнаність щодо кібербезпеки для персоналу, який виконує спеціалізовані ролі, а також підрядників,

	партнерів, постачальників та інших третіх осіб; запроваджено періодичне оцінювання користувачів щодо розуміння практик кібербезпеки відповідно до їхніх спеціалізованих ролей; встановлено вимоги щодо щорічного підвищення кваліфікації для покращення існуючих та впровадження нових практик кібербезпеки.

3.2.3. **PR.AT-03**: впроваджено у PR.AT-01, PR.AT-02.

3.2.4. **PR.AT-04**: впроваджено у PR.AT-02.

3.2.5. **PR.AT-05**: впроваджено у PR.AT-02.

3.3. **Безпека даних (PR.DS)**: управління даними здійснюється відповідно до стратегії ризиків організації для захисту конфіденційності, цілісності та доступності інформації.

3.3.1. **PR.DS-01**: забезпечити конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем організації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.8.2.3; Загальні вимоги – п. 21, 38, 40, 42, 43, 50; НД ТЗІ 2.5-004-99 – 6.1, 6.2, 6.3, 7.1, 7.2; НД ТЗІ 3.6-006-24 – CA-3, CP-9, MP-8, SC-4, SC-7, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-3, SI-4, SI-7; Наказ-601 – PR.DS-1, PR.DS-5, PR.DS-6, PR.PT-2; COBIT 5 – APO01.06, BAI02.01, BAI06.01, DSS06.06; NIST SP 800-53 Rev 5.1.1 – CA-03, CP-09, MP-08, SC-04, SC-07, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-03, SI-04, SI-07.
Приклади заходів:	використовуються шифрування, цифрові підписи та криптографічні хеші для захисту конфіденційності та цілісності збережених даних у файлах, базах даних, образах дисків віртуальних машин, образах контейнерів та інших ресурсах; використовується повне шифрування дисків для захисту даних, що зберігаються на кінцевих пристроях користувачів; підтвердження цілісності програмного забезпечення здійснюється шляхом перевірки цифрових підписів; обмежено використання знімних носіїв для

	запобігання витоку даних; знімні носії, що містять незашифровану конфіденційну інформацію, фізично захищені наприклад, зберігаються у закритих сейфах або файлових шафах.

3.3.2. **PR.DS-02**: забезпечити конфіденційність, цілісність і доступність даних, що передаються.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3; Загальні вимоги – п. 34, 35, 36, 37; НД ТЗІ 2.5-004-99 – 6.5, 7.1,7.2, 7.4; НД ТЗІ 3.6-006-24 – AU-16, CA-3, SC-4, SC-7, SC-8, SC-11, SC-12, SC-13, SC-16, SC-40, SC-43, SI-3, SI-4, SI-7; НД ТЗІ 3.7-001-99 – п. 6.4.2; Наказ-601 – PR.DS-2, PR.DS-5; COBIT 5 – APO01.06, DSS06.06; NIST SP 800-53 Rev 5.1.1 – AU-16, CA-03, SC-04, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-40, SC-43, SI-03, SI-04, SI-07.
Приклади заходів:	застосувати шифрування, цифрові підписи та криптографічні хеші для захисту конфіденційності та цілісності при використанні мережевих комунікацій; здійснювати автоматичне шифрування або блокування вихідних електронних листів та інших комунікацій, що містять чутливі дані, залежно від класифікації таких даних; заблокувати доступ до особистої електронної пошти, сервісів обміну файлами, зберігання файлів та інших особистих додатків і сервісів комунікації з організаційних систем і мереж; забезпечити запобігання повторному використанню чутливих даних з продуктивних середовищ (наприклад, записи клієнтів) у інженерних, тестових та інших непродуктивних середовищах.

3.3.3. **PR.DS-10**: забезпечити конфіденційність, цілісність і доступність даних, що використовуються: до яких є доступ, які обробляються та регулярно оновлюються застосунками, користувачами або пристроями організації.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3; Загальні вимоги – п. 28, 29, 32, 37, 51; НД ТЗІ 2.5-004-99 – п. 6.4;

	НД ТЗІ 3.6-006-24 – AC-2, AC-3, AC-4, AU-9, AU-13, CA-3, CP-9, SA-8, SC-4, SC-7, SC-11, SC-13 , SC-24, SC-32, SC-39, SC-40, SC-43, SI-3, SI-4, SI-7, SI-10, SI-16; НД ТЗІ 3.7-001-99 – п. 6.4.2. Наказ-601 – PR.DS-5; COBIT 5 – APO01.06; NIST SP 800-53 Rev 5.1.1 – AC-02, AC-03, AC-04, AU-09, AU-13, CA-03, CP-09, SA-08, SC-04, SC-07, SC-11, SC-13 , SC-24, SC-32, SC-39, SC-40, SC-43, SI-03, SI-04, SI-07, SI-10, SI-16.
Приклади заходів:	здійснити видалення даних, які мають залишатися конфіденційними (наприклад, з процесорів та пам’яті), як тільки вони більше не потрібні; забезпечити захист даних, що використовуються, від доступу інших користувачів та процесів тієї ж платформи.

3.3.4. **PR.DS-11**: забезпечити створення, захист, підтримку та тестування резервних копій даних.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3; Загальні вимоги – п. 38; НД ТЗІ 2.5-004-99 – п. 8.3, 8.4; НД ТЗІ 3.6-006-24 – CP-6, CP-9; Наказ-601– PR.IP-4; COBIT 5 – APO13.01; NIST SP 800-218 – PS.3.1; NIST SP 800-53 Rev 5.1.1 – CP-06, CP-09.
Приклади заходів:	безперервно здійснювати резервне копіювання критичних даних у наближеному до реального часі; резервне копіювання інших даних здійснюється за встановленими графіками; тестування резервних копій та відновлення для всіх типів джерел даних здійснюються принаймні щороку; безпечно зберігати визначені резервні копії офлайн та поза межами офісу організації, щоб інцидент або катастрофа не пошкодили їх; зберігати резервні копії даних в різних місцях географічно та обмежити доступ до інформації про геолокацію місць зберігання.

