Ось декілька найвідоміших кібератак :

Хакерське угрупування Fin7 складу якого входили і українці . Це група людей що працюють злагоджено та вкрали приблизно 15 млн. банківських номерів та мають прибуток приблизно 50 млн. доларів в місяць . Вони розробляли шкідливі програмні засоби , крали банківські номери із баз даних ресторанів та магазинів і використовували методику фішингу .

Вірус Petya який наробив галасу в 2017 році . Він вразив багато банків , державних та комерційних підприємств . Цей вірус блокує доступ до жорсткого диску , та виводить повідомлення про вимагання викупу для розшифрування файлів комп'ютера .

Вірус WannaCry атакували комерційні та урядові установи 12 травня 2017 року . Також цього нападу зазнав увесь світ. Цей вірус шифрує файли а потім виводить повідомлення про ціну за яку ці файли будуть розшифровані , але у випадку якщо ви не заплатите протягом 7 днів, вірус знищить файли.

Anonimus – це сучасна міжнародна спільнота активістів у яких немає лідера . Вони виступають проти цензури , переслідування і нагляду . В знак протесту вони зламали багато державних веб-сайтів та великі організації з безпеки . В 2012 році Anonimus провела найбільшу DDoS-атаку в історії з застосуванням LIOC. Під час цієї атаки було виведено з ладу сайти ФБР , Білого дому, Американського управління авторського права , Міністерства юстиції , Universal Music Group , Американської асоціації звукозаписних компаній, Американської асоціації кінокомпаній.

Комп'ютерний черв'як Stuxnet що виводить з ладу комп'ютери під управлінням операційної системи Microsoft Windows , у 2012 році вивів з ладу іранські центрифуги . Він фізично руйнує інфраструктуру та може використовуватись для шпіонажу та збирання даних.

BlackEnergy3 –троянська програма через яку було вимкнено близько30 підстанцій та близько 230 тисяч мешканців на 6 годин залишились без світла. Зараження системи відбувається через вразливі документи Microsoft Office . Атак в Україні зазнали : «Прикарпаттяобленерго» , «Чернівціобленерго» та «Київобленерго».

Угруповання Fancy Bear , що спеціалізуються на кібершпигунстві відоме атаками на інформаційні системи урядових , військових , безпекових організацій . Це угрупування відносять до типу розвиненої сталої загрози . Також це угрупування відоме як Pawn Storm , Sofacy Group , APT28 , Sednit. Воно створювало фальшиві сервери, підроблені під корпоративні сервери жертв з метою викрадення їхніх облікових даних .

Зрозуміло що ми не можемо захиститися від усіх кібератак , але кожен з нас може не дозволити собі стати жертвою кіберзлочину . Для цього потрібно слідувати таким порадам : не слід надавати комусь персональні дані, паролі і коди-підтвердження з смс для операцій з картками; не довіряти повідомленням про виграші в лотереях; перевіряти інформацію за офіційним номером банку; не скачувати в інтернеті сумнівні файли; користуватись ліцензійним програмним забезпеченням; не переходити через підозрілі посилання на інші сайти; користуватися антивірусними програмами та використовувати тільки захищені мережі; створювати надійні паролі та періодично їх змінювати і використовувати інструменти конфіденційності браузерів. Сумнівний номер телефону чи картки можна перевірити на сайті кіберполіції, а також звернутися до спеціалістів із запитом .

Отже , в наш час існує дуже багато загроз нашим даним . Нажаль не всі слідують тим правилам безпеки в інформаційному просторі і тим самим наражають себе на небезпеку . Дуже важливо розвивати наші знання у сфері кібербезпеки .

Список використаних джерел

1. Екскурсія за лаштунки кіберзлочинності [Електронний ресурс]. Режим доступу: https://www.bbc.com/ukrainian/features-39091289

2. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби [Електронний ресурс]. Режим доступу: https://www.gurt.org.ua/articles/34602/

Поняття та зміст кіберзлочинності [Електронний ресурс]. Режим доступу: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/

УДК 004.056.5

КРИТЕРІЇ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Коротка Г.М., студентка гр. КБ - 161

Усов Я.Ю., викладач кафедри кібербезпеки та математичного моделювання

Чернігівський національний технологічний університет

Сучасна людина занурена в інформаційне середовище, адже глобальний процес інформатизації суспільства охопив практично всі країни світу і нині є головним чинником науково-технічного і соціально-економічного розвитку. Інформаційне середовище – сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також соціально-економічних і культурних умов реалізації процесів інформатизації. У зв'язку впровадженням інформаційних систем у фінансові, юридичні, промислові, торгові й соціальні галузі швидко зріс інтерес до проблем збереження й захисту інформації.

