УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Модуль 1. Теорія управління інформаційною безпекою

Лекція 3. Нормативна документація СУІБ

1. Підготовка документів для впровадження СУІБ.
2. Внутрішні документи. Політика ІБ.

Стандарт ISO 27001 містить кращі практики і загальні принципи з управління інформаційною безпекою компанії.

План впровадження стандарту

Підготовка документів

Для впроваадження СУІБ необхідно підготувати пакет документів, який має існувати і створюватись в компанії. Що створювати, а що ні – вирішує людина, відповідальна за проект. У кожному конкретному випадку перелік документів матиме конкретні особливості. Будь-який документ має переглядатися по мірі необхідності, але не менше 1 разу на рік.

Мінімальний набір документів, необхідних для ISO/IEC версії 2013:

№ п/п	Документи	Номер пункту стандарту
1	Область дії	4.3
2	Політика інформаційної безпеки	5.2, 6.2
3	Методологія оцінки і обробки ризиків	6.1.2
4	Положення про застосування	6.1.3 d)
5	План усунення ризиків	6.1.3 e), 6.2
6	Звіт про оцінку ризиків	8.2
7	Процедура управління документами	7.5
8	Процедура управління записами	7.5
9	Порядок внутрішнього аудиту	9.2
10	Порядок усунення несправностей	10.1

Мінімальний набір документів, необхідних для ISO/IEC версії 2013:

№ п/п	Документи	Номер пункту стандарту
11	Визначення ролей і обов’язків	A.7.1.2, A.13.2.4
12	Матеріально-технічні ресурси активів	A.8.1.1
13	Допустиме використання активів	A.8.1.3
14	Політика управління доступом	A.9.1.1
15	Політика управління IT	A.12.1.1
16	Принципи розробки захищеної системи	A.14.2.5
17	Політика безпеки постачальника	A.15.1.1
18	Процедура управління інцидентами	A.16.1.5
19	Процедурі безперервності бізнесу	A.17.1.2
20	Юридичні, регулюючі і договорні вимоги	A.18.1.1

Документи, що не є обов’язковими з точки зору стандарту:

№ п/п	Документи	Номер пункту стандарту
1	Політика використання власних пристроїв (BYOD)	A.6.2.1
2	Мобільні пристрої і політика віддаленого доступу	A.6.2.1
3	Політика класифікації інформації	A.8.2.1, A.8.2.2, A.8.2.3
4	Парольна політика	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
5	Політика знищення та утилізції	A.8.3.2, A.11.2.7
6	Процедура для роботи в контрольованих зонах	A.11.1.5
7	Політика чистого екрану і робочого столу	A.11.2.9
8	Політика управління змінами	A.12.1.2, A.14.2.4
9	Політика резервного копіювання	A.12.3.1
10	Політика передачі інформації	A.13.2.1, A.13.2.2, A.13.2.3
11	Аналіз впливу на бізнес	A.17.1.1
12	План тестування	A.17.1.3
13	Технічне обслуговування і огляд плану	A.17.1.3
14	Стратегія безперервності бізнесу	A.17.2.1

Внутрішні документи

- Наказ про рішення створити і впровадити СУІБ
- Наказ про призначення відповідальних осіб
- Наказ про створення комісії з питань ІБ
- Протоколи засідань комісії з питаньІБ

Типова структура документа СУІБ

1. Ціль створення документа
2. Область дії документа, ролі і обов’язки задіяних сторін
3. Посилання на перехресні документи
4. Основна частина документа, яка містить саму суть політики, процедури і т.д.
5. Розділ про перегляд документа з вказуванням терміну перегляду
6. Історія змін

Процедура управління документами і записами

Основні розділи

- Правила форматування документів
- Опис процесів роботи з різними внутрішніми документами різного типу
- Правила інформування співробітників компанії
- Ідентифікація документів

Політика ІБ. Основні положення

Політика затверджується керівником компанії одноосібно або спільно з радою директорів компанії.

Основні положення

Співробітник, відповідальний за забезпечення ІБ в компанії, здійснює управління процесами інформаційної безпеки, забезпечуючи грамотне управління інформаційними ресурсами.

Для управління інформаційними ресурсами і СУІБ в компанії може бути створений комітет з ІБ, що забезпечує прийняття регламентів і заходів забезпечення ІБ колегіальним способом.

Співробітник, відповідальний за ІБ, щорічно і при появі істотних змін проводить аналіз існуючих політик ІБ з метою забезпечення їх постійної придатності, адекватності та результативності.

Співробітник, відповідальний за ІБ, відповідає за визначення детальних вимог до системи інформаційної безпеки і контролює виконання цих вимог.

Доступ до інформації та інформаційних ресурсів компанії надається тільки особам / співробітникам, яким цей доступ необхідний для виконання посадових або договірних зобов'язань. При цьому рівень доступу - мінімально можливий.

Для кожного інформаційного ресурсу компанії визначено власника ресурсу (Співробітник або підрозділ), що відповідає за надання доступу до ресурсу і ефективне функціонування заходів захисту інформації, застосованих для захисту ресурсу.

Політика ІБ. Основні положення

Основні положення

За всіма фактичним або можливим порушенням інформаційної безпеки проводиться розслідування з метою визначення причин настання інциденту. У разі необхідності, до розслідування можуть підключатися сторонні компанії.

Засоби управління інформаційною безпекою впроваджуються по результатами проведення оцінки ризиків інформаційної безпеки.

У компанії проводиться регулярне навчання персоналу в області інформаційної безпеки.