3.3.5. **PR.DS-03:** впроваджено у ID.AM-08, PR.PS-03.

3.3.6. **PR.DS-04:** перенесено до PR.IR-04.

3.3.7. **PR.DS-05:** впроваджено у PR.DS-01, PR.DS-02, PR.DS-10.

3.3.8. **PR.DS-06:** впроваджено у PR.DS-01, DE.CM-09.

3.3.9. **PR.DS-07:** впроваджено у PR.IR-01.

3.3.10. **PR.DS-08:** впроваджено у ID.RA-09, DE.CM-09.

3.4.**Безпека платформ (PR.PS):** керування апаратним та програмним забезпеченням (наприклад, мікропрограми, операційні системи, застосунки), службами фізичних і віртуальних платформ відповідно до стратегії ризиків організації для захисту їх конфіденційності, цілісності та доступності.

3.4.1. **PR.PS-01**: встановити та застосовувати методи керування конфігурацією.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4; Загальні вимоги – п. 7, 10, 41, 43; НД ТЗІ 1.1-002-99 – п. 7.4; НД ТЗІ 2.5-004-99 – п. 10.1, 10.6; НД ТЗІ 3.6-006-24 – CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11; Наказ-601 – PR.IP-1, PR.IP-3, PR.PT-2, PR.PT-3; COBIT 5 - BAI01.06, BAI06.01, BAI10.01, BAI10.02, BAI10.03, BAI10.05; NIST SP 800-218 – PO.5.2, PS.1.1; NIST SP 800-53 Rev 5.1.1 – CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11.
Приклади заходів:	встановити, протестувати, розгорнути та підтримувати захищені базові конфігурації, які забезпечують виконання політик кібербезпеки організації та надають лише необхідні можливості (тобто принцип максимально обмеженої функціональності); переглянути всі налаштування конфігурацій за замовчуванням, які можуть потенційно вплинути на кібербезпеку при встановленні або оновленні програмного забезпечення; проводиться моніторинг виконуваного програмного забезпечення на предмет виявлення його відхилень від схвалених базових конфігурацій.

3.4.2. **PR.PS-02**: забезпечити належне обслуговування, заміну та видалення програмного забезпечення відповідно до ризику.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.11.2.4, A.15.1.1, A.15.2.1; Загальні вимоги – п. 36; НД ТЗІ 3.6-006-24 – CM-11, MA-3, SA-10, SI-2, SI-7; Наказ-601 – PR.IP-12, PR.MA-2; COBIT 5 – DSS05.04; NIST SP 800-218 – PO.5.2; NIST SP 800-53 Rev 5.1.1 – CM-11, MA-03(06), SA10(01), SI-02, SI-07.
Приклади заходів:	здійснювати виконання поточного та екстреного виправлення вразливостей у встановлені терміни, зазначені в плані управління вразливостями; здійснювати оновлення образів контейнерів та розгортання нових екземплярів контейнерів, щоб заміняти, а не оновлювати існуючі екземпляри; здійснювати заміну програмного забезпечення та версії сервісів, що досягли кінця життєвого циклу, на підтримувані та обслуговувані версії; здійснювати видалення несанкціонованого програмного забезпечення та сервісів, які становлять надмірні ризики; здійснювати видалення будь-яких непотрібних компонентів програмного забезпечення (наприклад, утиліт операційної системи), які можуть бути використані зловмисниками; затвердити та виконувати заходи планів підтримки та обслуговування програмного забезпечення і сервісів, що досягли кінця життєвого циклу.

3.4.3. **PR.PS-03**: забезпечити обслуговування, заміну та видалення обладнання відповідно до ризику.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.11.1.2, A.11.2.4, A.11.2.5; Загальні вимоги – п. 10, 39; НД ТЗІ 1.4-001-2000 – п. Д5.6.5; НД ТЗІ 3.6-006-24 – CM-7, SA-10, SC-3, SC-39, SC-49, SC-51; COBIT 5 – BAI09.03; NIST SP 800-218 – PO.5.2; NIST SP 800-53 Rev 5.1.1 – CM-07(09), SA-10(03), SC-03(01), SC-39(01), SC-49, SC-51.
Приклади заходів:	здійснювати заміну апаратного забезпечення, коли воно не має необхідних можливостей безпеки або не може

	підтримувати програмне забезпечення з необхідними можливостями безпеки; затвердити та виконувати заходи планів підтримки та обслуговування апаратного забезпечення, що досягло кінця життєвого циклу; здійснювати утилізацію апаратного забезпечення безпечно, відповідально та з можливістю аудиту.

3.4.4. **PR.PS-04**: створити записи журналів подій, які зроблені доступними для постійного моніторингу.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1; Загальні вимоги – п. 19, 20, 21, 22, 23; НД ТЗІ 2.5-004-99 – 9.1; НД ТЗІ 3.6-006-24 – AU-1, AU-2, AU-3, AU-6, AU-7, AU-11; Наказ-601 – PR.PT-1; COBIT 5 – APO11.04; NIST SP 800-218 – PO.3.3; NIST SP 800-53 Rev 5.1.1 – AU-01,AU-02, AU-03, AU-06, AU-07, AU-11.
Приклади заходів:	налаштувати всі операційні системи, додатки та сервіси (включаючи хмарні ресурси) для генерації записів в журнали подій; налаштувати генератори журналів для безпечного обміну їхніми журналами із системами та службами інфраструктури реєстрації організації; налаштувати генератори записів журналів подій для запису даних, необхідних для архітектур з нульовою довірою.

3.4.5. **PR.PS-05**: заборонити встановлення та виконання несанкціонованого програмного забезпечення.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CM-7, SC-34; NIST SP 800-53 Rev 5.1.1 – CM-07(02), CM-07(04), CM-07(05), SC-34.
Приклади заходів:	якщо цього вимагає ризик, обмежено використання програмного забезпечення лише дозволеними продуктами, а використання неавторизованого програмного забезпечення заборонено; джерело походження та цілісність нового програмного забезпечення перед його встановленням перевірено;

	налаштовано платформи на використання лише затверджених служб DNS, які блокують доступ до відомих шкідливих доменів, та на встановлення лише програмного забезпечення, схваленого організацією; налаштовано платформи для інсталювання лише затвердженого організацією програмного забезпечення.

