CERT-UA

Лист та методика (приклад)

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

Прим. №__

Віце-прем’єр-міністру України,
Міністру регіонального розвитку,
будівництва та житлово-комунального
господарства

Зубко Г. Г.

вул. Велика Житомирська, 9, м. Київ ,
01601

Щодо проведення оцінки стану захищеності

Шановний Геннадію Григоровичу!

Згідно з Порядком оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженим наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України (далі - Держспецзв’язку) від 02.12.2014 № 660 та зареєстрованим в Міністерстві юстиції України від 28.01.2015 № 90/26535 Держспецзв’язку планує розпочати оцінку стану захищеності в інформаційно-телекомунікаційних системах Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України з 04.02.2016.

Проведення вказаних робіт планується здійснювати відповідно до загальної програми і методики, яка додається.

Прошу Вашого сприяння у проведенні зазначених робіт.

Додатки: 1. Загальна програма і методика оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України, на 4 арк., прим. № 1.
2. Перелік комп’ютерного обладнання, яке використовується для проведення робіт, на 1 арк., прим. № 1.
3. Перелік спеціалізованого програмного забезпечення, яке використовується для проведення робіт, на 1 арк., прим. № 1.

З повагою

Голова Служби Л.О. Євдоченко

вик. О.І. Міснік, тел. 2818825

Прим. №___

Перелік комп’ютерного обладнання, яке використовується
для проведення робіт

№ з/п	Найменування обладнання	Серійний номер
1	Мобільний АРМ HP ProBook 4540s	2CE234OVK2
2	Мобільний АРМ Lenovo G50	PF07H54A
3	Мобільний АРМ Lenovo G505S	CB26878406
4	Мобільний АРМ HP Compaq 6735s	CNU9170QWR
5	Мобільний АРМ HP ProBook 4540s	2CE234ORGP

Прим. №__

Перелік спеціалізованого програмного забезпечення, яке використовується для проведення робіт

№ з/п	Найменування СПЗ	Призначення
1	Nessus	Сканер вразливостей
2	OpenVas	
3	Ethereal	Програмне забезпечення аналізу IP-пакетів
4	Wireshark	
5	Dsniff	Програмне забезпечення аналізу та генерації IP-пакетів
6	Ettercap	
7	Nmap	Сканер портів
8	Cain & Abel	Програмне забезпечення аналізу та генерації IP-пакетів
9	Lantricks	Набір утиліт для визначення технічних засобів в мережі та відкритих мережевих портів
10	WiFi Hopper	Програмне забезпечення для роботи з Wi-Fi мережами
11	NetStumbler	
12	MetaGeek inSSIDer	
13	WirelessMon	
14	CommView for WiFi	Програмне забезпечення аналізу IP-пакетів (Wi-Fi)
15	Kismet	
16	OmniPeek Portable Network Analyzer	Програмне забезпечення для аналізу Wi-Fi мереж
17	Airsnort	Відтворення інформаційного наповнення пакетів
18	Airsnarf	
19	Aircrack-ng	
20	LookatLan	Сканер мережі
21	gsecdump	Програмне забезпечення для аналізу хешей паролів
22	Vega	Web сканер
23	Sipt	Пошук Sql injection
24	Havij	
25	Metasploit framework	Програмне забезпечення для перевірки можливості реалізації вразливостей

Прим. №___

ЗАТВЕРДЖУЮ
Голова Державної служби
спеціального зв'язку та
захисту інформації України

Л.О. Євдоченко

___.___.2016

ЗАГАЛЬНА ПРОГРАМА І МЕТОДИКА
оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України

І. Загальні положення

1.1. Загальна програма і методика оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України (далі – загальна програма і методика) розроблена відповідно до пункту 9 Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 02.12.2014 № 660, зареєстрованого в Міністерстві юстиції України 28.01.2015 № 90/26535 (далі – Порядок).

1.2. Цей документ визначає загальні етапи та методичні засади проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі – ІТС) Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України (далі – суб'єкт оцінки).

1.3. Терміни у цьому документі вживаються у такому значенні:

спеціалізоване програмне забезпечення – програмне забезпечення, що використовується для проведення оцінки стану захищеності державних інформаційних ресурсів в ІТС;

сканування – процес аналізу встановленого в ІТС програмного забезпечення із застосуванням спеціалізованого програмного забезпечення з метою виявлення ознак реалізованих технічних рішень, що можуть призвести до виникнення загроз інформації, яка зберігається та/або циркулює в цій системі.

Інші терміни вживаються у значеннях, наведених у Законах України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Державну службу спеціального зв'язку та захисту інформації України», Порядку, ДСТУ 3396.2-97, НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації у комп'ютерних системах від несанкціонованого доступу».

1.4. Вимоги цього документа є обов'язковими для комісій, що створюються Держспецзв'язку відповідно до Порядку (далі – комісія), з метою проведення оцінки стану захищеності державних інформаційних ресурсів в ІТС суб'єкту оцінки.

1.5. Заходи, визначені цим документом, повинні здійснюватися з дотриманням вимог щодо конфіденційності, цілісності та доступності інформації, яка зберігається та/або циркулює в ІТС суб'єкту оцінки.

II. Загальна програма оцінки стану захищеності державних інформаційних ресурсів в ІТС.

2.1. Перелік етапів оцінки стану захищеності державних інформаційних ресурсів в Міністерстві регіонального розвитку, будівництва та житлово-комунального господарства України наведено в таблиці 1.

Таблиця 1

Перелік етапів оцінки стану захищеності державних інформаційних ресурсів в ІТС Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України.