У компанії щорічно проводиться незалежний аудит інформаційної безпеки, що забезпечує актуалізацію системи в цілому.

Компанія раз на рік проводить внутрішній аудит інформаційної безпеки.

У компанії створено і реалізовано детальні політики та процедури для підтримки основної політики.

Компанія виконує законодавчі і нормативні вимоги, пред'являються до неї.

Реєстр ресурсів

№ п/п	Тип ресурсу	Власник ресурсу	Власник ризику	Користувач ресурсу	К	Ц	Д
	Інформація						
	Обладнання (комп’ютерне, прикладне мережеве)						
	Програмне забезпечення						
	Сервіси (внутрішні, зовнішні)						
	Персонал						
	Приміщення						

Методологія оцінки і обробки ризиків, звіт

Шкала цінності ресурсів

Цінність ресурсу	Опис
1	Втрата конфіденційності, і / або цілісності, і / або доступності ресурсу практично не призводить до наслідків з фінансовими втратами.
2	Втрата конфіденційності, і / або цілісності, і / або доступності ресурсу призводить до незначних фінансових втрат і має незначний вплив на репутацію компанії.
3	Втрата конфіденційності, і / або цілісності, і / або доступності ресурсу призводить до значних фінансових втрат і має значний вплив на репутацію компанії.
4	Втрата конфіденційності, і / або цілісності, і / або доступності ресурсу призводить до великих фінансових втрат (визначити суму), має значний вплив на репутацію компанії і може привести до зупинці роботи бізнес-процесу.

Методологія оцінки і обробки ризиків, звіт

Шкала ступеню вразливості ресурсів

Цінність ресурсу	Опис
1	Вразливість практично не призводить до розкриття конфіденційної інформації.
2	Вразливість призводить до розкриття відомостей, які відносяться до комерційної таємниці, персональних даних, і призводить до фінансових втрат.
3	Вразливість призводить до розкриття відомостей, які відносяться до комерційної таємниці, персональних даних, і призводить до значних фінансових втрат, має значний вплив на репутацію компанії і може привести до зупинки роботи бізнес-процесу.
4	Приводить до зупинки бізнес-процесу і порушення закону.

Методологія оцінки і обробки ризиків, звіт

Шкала ймовірності реалізації загроз

Цінність ресурсу	Опис
1	Загроза має місце в історичному аспекті.
2	Загроза виникає 2-3 рази на рік по галузі.
3	Загроза виникала 1 раз в компанії.
4	Загроза проявляється 2-3 рази на рік в компанії.

Рівень ризику по окремим парам загроза/вразливість

$$Р=ЦН*СВ*В$$

ЦН – цінність активу

СВ – ступінь вразливості ресурсу

В – вірогідність реалізації загрози

Методологія оцінки і обробки ризиків, звіт

Приклад звіту по оцінці ризиків для ресурсів СУІБ компанії

Ресурс	Загрози	Вразливості	ЦН	СВ	В	Р
Комп’ютер ХХХ	НСД	Вільний доступ до робочого місця	3	3	2	18

Шкала визначення критеріїв прийняття рішення

Умовне позначення ризику	Числове значення оцінки ризику	Рішення відносно подальшої обробки ризику
Низький ризик	1-10	Ризик вважається незначним. Обробка не вимагається.
Середній ризик	11-21	Обробка ризику може виконуватися або не виконуватися
Високий ризик	22-64	Ризик вважається суттєвим. Обробка обов’язкова.

Положення про застосування

№ контролю	Назва	Опис	Застосування контролю	Причина виключення контролю	Метод реалізації
A.5	Політика безпеки				
A.5.1	Політика Інформаційної безпеки				
A.5.1.1	Документована політика ІБ	Політика ІБ має бути затверджена керівництвом, видана і доведена до відома всіх співробітників організації, а також сторонніх організацій	Так		Політика СУІБ
A.5.1.2	Перегляд політики ІБ	Політика ІБ має бути піддана аналізу і перегляду через задані проміжки часу або при появі суттєвих змін характеристик цілей безпеки	Так		Політика СУІБ

Положення про застосування

№ контролю	Назва	Опис	Застосування контролю	Причина виключення контролю	Метод реалізації
A.6	Організація інформаційної безпеки				
A.6.1	Внутрішня організація				
A.6.1.1	Ролі та відповідаль-ність в рамках ІБ	Всі відповідальності в полі ІБ мають бути визначені та закріплені	Так		Обов’язки персоналу по забезпеченню ІБ перераховані в різних документах СУІБ
A.6.1.2	Розподіл Обов’язків по забезпеченню ІБ	Суперечливі обов’язки і зони відповідальності мають бути розподілені з метою зниження можливостей для НС, випадкової зміни чи неправильного використання активів організації	Так		Обов’язки персоналу по забезпеченню ІБ перераховані в різних документах СУІБ

План усунення ризиків

Тип ресурсу	Загрози	ЦН	СВ	В	Р	ДР	Заплановані контрміри	ОР	Термін реалізації контрміри	Відповідальний

ЦН – цінність активу;
СВ – ступінь вразливості ресурсу (оцінюється по шкалі від 1 до 4);
В – вірогідність реалізації загрози;
Р – рівень ризику;
ДР – допустимий рівень ризику;
ОР – остаточний рівень ризику.

Політика контролю доступу

Отримання доступу до інформаційних ресурсів компанії

Повернення ресурсів компанії по закінченню договорів

Використання корпоративної мережі та мережі Інтернет