3.4.6. **PR.PS-06**: інтегрувати практики безпечної розробки програмного забезпечення та контролювати їх виконання протягом життєвого циклу розробленого програмного забезпечення.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – SA-3, SA-8, SA-10, SA-11, SA-15, SA-17; Наказ-601 – PR.IP-2; NIST SP 800-53 Rev 5.1.1 – SA-03, SA-08, SA-10, SA-11, SA-15, SA-17.
Приклади заходів:	усі компоненти програмного забезпечення, розробленого організацією, захищені від втручання та несанкціонованого доступу; усе програмне забезпечення, вироблене організацією, перевірене на відсутність вразливостей у його оновленнях; програмне забезпечення, що використовується у виробничих середовищах, обслуговується і безпечно утилізується, коли воно більше не потрібне.

3.5. **Стійкість технологічної інфраструктури (PR.IR)**: керування архітектурою безпеки відповідно до стратегії ризиків організації для захисту конфіденційності, цілісності та доступності активів, а також забезпечення стійкості організації.

3.5.1. **PR.IR-01**: забезпечити захист мережі та середовища від неавторизованого логічного доступу та використання.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3; Загальні вимоги – п. 18, 25, 26, 27, 28, 29, 30, 31, 32, 35; НД ТЗІ 2.5-004-99 – п. 9.5; НД ТЗІ 3.6-006-24 – AC-3, AC-4, SC-4, SC-5, SC-7; НД ТЗІ 3.7-001-99 – п. 6.4.1; Наказ-601 – PR.AC-3, PR.AC-5, PR.DS-7, PR.PT-4; COBIT 5 – DSS01.04, DSS05.05; NIST SP 800-218 – PO.5.1; NIST SP 800-53 Rev 5.1.1 – AC-03, AC-04, SC-04, SC-05, SC-07.

Приклади заходів:	мережі організації та хмарні платформи логічно сегментовані відповідно до меж довіри та типів платформ (наприклад, IT, IoT, OT, мобільні, гості) і необхідні комунікації дозволені лише між сегментами; мережі організації логічно сегментовані від зовнішніх мереж і дозволені лише необхідні комунікації для входу в мережі організації із зовнішніх мереж; впроваджено архітектури з нульовою довірою, щоб обмежити доступ до кожного ресурсу до мінімально необхідного; перевірено кібербезпеку кінцевих точок перед тим, як їм надано доступ і використання виробничих ресурсів.

3.5.2. **PR.IR-02**: забезпечити захист технологічних активів від загроз навколишнього середовища.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3; Загальні вимоги – п. 49, 50, 51; НД ТЗІ 2.5-004-99 – п. 8.1; НД ТЗІ 3.6-006-24 – CP-2, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18, PE-23; Наказ-601 – PR.IP-5; COBIT 5 – DSS01.04, DSS05.05; NIST SP 800-53 Rev 5.1.1 – CP-02, PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18, PE-23.
Приклади заходів:	забезпечується захист обладнання організації від відомих екологічних загроз, таких як затоплення, пожежа, вітер, надмірна спека та вологість; захист від екологічних загроз та положення про належну операційну інфраструктуру включено у вимоги до постачальників послуг, які експлуатують системи від імені організації.

3.5.3. **PR.IR-03**: реалізувати механізми для досягнення вимог стійкості в нормальних і несприятливих ситуаціях.

Нормативні посилання:	Загальні вимоги – п. 12, 38; НД ТЗІ 1.1-002-99 – п. 6.4; НД ТЗІ 2.5-004-99 – п. 8.2, A.3.2; НД ТЗІ 3.6-006-24 – CP, IR, SA-8, SC-6, SC-24, SC-36, SC-39, SI-13; Наказ-601 – PR.PT-5;

	COBIT 5 – BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05; NIST SP 800-53 Rev 5.1.1 – CP, IR, SA-08, SC-06, SC-24, SC-36, SC-39, SI-13.
Приклади заходів:	запобігання використанню єдиних точок відмови в системах та інфраструктурі; здійснюється балансування навантаження для збільшення потужності та підвищення надійності; використовуються компоненти з високою доступністю, такі як резервне зберігання та джерела живлення, для підвищення надійності системи.

3.5.4. **PR.IR-04**: забезпечити управління пропорційністю та адекватністю застосування ресурсів для їх доступності.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CP-6, CP-7, CP-8, PM-3, PM-9; Наказ-601 – PR.DS-4; NIST SP 800-53 Rev 5.1.1 – CP-06, CP-07, CP-08, PM-03, PM-09.
Приклади заходів:	проводиться моніторинг використання пристроїв зберігання даних, живлення, обчислювальних ресурсів, пропускної здатності мережі та інших ресурсів; впроваджено прогнозування майбутніх потреб та відповідне масштабування ресурсів.

3.6. Управління ідентифікацією та контролем доступу (**PR.AC**): переміщено в PR.AA.

3.6.1. **PR.AC-01**: впроваджено у PR.AA-01, PR.AA-05.

3.6.2. **PR.AC-02**: перенесено у PR.AA-06.

3.6.3. **PR.AC-03**: впроваджено у PR.AA-03, PR.AA-05, PR.IR-01.

3.6.4. **PR.AC-04**: перенесено у PR.AA-05.

3.6.5. **PR.AC-05**: впроваджено у PR.IR-01.

3.7. **Процеси і процедури захисту інформації** (**PR.IP**) перенесено до інших категорій.

3.7.1. **PR.IP-01**: впроваджено у PR.PS-01.

3.7.2. **PR.IP-02**: впроваджено у ID.AM-08, PR.PS-06.

3.7.3. **PR.IP-03**: впроваджено у PR.PS-01, ID.RA-07.

3.7.4. **PR.IP-04**: перенесено у PR.DS-11.

