Організація забезпечення конфіденційності, цілісності і доступності інформації у бюджетній сфері (основні напрямки впровадження)

ВЕБІНАР ДЛЯ ПРЕДСТАВНИКІВ БЮДЖЕТНИХ ТА КОМУНАЛЬНИХ УСТАНОВ

Денис Южаков
фахівець з внутрішнього аудиту/контролю
14 травня 2024

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

ПЛАН

Вступ (нормативна база).
1. Організаційна структура.
2. Інтеграція інформаційної безпеки у системи внутрішнього контролю.
    2.1. Елементи внутрішнього контролю.
    2.2. Управління ризиками.
3. Показники рівня забезпечення безпеки інформації.
    3.1. Цілі процесів.
    3.2. Метрики процесів.
4. Впровадження цілей заходів безпеки та заходів безпеки.
    4.1. Фізична безпека.
    4.2. Інформація з обмеженим доступом.
    4.2. Інтелектуальний захист.

Нормативна база

Бюджетний кодекс України від 08.07.2010 р, ст. 26 «Контроль та аудит у бюджетному процесі»

ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. (ДСТУ EN ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги)

ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

ВИЗНАЧЕННЯ

Внутрішнім контролем є комплекс заходів, що застосовуються керівником для:

забезпечення дотримання законності та ефективності використання бюджетних коштів,

досягнення результатів відповідно до встановленої мети, завдань, планів і вимог щодо діяльності бюджетної установи та її підвідомчих установ.

Розпорядники бюджетних коштів в особі їх керівників організовують внутрішній контроль і внутрішній аудит та забезпечують їх здійснення у своїх закладах та у підвідомчих бюджетних установах.

ч. 3 ст. 26 БКУ

Обов'язок

Організація повинна розробити, впровадити, підтримувати та постійно вдосконалювати систему інформаційної безпеки

ДСТУ ISO/IEC 27001:2023

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Організаційна структура

Організація повинна визначити внутрішні та зовнішні обставини, які важливі для її цілей та впливають на можливість досягнення наперед запланованого результату(-ів) її системи управління інформаційною безпекою

За напрямками діяльності
Створення та підтримка системи управління інформаційною безпекою.
Визначення та керівництво планом зменшення ризику інформаційної безпеки.
Контроль та перегляд системи управління інформаційною безпекою.
Захист від зловмисного програмного забезпечення.
Управління безпекою мережі та підключення.
Управління захистом кінцевої точки.
Управління ідентифікацією користувача та доступом за логінами.
Управління фізичного доступу до IT-ресурсів.
Управління документами з обмеженим доступом і пристроями виведення.
Моніторинг інфраструктури для проведення заходів, пов'язаних з безпекою.

За типом інформації
Стратегія інформаційної безпеки
Бюджет інформаційної безпеки
План інформаційної безпеки
Політика
Вимоги щодо інформаційної безпеки
Пізнавальні матеріали
Звіти про огляд інформаційної безпеки
Каталог служби захисту інформації
Профіль інформаційного ризику
Інформаційна панель інформаційної безпеки

Відповідальний
Підзвітний
Проконсультований
Поінформований

ВНУТРІШНІ	ЗОВНІШНІ	Затверджувач
		Автор
		Проінформований про тип інформації
		Користувач інформаційного типу

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Інтеграція інформаційної безпеки у системи внутрішнього контролю

Елементи внутрішнього контролю

Елементи внутрішнього контролю взаємопов'язані, стосуються всієї діяльності та фінансових і нефінансових процесів в установі

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

ПЛАНУВАННЯ

Під час планування системи управління інформаційною безпекою організація повинна визначити ризики та можливості, які потрібно мати на увазі, щоб:

- а) гарантувати, що система управління інформаційною безпекою може досягти запланованого результату(-ів);
- б) запобігти або зменшити небажані ефекти; і
- в) досягти постійного вдосконалення;
- г) планувати дії, які стосуються цих ризиків та можливостей, і
- д) як саме:
- інтегрувати й упровадити ці дії до процесів її системи управління інформаційною безпекою; та
- оцінювати ефективність цих дій.

