Використання можливих методів тестування та діагностики мереж, дозволить своєчасно виявити та виправити якомога швидше підвищити ефективність та збільшити експлуатаційних термін мережі.

Для побудови моделі забезпечення стійкості компютерної мережі було обрано найбільш відомий та використовуваний метод тестування мережі - метод тестування навантаження.

Даний тип тестування дозволить в повній мірі оцінити поведінку системи при зростаючому навантаженні. Його ціль – визначення максимального навантаження, яке може витримати система. За навантаження може сприйматися як кількість користувачів, так і кількість операцій.

Отже, було проаналізовано та виділено основні проблеми надійності та відмовостійкості комп'ютерних мереж. Цілі стійкості комп'ютерної мережі можна розділити на три категорії: запобігання, виявлення та реагування. Виявлення вторгнень відіграє критичну роль в безпеці більшості систем, так як методи встановлення паролів та контроль доступу часто можуть бути скомпроментовані. Тож при управлінні мережею необхідно включати додаткові механізми виявлення вторгнень. Не менш важливим є і аналіз виявлених вторгнень, що дозволить скорегувати або заблокувати загрозу. Та реагування, що дозволить залишити мережу доступною. До того ж розглянуто класифікацію методів тестування мережі та обрано найоптимальніший – метод тестування навантаження. Отримані дані будуть використані в подальших дослідженнях у цьому напрямку для розробки моделі забезпечення стійкості комп'ютерних мереж.

Список використаних джерел

1. Muriel Médard, Steven S. Lumetta. Network Reliability and Fault Tolerance March 2003 [Электронный ресурс] / Muriel Médard, Steven S. Lumetta - Режим доступу до ресурсу: https://www.researchgate.net/publication/2884965_Network_Reliability_and_Fault_Tolerance.
2. Paul Rubens. Understanding Fault Tolerance: Securing Your System [Электронный ресурс] / Paul Rubens - Режим доступу до ресурсу: https://www.enterprisestorageforum.com/storage-management/fault-tolerance.html.
3. Нагрузочной тестирование [Электронный ресурс] - Режим доступа до ресурсу: https://www.performance-lab.ru/blog/load-testing/testirovanie-proizvoditelnosti.
4. В. Олифер. "Компьютерные сети. Принципы, технологии, протоколы. Учебник" / В. Олифер, Н. Олифер., 2016. - (5).
5. А. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. КОМП'ЮТЕРНІ МЕРЕЖІ / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. - Львів: Магнолія 2006, 2013 - 253 с.

УДК 004.056

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ

Тимошенко Є. М., студ. гр. КБ-161
Науковий керівник: **Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

Цінність інформації можуть визначити лише і виключно суб'єкти захисту інформації люди та/або соціальні групи. Більш того: саме поняття цінності інформації носить суб'єктивний характер: різні люди (соціальні групи) цілком можуть надати різну цінність для однієї й тієї ж самої інформації. Крім того, цінність інформації є різною для різної діяльності людини та/або соціальної групи. Таким чином, і тут наявність моделі для опису діяльності людини та соціальної групи є фактором, який здатний підвищити захищеність інформації.

Наведемо аналіз основних існуючих формальних моделей інформаційної безпеки. Розглянуто лише ті складові моделей та методів, які описують суб'єктну складову, так як саме врахування «не ідеальності» суб'єктів та суб'єкт-суб'єктних відношень є сьогодні одним із головних джерел зниження рівня захищеності людини та соціальної групи.

Моделі забезпечення конфіденційності.

Модель Харрісона-Руззо-Ульмана (модель дискреційного керування (розмежування) доступом).

Головною особливістю якої є матриця з повним описом призначених для користувача прав до файлів. Зміни в цю матрицю вводяться за допомогою спеціальних команд. Основним завданням будь-якої моделі управління доступом є обмеження на обробку операцій, які дозволено проводити суб'єкту (користувачеві) над об'єктом. Такими операціями можуть бути, наприклад, читання (потік інформації від об'єкта до суб'єкта) і запис (потік інформації від суб'єкта до об'єкта). Для цього вводяться такі позначення S – множина суб’єктів, O – множина об’єктів, R – множина прав доступу. Для реалізації цих прав в даній моделі використовується матриця доступів M, рядки якої відповідають суб'єктам, а стовпці - об'єктам. На перетині рядків і стовпців вказані права доступу, якими володіє даний суб'єкт по відношенню до даного об'єкту.

Мандатна модель керування доступом Белла-ЛаПадули.