3.7.5. **PR.IP-05**: перенесено у PR.IR-02.

3.7.6. **PR.IP-06**: впроваджено у ID.AM-08.

3.7.7. **PR.IP-07**: впроваджено у ID.IM, ID.IM-03.

3.7.8. **PR.IP-08**: перенесено у ID.IM-03.

3.7.9. **PR.IP-09**: перенесено у ID.IM-04.

3.7.10. **PR.IP-10:** впроваджено у ID.IM-02, ID.IM-04.

3.8. **Обслуговування (PR.MA)** впроваджено в ID.AM-08.

3.8.1. **PR.MA-01**: впроваджено у ID.AM-08, PR.PS-03.

3.8.2. **PR.MA-02**: впроваджено у ID.AM-08, PR.PS-02.

3.9. **Технології захисту (PR.PT)** впроваджено в інших категоріях.

3.9.1. **PR.PT-01**: впроваджено у PR.PS-04.

3.9.2. **PR.PT-02**: впроваджено у PR.DS-01, PR.PS-01.

3.9.3. **PR.PT-03**: впроваджено у PR.PS-01.

3.9.4. **PR.PT-04**: впроваджено у PR.AA-06, PR.IR-01.

3.9.5. **PR.PT-05**: перенесено у PR.IR-03.

4. ВИЯВЛЕННЯ (DE): проведення ідентифікації, збору та обробки кіберінцидентів/кібератак.

4.1. **Безперервний моніторинг (DE.CM)**: моніторинг активів з метою виявлення аномалій, індикаторів компрометації та інших потенційно несприятливих подій.

4.1.1. **DE.CM-01**: проводити постійний моніторинг мереж та мережевих служб для виявлення потенційно несприятливих подій.

Нормативні посилання:	Загальні вимоги – п. 4; НД ТЗІ 2.5-004-99 – п. 6.4, 9.1; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-24 – AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4; Наказ-601 – DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-7; COBIT 5 – DSS05.07; NIST SP 800-53 Rev 5.1.1 – AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04.
Приклади заходів:	забезпечено відстеження DNS, BGP та інших мережевих служб на наявність небажаних

	подій; забезпечено відстеження дротових та бездротових мереж на наявність підключень із неавторизованих кінцевих точок; забезпечено моніторинг засобів на наявність несанкціонованих або шахрайських бездротових мереж; здійснено порівняльний аналіз фактичних мережевих потоків з базовими лініями, щоб виявити відхилення; проведено моніторинг мережевих комунікацій для виявлення змін у положеннях безпеки з метою нульової довіри.

4.1.2. **DE.CM-02**: проводити постійний моніторинг фізичного середовища для виявлення потенційно несприятливих подій.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CA-7, PE-3, PE-6, PE-20; Наказ-601 – DE.CM-2; NIST SP 800-53 Rev 5.1.1 – CA-07, PE-03, PE-06, PE-20.
Приклади заходів:	відстежуються журнали подій систем контролю фізичного доступу (наприклад, зчитувачів бейджів), щоб знайти незвичайні шаблони доступу (наприклад, відхилення від норми) і невдалі спроби доступу; переглянуто та відстежено записи фізичного доступу (наприклад, з реєстрації відвідувачів, аркушів входу); забезпечено контроль засобів контролю фізичного доступу (наприклад, замки, засувки, петлі, сигналізацію) на наявність ознак втручання; забезпечено контроль фізичного середовища за допомогою систем сигналізації, камер і охоронців.

4.1.3. **DE.CM-03**: проводити постійний моніторинг діяльності персоналу та використання ним технологій для виявлення потенційно несприятливих подій.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 –A.12.4.1; Загальні вимоги – п. 19; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 9.1, 9.2, 9.7, 9.8, 9.9; НД ТЗІ 3.6-006-24 – AC-2, AU-12, AU- 13, CA-7, CM-10, CM-11; Наказ-601 – DE.CM-3, DE.CM-7; NIST SP 800-53 Rev 5.1.1 – AC-02, AU-12, AU-13, CA-07, CM-10, CM-11.
Приклади заходів:	забезпечено використання програмного забезпечення для аналітики поведінки з

	метою виявлення аномальної активності користувачів, щоб пом'якшити внутрішні загрози; забезпечено відстеження журналів логічних систем контролю доступу, щоб знайти незвичайні шаблони доступу та невдалі спроби доступу; забезпечено відстеження на постійній основі технології обману, включаючи облікові записи користувачів, для будь-якого використання.

4.1.4. **DE.CM-06**: проводити постійний моніторинг діяльності і послуг зовнішнього постачальника для виявлення потенційно несприятливих подій.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.14.2.7, A.15.2.1; Загальні вимоги – п. 7; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-24 – CA-7, PS-7, SA-4, SA-9, SI-4; Наказ-601 – DE.CM-6, DE.CM-7; COBIT 5 – APO07.06; NIST SP 800-53 Rev 5.1.1 – CA-07, PS-07, SA-04, SA-09, SI-04.
Приклади заходів:	забезпечено відстеження віддаленого та локального адміністрування й технічного обслуговування, які зовнішні постачальники виконують у системах об'єкта кіберзахисту; забезпечено моніторинг активності надавачів хмарних послуг, постачальників послуг Інтернету та інших постачальників послуг на наявність відхилень від очікуваної поведінки.

