CERT-UA

План-методика виконання робіт з оцінки стану захищеності ДІР в ІТС

Автори:
Міснік Олексій
Антонішин Михайло
Computer Emergenscy Response Team of Ukraine – CERT-UA
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

№	Етапи робіт	Термін виконання	Проміжний результат	Примітка
0.	Збір загальної інформації			
0.1	Організаційно-штатна структура Об'єкту оцінки. Визначення підрозділів, співробітники яких підлягатимуть інтерв'юванню.		Протокол робочої наради	
0.2	Обговорення етапу анкетування співробітників. Визначення і погодження переліку питань.			
0.3	Обговорення питання порядку отримання конфігураційних файлів.			
0.4	Визначення меж мережевого контуру з метою ідентифікації області дії під час моделювання «зовнішніх загроз».			
0.5	Узгодження загальних організаційних питань			
1.	Призначення ІТС. Інвентаризація інформаційних активів. Ідентифікація технічно-виробничих (бізнес-) процесів.			
1.1	З'ясування переліку виробничих (бізнес-) процесів (далі – Процес), функціонування яких забезпечується інформаційно-телекомунікаційною системою (далі – ІТС) Об'єкта.		Перелік виробничих процесів	
1.2	Формування переліку автоматизованих та інформаційних систем (із зазначенням їх структури, складу, програмного забезпечення, технології, апаратних засобів), що підтримують існуючі Процеси. Розробка реєстру інформаційних (систем) активів Об'єкта.		Перелік (реєстр) інформаційних активів	
1.3	Вивчення організаційно-розпорядчих документів з метою визначення статусу систем на Об'єкті, ідентифікації відповідальних осіб та аналізу повноти вимог в частині, що стосується питань інформаційної безпеки.			
1.4	Збір та систематизація даних щодо програмно-апаратного забезпечення, яке використовується: - серверне обладнання;		Перелік програмного і апаратного забезпечення	

	- активне мережеве обладнання; - автоматизовані робочі місця - програмно-апаратні засоби захисту **Необхідна інформація: виробник, hostname, конфігурація:CPU/RAM/ROM, мережеві ідентифікатори, операційна система, призначення.* - програмне забезпечення, що використовується (операційні системи, прикладні програми).			
2.	Аналіз організаційно-правового забезпечення			
2.1	Аналіз організаційно-правового забезпечення передбачає перевірку наявності та повноти змісту керівних і розпорядчих документів, а саме: - стратегії (концепції) розвитку інформаційних технологій; - політики інформаційної безпеки; - плану захисту інформації; - інструкцій, що регламентують основні процеси експлуатації і життєзабезпечення ІТС Об'єкта, а також питання захисту інформації, яка в ній циркулює; - інших службових документів (заявок, реєстраційних журналів тощо). - договірні документи (послуги з доступу до Інтернет тощо).		Перелік наданої (наявної) документації. Звіт щодо стану нормативно-правового забезпечення і його відповідності	
3.	Класифікація інформаційних ресурсів			
3.1	Класифікація інформації (за видом, за порядком доступу), що обробляється за допомогою автоматизованих систем (програмно-апаратних комплексів) і циркулює в ІТС Об'єкта. Аналіз організаційно-розпорядчих документів, що передбачають класифікацію інформації за категоріями та порядок віднесення останньої до них.			Проведення бесід з відповідальними представниками структурних підрозділів
3.3	Визначення осередків (місць) обробки інформації та складання карти інформаційних потоків*. ** Карта інформаційних потоків має враховувати існуючу структуру ІТС та відображати:* *- вид інформації, що передається;*		Карта інформаційних потоків	

	- назву АС/ПАЗ, за допомогою яких вона обробляється; *- види середовищ розповсюдження, якими вона циркулює, та способи передавання;* *- напрями інформаційного обміну (від джерела до отримувача).* *Кінцева версія КІП формується після складання схеми логічної сегментації та адресації в комп'ютерній мережі Об'єкта.*			
4.	Аналіз порядку розподілу прав доступу			
4.1	З'ясування переліку категорій (ролей) користувачів, визначення наявних у них прав і виду доступу до автоматизованих систем; аналіз документів та ідентифікація відповідальних за АС осіб.			
4.2	Побудова матриці доступу до автоматизованих систем*. ** Окремо відображаються співробітники, які мають право адміністративного доступу до програмного і/або апаратного забезпечення Об'єкта.*		Карта розподілу прав доступу (матриця доступу)	Зведена таблиця формується за участю компетентних співробітників Об'єкта
5.	Фізичне обстеження місць розміщення апаратного забезпечення			
5.1	Опис серверного приміщення (засоби пожежної безпеки, система підтримки кліматичних умов, електроживлення). **при обстеженні врахувати вимоги стандарту TIA/EIA-942*		Звіт щодо оцінки відповідності ЦОД вимогам TIA/EIA-942	Фахівцям Виконавця має бути наданий доступ до серверного приміщення та інших місць розміщення обладнання
5.2	Вивчення порядку розміщення апаратного-забезпечення (в т.ч. того, що знаходиться за межами серверного приміщення), аналіз зв'язків між ним, ідентифікація зв'язків з іншими мережами передачі даних.			
5.3	Розробка схеми фізичної комутації активного мережевого, серверного обладнання і засобів захисту.		Схема фізичної комутації апаратного забезпечення.	
5.4	Інвентаризація програмно-апаратного забезпечення		Звіти та статистичний зріз	Із врахуванням п. 1.4
6.	Аналіз порядку функціонування інформаційно-телекомунікаційної системи			