№ пункту.	Назва заходу	Термін виконання
2.1.1	Ознайомлення зі схемами фізичної комутації, схемами адресації та маршрутизації в ІТС. Визначення встановленого режиму доступу до інформації, яка зберігається та/або циркулює в ІТС. Заповнення переліку питань про ІТС відповідальним за інформаційну безпеку об'єкту оцінки та подання його комісії.	04.02.2016
2.1.2	Визначення існуючого в ІТС порядку використання облікових записів та паролів користувачів, а також аналіз реалізованих правил розмежування доступу в операційних системах (далі – ОС) мережевого, серверного обладнання, засобів захисту та АРМ в ІТС.	08.02.2016
2.1.3	Визначення наявних в ІТС мережевих адрес, типів протоколів обміну даними, що в ній обробляються. Встановлення сенсору системи IP Guard.	22.02.2016
2.1.4	Сканування активного мережевого, серверного обладнання, засобів захисту та АРМ в ІТС.	29.02.2016
2.1.5	Визначення порядку та повноти фіксації інформації про системні події в ІТС.	14.03.2016
2.1.6	Складання акта оцінки стану захищеності державних інформаційних ресурсів в ІТС.	21.03.2016

2.2. Залежно від режиму доступу до інформації чи інших обставин, комісією може бути прийнято рішення про іншу послідовність та/або зменшення обсягів проведення оцінки стану захищеності державних інформаційних ресурсів в ІТС суб'єкту оцінки з обов'язковим зазначенням про це в акті, форма якого наведена у Порядку.

III. Методика оцінки стану захищеності державних інформаційних ресурсів в ІТС.

3.1. Заходи, визначені у підпункті 2.1.1, здійснюються з метою прийняття рішення про обсяги оцінки стану захищеності та порядку застосування при цьому програмно-технічних засобів шляхом ознайомлення, за наявності, з внутрішніми наказами та нормативними документами, що стосуються функціонування ІТС, а також з існуючою проектною та експлуатаційною документацією на ІТС (схеми фізичної комутації, схеми адресації та маршрутизації).

Після визначення встановленого у суб'єкта оцінки режиму доступу до інформації, що зберігається та/або циркулює в ІТС, комісією приймається рішення щодо порядку застосування програмно-технічних засобів для проведення подальших заходів з оцінки стану захищеності державних інформаційних ресурсів в ІТС суб'єкту оцінки.

3.2. Заходи, визначені у підпункті 2.1.2, здійснюються шляхом пошуку облікових записів за умовчанням, а також правил, наявність яких може призвести до виникнення загроз інформації, що зберігається та/або циркулює в ІТС.

Перевірка наявності облікових записів за умовчанням проводиться шляхом спроб отримання доступу до інформаційних ресурсів обладнання з використанням даних, які відповідно до інформації виробників операційних систем активного мережевого, серверного обладнання, засобів захисту та АРМ використовуються при інсталяції вказаних операційних систем за умовчанням.

Здійснюється аналіз на наявність некоректних з боку інформаційної безпеки (надлишкових, за умовчанням тощо) правил розмежування доступу до мережевих та/або локальних інформаційних ресурсів в ОС активного мережевого, серверного обладнання, засобів захисту та АРМ в ІТС.

Результатами проведення заходів підпункту 2.1.2 є перелік налаштувань облікових записів, правил розмежування доступу та паролів користувачів в ОС активного мережевого, серверного обладнання, засобів захисту та АРМ в ІТС, використання яких може призвести до виникнення загроз інформації, що зберігається та/або циркулює в ІТС.

3.3. Заходи, визначені у підпункті 2.1.3, здійснюються за допомогою спеціалізованого програмного забезпечення.

Результатом проведення таких заходів є встановлення наявних в ІТС мережевих адрес, типів даних, що в ній обробляються, а також виявлення сторонніх (не документованих) протоколів тощо, наявність яких може призвести до виникнення загроз інформації, що зберігається та/або циркулює в ІТС.

Визначається перелік обладнання, що підлягає скануванню.

3.4. Заходи, визначені у підпункті 2.1.4, здійснюються за допомогою спеціалізованого програмного забезпечення. Рішення щодо можливості проведення вказаних заходів приймається з урахуванням режиму доступу до інформації в ІТС, а також за результатами аналізу документів, що стосуються функціонування ІТС.

Сканування здійснюється шляхом прямого та/або віддаленого підключення до ІТС суб'єкту оцінки.

За результатами аналізу звітів спеціалізованого програмного забезпечення формується перелік вразливостей ОС та програмного забезпечення активного мережевого, серверного обладнання, засобів захисту та АРМ, наявність яких може призвести до виникнення загроз інформації, що зберігається та/або циркулює в ІТС.

Визначається перелік мережевого, серверного обладнання, засобів захисту та АРМ в ІТС, з яких необхідно отримати файли журналів системних подій.

3.5. Заходи, визначені у підпункті 2.1.5, здійснюються з метою визначення наявності та повноти фіксації інформації про:

реалізацію механізмів (використані технології) контролю функціонування мережевого, серверного обладнання, засобів захисту та АРМ в ІТС;

додаткові відомості стосовно подій, що можуть мати відношення до захисту інформації, а саме про: невдалі спроби авторизації та аутентифікації суб'єктів інформаційного обміну; повідомлення від процесів, що забезпечують інформаційний обмін та захист інформації; будь-які інші повідомлення стосовно аномальності параметрів інформаційного обміну.

Результатом аналізу є перелік системних подій, що не фіксуються у файлах журналів системних подій і це може призвести до виникнення загроз інформації, яка зберігається та/або циркулює в ІТС.

3.6. За результатами оцінки стану захищеності складається акт, форма якого наведена у Порядку.

В.о. начальника ДЦКЗ Держспецзв'язку В.В. Лещук
__.___.2016