Для запобігання загроз інформаційній безпеці створюються комплекси засобів захисту інформаційного середовища. Комплекс засобів захисту інформації — це сукупність програмно-апаратних

засобів, що забезпечують реалізацію політики безпеки інформації. Для оцінки функціональних можливостей використовуваних засобів захисту існують певні вимоги, критерії, які визначені відповідним нормативним документом, що надає нормативно-методологічну базу під час розроблення комплексів засобів захисту від несанкціонованого доступу до конфіденційної інформації, яка обробляється в інформаційному середовищі та проведення аналізу та оцінки захищеності інформації від несанкціонованого доступу в середовищі.

Одним з критеріїв захищеності інформації, яка обробляється та зберігається в інформаційному середовищі є забезпечення конфіденційності.. Критерій конфіденційності реалізується наступними заходами:

1) використання довірчої конфіденційності для розподілу доступу користувачів до захищених об'єктів і дає можливість їм керувати обігом інформації в інформаційному середовищі від захищених об'єктів, що належать їх домену, до інших користувачів;

2) надання адміністративної конфіденційності для надання можливості адміністратору системи безпеки керувати рухом інформації від захищених об'єктів в інформаційному середовищі до користувачів;

3) забезпечення правильного повторного використання об’єктів, які містять інформацію, з обмеженим доступом і ресурси яких поділяються між користувачами інформаційного середовища та прикладними процесами, не вміщаючи інформацію, що використовувалась попереднім користувачем або процесом;

Наступним критерієм захищеності інформаційного середовища є цілісність. Він визначає можливості інформаційного середовища по забезпеченню цілісності оброблюваної інформації, що зберігається в ньому. Критерій цілісності передбачає виконання таких вимог:

1) застосування довірчої цілісності з метою захисту інформації, що обробляється, від недозволеної модифікації і керування користувачем обігом інформації в інформаційному середовищі між користувачами та захищеними об’єктами;

2) реалізація адміністративної цілісності для забезпечення захисту оброблюваної інформації від неправомірної модифікації і надання можливості адміністратору захисту керувати потоками інформації між користувачами та захищеними об'єктами;

3) забезпечення можливості відкату для можливості відміни послідовності дій й повернення об'єкта, з яким працював користувач, до попереднього стану;

4) наявність цілісності при обміні, щоб забезпечити захист від несанкціонованої модифікації об'єктів при їх переміщенні через незахищене інформаційне середовище.

Критерій доступності регламентує роботу засобів, що забезпечують доступність інформаційного середовища в цілому, окремих його функцій або його ресурсів на певному інтервалі часу для авторизованих користувачів, а також гарантувати функціонування КС у разі відмови її окремих компонентів. Як заходи забезпечення доступності розглядаються контроль по використанню ресурсів системи, забезпечення стійкості системи до відмов і відновлення системи в умовах виходу з ладу її компонентів. При забезпеченні доступності інформаційного середовища мають бути реалізовані наступні політики:

1) політика використання ресурсів для взаємодії інформаційних об’єктів, що обробляються в інформаційному середовищі, передбачаючи можливість встановлення обмежень на їх використання користувачами всіх категорій;

2) політика стійкості до відмов, що гарантує працездатність і доступність ресурсів інформаційного середовища при виході з ладу окремих компонентів;

3) політика відновлень після збоїв, що дозволяє повернути інформаційну систему в безпечний стан після відмов або збоїв обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення, іншими непередбачуваними ситуаціями.

Критерій аудиту дозволяє контролює роботу засобів, що дозволяють встановити відповідальність користувачів за небезпечні для інформаційного середовища дії шляхом реєстрації та аналізу подій, що мають відношення до безпеки інформаційного середовища. Даний критерій забезпечується наступними засобами:

1) ідентифікація й аутентифікація для визначення і перевірки особистості користувача, який намагається одержати доступ до інформаційного середовища;

2) достовірний канал, який гарантує взаємодію користувача з компонентами системного та функціонального, що використовуються для здійснення механізмів захисту середовища;

3) цілісність комплексу захисту середовища для визначення міри здатності комплексу засобів захисту захищати себе і гарантувати свою спроможність керувати захищеними об’єктами;