6.1	Загальна структура корпоративної мережі (філії, структурні підрозділи, зв'язки між ними).		Загальна структурна схема корпоративної мережі Об'єкта	
6.2	Детальна структура корпоративної мережі: - структура телекомунікаційної мережі; мережева топологія; - порядок сегментації ЛОМ; - порядок розмежування інформаційних потоків; - маршрутизація і IP-адресація; - характеристика підключень до інших мереж передачі даних (вхідних та вихідних); - характеристика бездротових мереж; - телефонний зв'язок; ВКЗ.		Схема адресації і маршрутизації	
6.3	Основні сервіси та служби: - підключення до Інтернет (обмеження, характеристика каналів доступу, proxy); - централізоване управління корпоративною мережею, об'єднання комп'ютерів (домен, робоча група тощо); - система корпоративного електронного поштового обміну; - обробка і зберігання даних (smb, ftp, dfs); - бази даних та системи керування ними; - система доменних імен dns; - системи дистанційного банківського обслуговування; - Інтернет-ресурси (веб-сайт).			
6.4	Характеристика захищеного вузла доступу до мережі Інтернет (за наявності).			
7.	Аналіз організаційно-технічного забезпечення			
7.1	Технічні заходи захисту			
7.1.1	Резервування апаратного забезпечення.			
7.1.2	Порядок зберігання конфігурацій та іншої технологічної інформації.			
7.1.3	Порядок здійснення резервного копіювання даних.			

7.1.4	Порядок моніторингу працездатності активного мережевого та серверного обладнання, а також каналів зв'язку.			
7.1.5	Порядок реєстрації (фіксації) і зберігання інформації про системні події і події безпеки.			
7.1.6	Порядок оновлення програмного забезпечення; порядок контролю та підтримки програмного забезпечення в актуальному стані.			
7.1.7	Обмеження підключення до СКС/ЛОМ.			
7.1.8	Правила розмежування прав доступу до елементів системи.			
7.1.9	Порядок введення/виведення інформації.			
7.1.10	Віддалене адміністрування - порядок ізоляції технологічних інформаційних потоків; - обмеження доступу до адміністративних інтерфейсів; - протоколи та засоби адміністрування; - ідентифікація, авторизація і облік.			З урахуванням матриці доступу
7.1.11	Парольна політика. Автентифікація, авторизація і облік.			
7.1.12	Обробка інцидентів інформаційної безпеки. Служба HelpDesk.			
7.2	Засоби мережевого захисту			
7.2.1	Антивірусний захист			
7.2.2	Міжмережеве екранування та фільтрація інформаційних потоків			
7.2.3	Системи виявлення і протидії вторгненням; захист від мережевих атак.			
7.2.4	Захист інформації від витоку.			
7.2.5	Криптографічний захист інформації.			
7.2.5	Контроль захищеності систем та їх відповідності стандартам інформаційної безпеки.			
8.	Аналіз користувацького сегменту			
8.1	Визначення категорій користувачів ІТС відповідно до виконуваних ними функцій та наданих повноважень.			

8.2	Проведення аналізу наступних налаштувань: - політики облікових записів (політики паролів та політики блокування облікового запису); - локальної політики (політики аудиту, параметрів призначення прав користувачам, параметрів безпеки, журналу подій, системних служб); - адміністративних шаблонів.			
8.3	Порядок безпечної експлуатації засобів обчислювальної техніки та програмного забезпечення.			
9.	Система контролю і управління доступом			
9.1	Питання, що вивчаються: - фізична охорона; - контрольно-пропускний режим; засоби ідентифікації; - охоронна сигналізація; - внесення/винесення матеріальних цінностей; - контроль доступу до приміщень. - відеоспостереження.			
10.	Аналіз функціональних обов’язків та роботи служби захисту інформації			
10.1	Аналіз обов’язків, характеристика ступеня інтегрованості у Процеси Об’єкта, порядку здійснення діяльності.			
12.	Моделювання дій внутрішнього зловмисника (інсайдера).			
12.1	Сканування технічних вразливостей.		Перелік виявлених вразливостей; рекомендації по їх усуненню.	
12.2	Перевірка можливості експлуатації вразливостей.		Факти підтвердження можливості експлуатації вразливостей (відео, знімки екрану).	
12.3	Перевірка можливості реалізації мережевих атак, спрямованих на порушення конфіденційності		Приклади реалізації атак (відео, знімки	

	інформаційних потоків, отримання несанкціоновано доступу до елементів ІТС та порушення штатного режиму функціонування систем.		екрану).	
13.	Моделювання дій зловмисника, спрямованих на елементи ІТС Об'єкта з мережі Інтернет.			
13.1	Сканування технічних вразливостей.		Перелік виявлених вразливостей; рекомендації по їх усуненню.	
13.2	Перевірка можливості експлуатації вразливостей.		Факти підтвердження можливості експлуатації вразливостей (відео, знімки екрану).	
14.	Оформлення висновків та рекомендацій			