4.1.5. **DE.CM-09**: проводити постійний моніторинг використання комп'ютерного обладнання та програмного забезпечення, середовища їх виконання та даних для виявлення потенційно несприятливих подій.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3; Загальні вимоги – п. 44, 45, 46, 47, 48; НД ТЗІ 2.5-004-99 – 7.1, 7.2, 7.3, 7.4; НД ТЗІ 3.6-006-24 – AC-4, AC-9, AU-12, CA-7, CM-3, CM-6, CM-10, CM-11, SC-34, SC-35, SI-4, SI-7; Наказ-601 – PR.DS-6, PR.DS-8, DE.CM-4, DE.CM-5, DE.CM-7; NIST SP 800-53 Rev 5.1.1 – AC-04, AC-09, AU-12, CA-07, CM-03, CM-06, CM-10, CM-11, SC-34, SC-35, SI-04, SI-07.
Приклади заходів:	забезпечено моніторинг електронної пошти,

	Інтернету, обміну файлами, служб спільної роботи та інших поширених векторів атак для виявлення зловмисного програмного забезпечення, фішингу, витоку та крадіжки даних та інших небажаних подій; забезпечено відстеження спроби автентифікації, щоб виявити атаки на облікові дані та неавторизоване повторне використання облікових даних; забезпечено відстеження конфігурації програмного забезпечення на наявність відхилень від базових рівнів безпеки; забезпечено контроль апаратного та програмного забезпечення на наявність ознак втручання; забезпечено використання технологій з присутністю на кінцевих точках для виявлення проблем забезпечення кібербезпеки (наприклад, відсутні патчі, зараження зловмисним програмним забезпеченням, несанкціоноване програмне забезпечення) з метою перенаправлення кінцевих точок в середовище відновлення до того, як буде авторизовано доступ.

4.1.6. **DE.CM-04**: впроваджено у DE.CM-01, DE.CM-09.

4.1.7. **DE.CM-05**: впроваджено у DE.CM-01, DE.CM-09.

4.1.8. **DE.CM-07**: впроваджено у DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09.

4.1.9. **DE.CM-08**: впроваджено у ID.RA-01.

4.2. **Аналіз несприятливих подій (DE.AE):** аналіз аномалій, індикаторів компрометації та інших потенційно несприятливих подій, щоб їх охарактеризувати та виявити інциденти кібербезпеки.

4.2.1. **DE.AE-02**: впровадити періодичне проведення аналізу потенційно несприятливих подій для кращого розуміння пов’язаних подій.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – AU-6, CA-7, IR-4, SI-4; Наказ-601 – DE.AE-2; NIST SP 800-53 Rev 5.1.1 – AU-06, CA-07, IR-04, SI-04.
Приклади заходів:	впроваджено систему управління інформацією та подіями безпеки (SIEM) або інші інструменти для постійного моніторингу подій у журналі на наявність відомої зловмисної та підозрілої активності;

	використовується актуальна інформація про кіберзагрози в інструментах аналізу журналів, щоб підвищити точність виявлення та охарактеризувати суб'єкти загрози, їхні методи та показники компрометації; забезпечено регулярне проведення (вручну) перевірки подій журналу для технологій, які не можна належним чином контролювати за допомогою автоматизації; використано інструменти аналізу журналів для створення звітів про свої висновки.

4.2.2. **DE.AE-03**: впровадити періодичне проведення пошуку та зіставлення інформації з кількох джерел.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – AU-6, CA-7, PM-16, IR-4, IR-5, IR-8, SI-4; Наказ-601 – DE.AE-3; NIST SP 800-53 Rev 5.1.1 – AU-06, CA-07, PM-16, IR-04, IR-05, IR-08, SI-04.
Приклади заходів:	забезпечено постійне передавання даних журналу, створених з інших джерел, на відносно невелику кількість серверів журналів; використано технологію кореляції подій (наприклад, SIEM) для збору інформації, отриманої з кількох джерел; використано дані про кіберзагрози, щоб допомогти корелювати події серед джерел журналів.

4.2.3. **DE.AE-04**: забезпечити усвідомлення очікуваного впливу і масштабу несприятливих подій.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – PM-9, PM-11, PM-18, PM-28, PM-30; Наказ-601 – DE.AE-4; NIST SP 800-53 Rev 5.1.1 – PM-09, PM-11, PM-18, PM-28, PM-30.
Приклади заходів:	впроваджено SIEM або інші інструменти для оцінки впливу та масштабу, а також переглянуто й уточнено оцінки; створено власні оцінки впливу та масштабу.

4.2.4. **DE.AE-06**: забезпечити передавання інформації про несприятливі події до уповноважених підрозділів (організацій) для використання відповідного інструментарію.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4, PM-15, PM-16, RA-4, RA-10; Наказ-601 – DE.DP-4;

	NIST SP 800-53 Rev 5.1.1 – IR-04, PM-15, PM-16, RA-04, RA-10.
Приклади заходів:	використано програмне забезпечення для кібербезпеки, щоб створювати сповіщення та передавати їх до центру безпеки (SOC), служб реагування на інциденти та інструментів реагування на інциденти; забезпечено доступ служб реагування на інциденти та іншого уповноваженого персоналу до результатів аналізу журналу в будь-який час; забезпечено автоматичне створення та призначення сигналів у системі оповіщення, коли виникають певні типи несприятливих подій; забезпечено ручне створення та призначення сигналів у системі оповіщення об’єкта кіберзахисту, коли технічний персонал виявляє ознаки компрометації.

4.2.5. **DE.AE-07**: забезпечити збирання, виявлення та аналіз інформації про кіберзагрози та іншої контекстної інформації.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – PM-16, RA-3, RA-10; Наказ-601 – DE.AE-3; NIST SP 800-53 Rev 5.1.1 – PM-16, RA-03, RA-10.
Приклади заходів:	забезпечено безпечне надання інформації про кіберзагрози технологіям виявлення, процесам і персоналу; забезпечено безпечне надання інформації від інвентаризації активів до технологій виявлення, процесів і персоналу; забезпечено швидке отримання та швидкий аналіз інформації про вразливості технологічної інфраструктури від постачальників, третіх сторін і сторонніх консультантів із безпеки.

4.2.6. **DE.AE-08**: впровадити здійснення оголошення про інцидент, коли несприятливі події відповідають визначеним критеріям інциденту.

Нормативні посилання:	Загальні вимоги – п. 4; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-24 – IR-4, IR-5, IR-8; Наказ-601 – DE.AE-5; COBIT 5 – APO12.06; NIST SP 800-53 Rev 5.1.1– IR-04, IR-08.
Приклади заходів:	застосовано критерії інциденту до відомих і припущених характеристик діяльності, щоб визначити, чи слід оголошувати інцидент;

	враховано відомі помилкові спрацьовування під час застосування критеріїв інциденту.