УПРАВЛІННЯ РИЗИКАМИ

Оцінка ризиків інформаційної безпеки

- встановлення та підтримка критеріїв ризиків інформаційної безпеки;
- гарантування, що повторні оцінки ризиків інформаційної безпеки призводять до послідовних, дійових та порівняльних результатів;
- ідентифікація ризиків інформаційної безпеки;
- здійснення аналізу ризиків інформаційної безпеки;
- оцінка ризиків інформаційної безпеки

Оброблення ризиків інформаційної безпеки

- вибір доречних опцій оброблення ризиків інформаційної безпеки з урахуванням результатів оцінки ризиків;
- визначення всіх заходів безпеки, які необхідно впровадити для вибраної(-их) опції(-ій) оброблення ризиків;
- порівняння заходів безпеки з еталонними, підтвердження того, що не було опущено потрібних заходів безпеки;
- підготовка Положення щодо застосовності;
- розробка плану оброблення ризиків інформаційної безпеки;
- отримання від власників ризиків підтвердження плану оброблення ризиків інформаційної безпеки та згоди на залишкові ризики інформаційної безпеки

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Внутрішній аудит

Організація повинна проводити внутрішні аудити через заплановані інтервали часу

Цілі внутрішнього аудиту

- Система менеджменту інформаційної безпеки відповідає власним вимогам організації до такої системи та вимогам зовнішніх нормативних документів
- Підтвердження, що система менеджменту інформаційної безпеки результативно запроваджена та функціонує

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Програма внутрішнього аудиту

При розробці програми необхідно враховувати вагомість досліджуваних процесів та результати попередніх аудитів

РОЗДІЛИ ЗМІСТУ ПРОГРАМИ
Критерії та обсяги аудиту для кожного дослідження
Склад аудиторів та гарантії об'єктивність та незалежність процесу
Гарантії отримання результатів аудитів відповідними керівниками

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Моніторинг, вимірювання, аналіз та оцінювання

Унормування моніторингу	що саме потрібно моніторити й вимірювати, включаючи процеси інформаційної безпеки та заходи безпеки
	методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів
	коли моніторинг та вимірювання потрібно виконувати
	хто повинен виконувати моніторинг та вимірювання
	коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати
	хто повинен аналізувати й оцінювати ці результати

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Цілі заходів безпеки

Цілі інформаційної безпеки мають:
відповідати політиці інформаційної безпеки
бути вимірюваними (якщо доцільно)
враховувати вимоги до інформаційної безпеки, які застосовують, а також результати оцінювання ризиків та оброблення ризиків
відстежуватися з точки зору їх виконання
доведені до персоналу
відповідним чином оновлюватися
бути доступними у документальній формі

При плануванні шляхів досягнення цілей щодо інформаційної безпеки необхідно визначити:				
Що буде зроблено	Необхідні ресурси	Відповідальні виконавці	Терміни досягнення цілей	Як оцінюватимуться результати

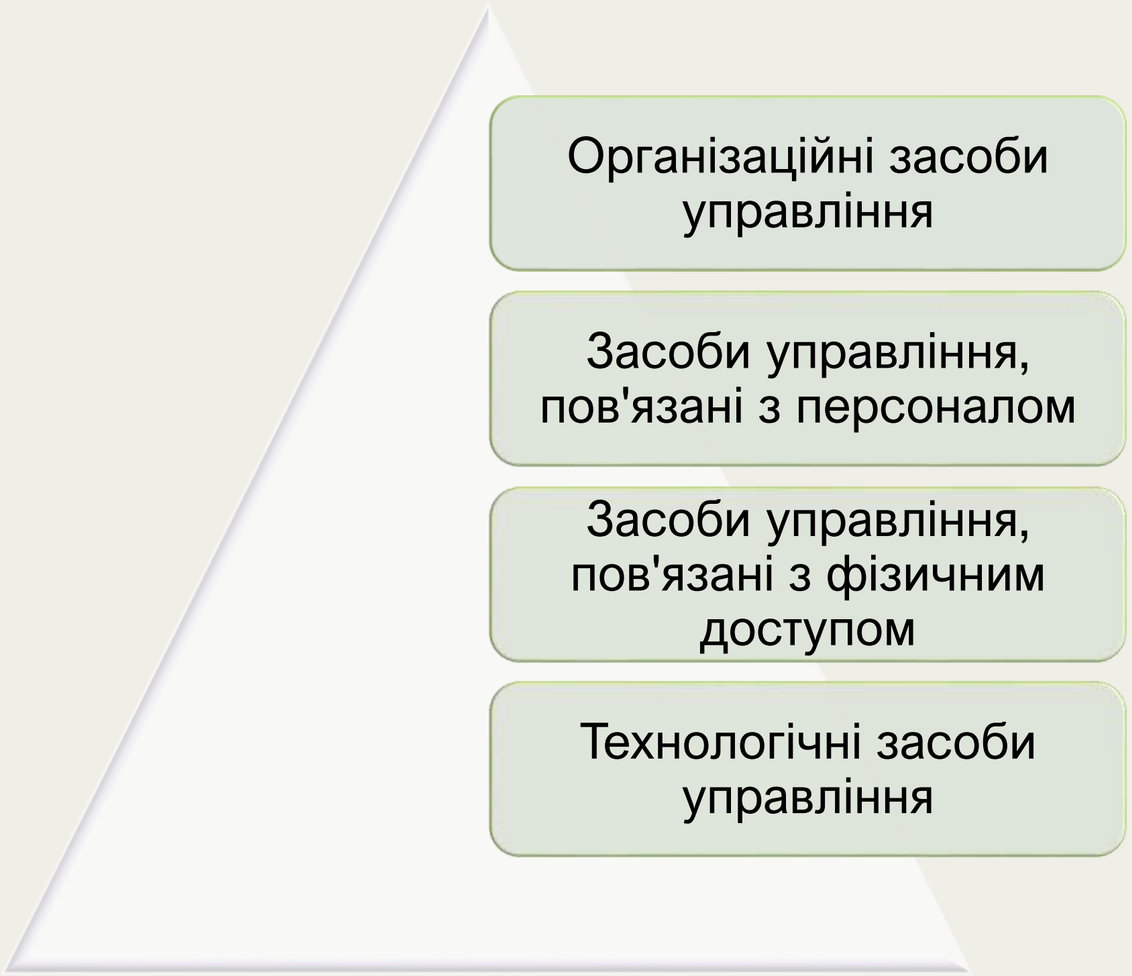
КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Оцінка цілей заходів безпеки