4) самотестування, що дозволяє перевірити комплекс засобів захисту і гарантувати коректність функціонування і цілісність певної сукупності функцій інформаційного середовища;

5) розподіл обов’язків для розмежування доступу користувачів, залежно від їх ролі, з метою уникнення потенційних збитків від навмисних або помилкових дій користувачів й обмеження доступу до конфіденційної інформації;

6) ідентифікація і аутентифікація при обміні для забезпечення взаємної достовірності між двома

Таким чином, ми проаналізували критерії захищеності інформаційного середовища, а саме:

- критерій захисту конфіденційності інформації;
- критерій збереження цілісності інформації;
- критерій збереження працездатності інформаційного середовища;
- критерій аудиту інформаційного середовища.

Експертна комісія, яка перевіряє рівень захищеності інформаційного середовища, визначає кількість і рівень реалізованих в інформаційній системі послуг безпеки і ступінь дотримання вимог перерахованих вище критеріїв.

Список використаних джерел

1. Нормативний документ системи технічного захисту інформації [Електронний ресурс] // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 2002. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=81E66103A1845B5D12126F231FEBBD7D?showHidden=1&art_id=101885&cat_id=89734&ctime=1344501165427.

2. КЗЗ від НСД [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/term/34530.

3. Побудова раціонального захисту інформаційних ресурсів [Електронний ресурс] – Режим доступу до ресурсу: https://helpiks.org/6-9510.html.

УДК 004.056.5

АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Мальцева М.В., студ.гр. КБ-161,
Усов Я.Ю., викладач
Чернігівський національний технологічний університет

Для розвитку людського суспільства необхідні матеріальні, інструментальні, енергетичні та інші ресурси, в тому числі і інформаційні. Теперішній час характеризується небувалим зростанням обсягу інформаційних потоків. Це відноситься практично до будь-якій сфері діяльності людини.Інформація являє собою один з основних, вирішальних факторів, який визначає розвиток технології і ресурсів в цілому. Досліджування, що присвячені проблемі інформаційного суспільства та процесам інформатизації широко використовується поняття інформаційне середовище. Існує декілька визначень інформаційного середовища, а саме: інформаційне середовище — це світ інформації навколо людини і світ її інформаційної діяльності.Інформаційне середовище — це сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також політичні, економічні і культурні умови реалізації процесів інформатизації. [1]. Однією з основних властивостей інформаційного середовища є, на думку І.А. Носкова, його відкритість [2, с.34]. Основними рівнями інформаційного середовища є глобальний, міжнародний, загальнодержавний, регіональний, локальний. Основною властивістю інформаційного середовища є наповнюваність інформацією, її зберігання триглавий час, варіативність та спрямованість. Тому важлива безпека інформаційного середовища та забезпечення цілісності, повноти, доступності та конфіденційності інформації яка в ній поширюється. Перед тим як аналізувати основні підходи розглянемо основні етапи захисту інформаційного середовища. По-перше, необхідно віднести секретну інформацію до категорії обмеженого доступу, по-друге, прогнозувати і своєчасно виявляти загрози безпеки інформаційних ресурсів, причин, умов, що сприяють нанесенню фінансового, матеріального збитку, порушення нормального функціонування і розвитку. Також необхідним є створення механізму і умов оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних, технічних заходів, а також інших засобів забезпечення безпеки. Важливим є створення умов максимального можливого відшкодування та локації збитку, що наноситься неправомірним діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей. Перед будуванням моделі захисту інформаційного середовища розглядується наступні фактори: загрози інформаційної безпеки, які характеризуються ймовірністю виникнення і реалізації; уразливості інформаційного середовища та ризики. Після побудови моделі відбувається безпосередньо етап захисту інформаційного середовища.

До основних підходів можна віднести: програмний, апаратний, апаратно-програмний, правовий. Також для більш повної захищеності інформаційного середовища слід використати організаційний, криптографічний, інженерний та технічний захист.

Програмний захист – комплекс спеціальних програм програмного забезпечення, які реалізують захист інформації. Захисний програмний код може виступати в якості як окремо, в якості захисного програмного продукту (антивірус, міжмережевий екран як приклад), так и входити до складу інших, багатофункціональних програм, з метою захисту інформаційного середовища. При використані програмного захисту захищається лише інформація, а отже використанні лише цього способу недостатньо для повного захисту інформаційного середовища [3].