4.2.7. **DE.AE-01**: впроваджено у ID.AM-03.

4.2.8. **DE.AE-05**: перенесено до DE.AE-08.

4.3. **Процеси виявлення** (DE.DP): впроваджено у та перенесено до інших категорій.

4.3.1. **DE.DP-01**: впроваджено у GV.RR-02.

4.3.2. **DE.DP-02**: впроваджено у DE.AE.

4.3.3. **DE.DP-03**: впроваджено у ID.IM-02.

4.3.4. **DE.DP-04**: впроваджено у DE.AE-06.

4.3.5. **DE.DP-05**: впроваджено у ID.IM, ID.IM-03.

5. РЕАГУВАННЯ (RS): запобігання кіберінцидентам та кібератакам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення.

5.1. **Управління інцидентами (RS.MA):** керування реагуванням на виявлені інциденти кібербезпеки.

5.1.1. **RS.MA-01:** впровадити виконання планів реагування на інцидент в координації з відповідними третіми сторонами одразу після оголошення інциденту.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.5; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-24 – IR-6, IR-7, IR-8, SR-3, SR-8; Наказ-601 – RS.RP-1, RS.CO-4; COBIT 5 – BAI01.10; NIST SP 800-53 Rev. 5.1.1 – IR-06, IR-07, IR-08, SR-03, SR-08.
Приклади заходів:	забезпечено автоматичне виявлення інцидентів; залучено допомогу з реагування на інциденти на основі аутсорсингу; призначено керівника з реагування на кожний інцидент; ініційовано виконання додаткових планів кібербезпеки, якщо це необхідно для підтримки реагування на інциденти (наприклад, забезпечення безперервного функціонування та аварійне відновлення).

5.1.2. **RS.MA-02:** впровадити здійснення сортування звітів про інциденти після їх підтвердження.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5; Загальні вимоги – п. 22, 23; НД ТЗІ 3.6-006-24 – IR-4, IR-5, IR -6; Наказ-601 – RS.AN-1, RS.AN-2; COBIT 5 – DSS02.07; NIST SP 800-53 Rev. 5.1.1 – IR-04, IR-05, IR-06.
Приклади заходів:	переглянуто звіти про інциденти, підтверджено те, що вони пов'язані з кібербезпекою та вимагають заходів з реагування на інциденти; застосовано критерії для оцінки інциденту.

5.1.3. **RS.MA-03:** впровадити класифікацію та пріоритизацію інцидентів.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.4; НД ТЗІ 3.6-006-24 – IR-4, IR-5, IR-6; Наказ-601 – RS.AN-4, RS.AN-2; NIST SP 800-53 Rev. 5.1.1 – IR-04, IR-05, IR-06.
Приклади заходів:	проведено аналіз і класифікацію кіберінцидентів на основі їх таксономії (наприклад, порушення даних, програми-вимагачі, DDoS, компрометація облікового запису); визначено пріоритетність інцидентів на основі їх масштабу, ймовірного впливу та критичного часу; вибрано стратегію реагування на інциденти для активних інцидентів, збалансовано необхідність швидкого відновлення після інциденту з необхідністю спостерігати за зловмисником або проводити більш ретельне розслідування.

5.1.4. **RS.MA-04**: впровадити інформування та підвищення рівнів критичності інцидентів (за потреби).

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.6; Загальні вимоги – п. 22, 23; НД ТЗІ 3.6-006-24 – IR-4, IR-5, IR-6, IR-7; Наказ-601 – RS.AN-2, RS.CO-4; NIST SP 800-53 Rev. 5.1.1 – IR-04, IR-05, IR-06, IR-07.
Приклади заходів:	відстежено та перевірено статус усіх поточних інцидентів; забезпечено координацію підвищення

	рівня критичності інциденту та його ескалацію з визначеними внутрішніми та зовнішніми заінтересованими сторонами.

5.1.5. **RS.MA-05**: впровадити застосування критеріїв для ініціювання відновлення після інциденту.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4, IR-8; NIST SP 800-53 Rev. 5.1.1. – IR-04, IR-08.
Приклади заходів:	застосовано критерії відновлення інциденту до відомих і передбачуваних характеристик інциденту, щоб визначити, чи слід ініціювати процеси відновлення інциденту; враховано можливий збій при виконанні заходів із відновлення інциденту.

5.2. **Аналіз інциденту (RS.AN):** проведення розслідувань для забезпечення ефективного реагування та експертизи інцидентів, а також заходів із відновлення після них.

5.2.1. **RS.AN-03:** запровадити проведення аналізу для встановлення того, що відбулося під час інциденту та які джерела виникнення інциденту.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – AU-7, IR-4; Наказ-601– RS.AN-3; NIST SP 800-53 Rev. 5.1.1 – AU-07, IR-04.
Приклади заходів:	визначено послідовність подій, що відбулися під час інциденту, і які активи та ресурси були залучені до кожної події; проаналізовано вразливості, загрози та суб’єкти загрози, які прямо чи опосередковано залучені до інциденту; проаналізовано інцидент, щоб знайти основні системні причини; перевірено будь-яку технологію шахрайства у кіберпросторі, щоб отримати додаткову інформацію про поведінку зловмисників.

5.2.2. **RS.AN-06:** запровадити здійснення запису дій, які виконуються під час розслідування інциденту, та забезпечити цілісність та збереження таких записів..

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.4; НД ТЗІ 3.6-006-24 – AU-7, IR-4, IR-6; Наказ-601 – RS.AN-3; COBIT 5 – APO12.06, DSS03.02, DSS05.07; NIST SP 800-53 Rev. 5.1.1 – AU-07, IR-04, IR-06.

Приклади заходів:	забезпечено запис та неможливість перезапису дій кожного спеціаліста з реагування на інциденти та інших осіб (наприклад, системних адміністраторів, інженерів з кібербезпеки), які виконують завдання з реагування на інциденти; забезпечено наявність особи, яка веде розслідування виникнення інциденту, документує деталі інциденту і несе відповідальність за збереження цілісності документації та джерел усієї інформації, яка задокументована.