Політики безпеки
Організація інформаційної безпеки
Безпека людських ресурсів
Управління ресурсами СУІБ (системи управління інформаційною безпекою)
Контроль доступу
Криптографія
Фізична безпека та безпека інфраструктури
Безпека експлуатації
Безпека комунікацій
Придбання, розроблення та підтримка інформаційних систем
Взаємовідносини з постачальниками
Управління інцидентами інформаційної безпеки
Аспекти інформаційної безпеки управління безперервністю бізнесу
Відповідність

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Засоби управління інформаційною безпекою



КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Засоби управління, пов'язані фізичним доступом

Фізичні параметри безпеки	Фізичний вхід
Захист офісів, приміщень та пристроїв	Моніторинг фізичного захисту
Захист від фізичних та природніх загроз	Робота у захищених зонах
Пустий стіл та пустий екран	Розташування та захист обладнання
Захист активів поза територією	Засоби зберігання
Служби забезпечення	Захист кабельних мереж
Обслуговування обладнання	Безпечна утилізація та повторне використання обладнання

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Технологічні засоби управління

Кінцеві пристрої користувача	Привілейовані права доступу	Встановлення застосунків в операційній системі	Безпечне кодування
Обмеження доступу до інформації	Доступ до вихідного коду	Безпека мереж	Тестування забезпечення безпеки (при прийманні)
Безпечна аутентифікація	Керування продуктивністю	Безпека мережевих сервісів	Розробка передана на аутсорсинг
Захист від шкідливого програмного забезпечення	Керування технічними вразливостями	Розподіл мереж	Розмежування середовища розробки, тестування, експлуатації
Менеджмент конфігурацій	Видалення інформації	Веб-фільтрація	Керування змінами
Маскування даних	Попередження витоку даних	Використання криптографії	Дані для тестування
Резервне копіювання інформації	Надмірність пристроїв обробки інформації	Життєвий цикл розробки безпечного ПЗ	Захист інформаційних систем під час аудиту
Ведення журналів (логів)	Моніторинг дій	Застосування вимог безпеки	
Синхронізація годинників	Використання утиліт з привілейованими правами	Безпечна архітектура систем і принципи розробки	

Інші проблеми в організації захисту інформації

- Якість провайдера
- Застосування санкційного програмного забезпечення
- Фізична втрата обладнання

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ

Дякую за увагу!

ВЕБІНАР ДЛЯ ПРЕДСТАВНИКІВ БЮДЖЕТНИХ ТА КОМУНАЛЬНИХ УСТАНОВ

Денис Южаков
фахівець з внутрішнього аудиту/контролю
14 травня 2024 р.

КОМПЛЕКСНІ БЮДЖЕТНІ СИСТЕМИ