5.2.3. **RS.AN-07**: запровадити здійснення збору та забезпечити цілісність та збереження даних про інциденти та метаданих.

Нормативні посилання:	ДСТУ ISO/IEC 27001:2013 – A.16.1.4; НД ТЗІ 3.6-006-24 – AU-7, IR-4, IR-6; COBIT 5 – APO12.06, DSS03.02, DSS05.07; NIST SP 800-53 Rev. 5.1.1 – AU-07, IR-04, IR-06.
Приклади заходів:	забезпечено збирання, зберігання та захист цілісності усіх відповідних даних про інциденти та метаданих (наприклад, джерело даних, дата/час збору) на основі процедур поводження та зберігання доказів.

5.2.4. **RS.AN-08**: запровадити оцінювання масштабу інциденту та документально його підтверджувати.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4, IR-8, RA-03, RA-7; NIST SP 800-53 Rev 5.1.1 – IR-04, IR-08, RA-03, RA-07.
Приклади заходів:	переглянуто інші потенційні цілі інциденту, щоб знайти індикатори компрометації та докази в наполегливості; автоматично запускати інструменти на цільових об'єктах для пошуку індикаторів компрометації та доказів стійкості.

5.2.5. **RS.AN-01**: впроваджено у RS.MA-02.

5.2.6. **RS.AN-02**: впроваджено у RS.MA-02, RS.MA-03, RS.MA-04.

5.2.7. **RS.AN-04**: перенесено до RS.MA-03.

5.2.8. **RS.AN-05**: перенесено до ID.RA-08.

5.3. **Звітування про реагування на інциденти та комунікація (RS.CO)**: координація заходів реагування з внутрішніми та зовнішніми заінтересованими сторонами відповідно до законів, нормативних актів або політик.

5.3.1. **RS.CO-02**: запровадити сповіщення внутрішніх та зовнішніх заінтересованих сторін про інциденти.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4, IR-6, IR-7, SR-3, SR-8; CIS Critical Security Controls Version 8 – 17.2; Наказ-601 – RS.CO-2, RS.CO-3; NIST SP 800-53 Rev 5.1.1– IR-04, IR-06, IR-07, SR-03, SR-08.
Приклади заходів:	дотримано визначеної процедури оповіщення щодо порушення даних після виявлення інциденту з порушенням даних, включаючи сповіщення постраждалих клієнтів; повідомлено ділових партнерів і клієнтів про інциденти відповідно до вимог контракту; повідомлено правоохоронні органи та уповноважені органи про інциденти на основі затверджених критеріїв плану реагування на інциденти.

5.3.2. **RS.CO-03:** запровадити надання інформації визначеним внутрішнім і зовнішнім заінтересованим сторонам.

Нормативні посилання:	Загальні вимоги – п. 7; НД ТЗІ 3.6-006-24 – IR-4, IR-6, IR-7, SR-3, SR-8; Наказ-601 – RS.CO-3, RS.CO-5; NIST SP 800-53 Rev. 5.1.1 – IR-04, IR-06, IR-07, SR-03, SR-08.
Приклади заходів:	забезпечено безпечний обмін інформацією відповідно до планів реагування та договори про обмін інформацією; добровільно поширено інформацію із видаленням усіх конфіденційних даних серед центрів обміну та аналізу інформації про спостережувані TTP зловмисників; сповіщено відділ кадрів про випадки зловмисної внутрішньої діяльності; забезпечено регулярне інформування вищого керівництва про статус великих інцидентів; забезпечено дотримання правил і протоколів, визначених у контрактах, щодо обміну інформацією про інциденти між суб'єктом забезпечення кібербезпеки та його постачальниками; забезпечено координацію методів комунікації в кризових ситуаціях між суб'єктом забезпечення кібербезпеки та

	його критично важливими постачальниками.

5.3.3. **RS.CO-01**: впроваджено у PR.AT-01.

5.3.4. **RS.CO-04**: впроваджено у RS.MA-01, RS.MA-04.

5.3.5. **RS.CO-05**: впроваджено у RS.CO-03.

5.4. **Пом'якшення інциденту (RS.MI):** виконання дій щодо запобігання розширенню подій та пом'якшення їх наслідків.

5.4.1. **RS.MI-01**: забезпечити локалізацію інцидентів.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4; Наказ-601 – RS.MI-1; NIST SP 800-53 Rev. 5.1.1 – IR-04.
Приклади заходів:	забезпечено автоматичне виконання дій стримування за допомогою технологічних рішень (наприклад, антивірусне програмне забезпечення) та інших технологій (наприклад, операційні системи, пристрої мережевої інфраструктури), які мають функції забезпечення кібербезпеки; надано дозвіл службам реагування на інциденти вручну вибирати та виконувати дії стримування; надано дозвіл третій стороні (наприклад, постачальнику послуг Інтернету, постачальнику послуг управління безпекою) виконувати дії зі стримування від імені об’єкта кіберзахисту; забезпечено автоматичне перенесення скомпрометованих кінцевих точок у віртуальну локальну мережу (VLAN) для відновлення.

5.4.2. **RS.MI-02**: забезпечити ліквідацію інцидентів.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4; Наказ-601 – RS.MI-2; NIST SP 800-53 Rev. 5.1.1 – IR-04.
Приклади заходів:	забезпечено автоматичне виконання завдань стримування за допомогою впроваджених технологій кіберзахисту та інших технологій, які мають такі функції (наприклад, операційні системи, мережа пристроїв інфраструктури); надано дозвіл службам реагування на інциденти вручну вибирати та виконувати дії зі стримування інциденту;

	надано дозвіл третій стороні (наприклад, постачальнику послуг управління безпекою) виконувати дії зі стримування від імені об’єкта кіберзахисту.

5.4.3. **RS.MI-03**: впроваджено у ID.RA-06.

5.5. **Планування реагування (RS.RP)**: впроваджено у RS.MA.

5.5.1. **RS.RP-01**: впроваджено у RS.MA-01.

5.6. **Покращення (RS.IM)**: впроваджено у ID.IM.

5.6.1. **RS.IM-01**: впроваджено у ID.IM-03, ID.IM-04.

5.6.2. **RS.IM-02**: впроваджено у ID.IM-03.

6. ВІДНОВЛЕННЯ (RC): поновлення штатного режиму функціонування об’єктів кіберзахисту після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки та кіберінциденту.

6.1. **Виконання плану відновлення після інциденту (RC.RP)**: проведення відновлювальних заходів для забезпечення доступності систем і служб, які постраждали від кіберінцидентів.

6.1.1. **RC.RP-01:** забезпечити виконання передбачених планом реагування на інцидент частини заходів щодо відновлення одразу після їх ініціалізації в ході реагування на інцидент.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CP-10, IR-4, IR-8; Наказ-601 – RC.RP-1; NIST SP 800-53 Rev. 5.1.1 – CP-10, IR-04, IR-08.
Приклади заходів:	розпочато процедури відновлення під час або після процесів реагування на інциденти; ознайомлено всіх осіб, які відповідають за відновлення, про плани відновлення та повноваження, необхідні для виконання кожного аспекту планів.

6.1.2. **RC.RP-02**: забезпечити відбір, визначення обсягу, пріоритетність та виконання заходів з відновлення.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CP-10, IR-4, IR-8; Наказ-601 – RC.RP-1; NIST SP 800-53 Rev. 5.1.1 – CP-10, IR-04, IR-08.
Приклади заходів:	обрано дії з відновлення на основі критеріїв, визначених у плані реагування на інцидент, і доступних ресурсів;

	змінено обрані дії з відновлення на основі переоцінки організаційних потреб і ресурсів.

6.1.3. **RC.RP-03:** переконатися у цілісності резервних копій та інших ресурсів, які підлягають відновленню, перед їх використанням для відновлення.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CP-2, CP -4, CP -9. NIST SP 800-53 Rev. 5.1.1 – CP-02, CP -04, CP -09.
Приклади заходів:	перевірено відновлені активи на наявність ознак компрометації, пошкодження файлів та інших питань цілісності активів перед їх використанням.

6.1.4. **RC.RP-04**: переглянути критичні для місії організації функції для встановлення операційних норм після інцидентів.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – PM-8, PM-9, PM-11, IR-1, IR-8; NIST SP 800-53 Rev. 5.1.1 – PM-08, PM-09, PM-11, IR-01, IR-08.
Приклади заходів:	використано записи про вплив на організацію і категоризацію системи (включно з цілями надання послуг), щоб підтвердити, що основні послуги відновлюються у відповідному порядку; забезпечено співпрацю з власниками систем, щоб підтвердити успішне відновлення систем і повернення до штатного режиму функціонування; відстежено продуктивність відновлених систем, щоб перевірити адекватність відновлення.

6.1.5. **RC.RP-05**: переконатися в цілісності відновлених активів, відновленні систем та служб і підтвердити їх робочий стан.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – CP-10; NIST SP 800-53 Rev. 5.1.1 – CP-10.
Приклади заходів:	перевірено відновлені активи на наявність індикаторів компрометації та усунення основних причин інциденту перед їх штатним використанням; перевірено правильність і адекватність дій з відновлення, вжитих перед запуском відновленої системи в режимі онлайн.

6.1.6. **RC.RP-06:** задекларувати завершення відновлення після інциденту, підтвердження критеріїв та пов’язаної з інцидентом документації.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4, IR-8; NIST SP 800-53 Rev. 5.1.1 – IR-04, IR-08.
Приклади заходів:	підготовлено звіт про завершення дії, в якому задокументовано сам інцидент, вжиті заходи реагування та відновлення, а також отримані уроки; оголошено про закінчення відновлення після інциденту та досягнення відповідних критеріїв.

6.2. **Комунікація з відновлення після інциденту (RC.CO)**: координація заходів з відновлення з внутрішніми та зовнішніми сторонами.

6.2.1. **RC.CO-03**: з забезпечити інформування визначених внутрішніх і зовнішніх заінтересованих сторін про заходи з відновлення та прогрес у відновленні операційних спроможностей.

Нормативні посилання:	НД ТЗІ 3.6-006-24 – IR-4, IR-6, SR-8; Наказ-601 – RC.CO-3; NIST SP 800-221A – GV.CO-1; NIST SP 800-53 Rev 5.1.1 – IR-04, IR-06, SR-08.
Приклади заходів:	забезпечено безпечний обмін інформацією про відновлення, включаючи хід відновлення, відповідно до планів реагування та договори про обмін інформацією; забезпечено регулярне інформування вищого керівництва про стан відновлення та хід відновлення для великих інцидентів; дотримано правила і протоколи, визначені у контрактах між суб'єктом забезпечення кіберзахисту та його постачальниками, щодо обміну інформацією про інциденти; скоординовано кризову комунікацію між суб'єктом забезпечення кіберзахисту та його критично важливими постачальниками.

6.2.2. **RC.CO-04**: запровадити інформування суспільства про відновлення після інциденту, використовуючи затверджені методи та повідомлення.

Нормативні посилання:	Загальні вимоги – п. 7; НД ТЗІ 3.6-006-24 – CP-2, IR-4; Наказ-601 – RC.CO-1, RS.CO-2; COBIT 5 – EDM03.02, MEA03.02; NIST SP 800-221A – GV.CO-1; NIST SP 800-53 Rev 5.1.1 – CP-02, IR-04.
Приклади заходів:	дотримано процедури сповіщення про

	інцидент для відновлення порушення даних після інциденту; описано кроки, які вживалися для відновлення після інциденту та запобігання його повторенню.

6.2.3. **RC.CO-01**: впроваджено у RC.CO-04.

6.2.4. **RC.CO-02**: впроваджено у RC.CO-04.

6.3. **Покращення (RC.IM)**: впроваджено у ID.IM.

6.3.1. **RC.IM-01**: впроваджено у ID.IM-03, ID.IM-04.

6.3.2. **RC.IM-02**: впроваджено у ID.IM-03.