Ця система складається з допустимих наборів станів в яких знаходиться система елементами якої є суб’єкти та об’єкти. Об’єкти мають показники рівнів таємності, а суб’єкти рівні доступу, які дорівнюють рівню конфіденційності. Ця система захищена в тому випадку, коли кожен із станів системи відповідає політиці безпеки, даної інформаційної системи. Перехід між станами системи описується функцією переходу. А стан захищеності це тоді, коли суб’єкт має наявний доступ тільки до тих об’єктів, до яких дозволено на основі політики безпеки. Перед тим, як надати суб’єкту доступ до об’єкту у суб’єкта порівнюється рівень доступу та рівень таємності і тільки у тому випадку коли рівні співпадають суб’єкт отримає доступ до об’єкту. Все це описується в матриці доступу.

Моделі забезпечення цілісності.

Модель цілісності Кларка-Вільсона.

В основі моделі лежить поняття відносини між автентичним принципалом (тобто користувачем) і набором програм (тобто, ТПС), які працюють на безлічі елементів даних (наприклад, удіни і копра). Компоненти такого співвідношення, взяті разом, називають Кларка-Вілсона в три рази. Модель повинна також гарантувати, що різні органи несуть відповідальність за маніпулювання відносини між принципалами, транзакціями і елементами даних. Як короткого прикладу, користувач здатний сертифікації або створити відношення не має бути в змозі виконати програми, задані в цьому відношенні.

Модель забезпечення доступності.

Модель розподілення ресурсів Міллена.

Модель Міллена включає в себе цілком відповідний стратегії відмови в обслуговуванні набір правил, що характеризують сімейство обчислювальних систем, тобто ці правила побудовані таким чином, щоб включити в це сімейство поняття, які багато в чому допомогли б при описі і аналізі стратегій відмови в обслуговуванні.

В ході дослідження існуючих методів протидії інформаційно психологічним впливу, я пропоную переглянути суб’єкта не тільки як частину інформаційних відносин зі суб’єктами, але і як окрему особу та соціальну групу. З цього слідує, що потрібно звертатися до таких наук як психологія, соціологія та менеджмент, які дозволяють більш широко підкреслити потреби та важіль впливу на людину чи соціальну групу.

Для цього можна використати такі методі та теорії:

Менеджмент: змістовні теорії мотивації (ієрархія потреб Маслоу, теорія потреб МакКлеланда. двофакторна теорія Герцберга), процесуальні теорії мотивації (теорії X та Y МакГрегора, теорія очікувань Врума, модель Портера-Лоутера), стилі лідерства (стилі лідерства Льовіна, стилі лідерства Лейкарта), теорія конфлікту;

Соціологія: соціометрика Морено, соціальна психологія та соціальні технології;

Психологія: типологія Кречмера, типологія Шелдона, типологія Юнга, типологія Майєр-Бріггс, типологія Кеттела, типологія Айзенка.

Для виявлення методики оцінки протидії інформаційно психологічним впливам я пропоную використати метод експертних оцінок за допомогою критеріїв, які випливають з

ходу дослідження існуючих методів протидії інформаційно-психологічним впливам їх плюсів та мінусів в певних ситуаціях.

Також не слід забувати про забезпечення протидії інформаційно-психологічним впливам зі сторони особи, суспільства та держави. Я розглядаю в своїй роботі інформаційну політику різних країн в даному питанні. Та ще канали впливу на людину, суспільство такі як засоби масової інформації (телеканали, газети журнали). Інтернет ще один не менш важливий канал інформаційного впливу (соціальні мережі, месенджери, інформаційні портали та багато інших варіантів через яких можливо впливати на людину).

Висновок: данні моделі протидії інформаційно-психологічним впливам є основні та найпоширеніші у світі. Нажаль в сучасних моделях та методах захисту інформації суб'єктна компонента представлена явно в недостатньому обсязі. Разом із тим, її вплив на забезпечення інформаційно-психологічного захисту стрімко зростає із часом проаналізовано широкий спектр існуючих моделей та методів забезпечення захисту людини або соціальної групи від негативного інформаційного та інформаційно-психологічного впливу. Зокрема підкреслюється, що мотиваційні фактори мають високий рівень важливості. Сьогодні існуючі канали впливу на людину активно формують її емоційне сприйняття інформації. Внаслідок цього вже на рівні сприйняття інформації певні факти будуть нею відкинуті, а певні факти різко змінять свій реальний пріоритет. Сьогодні негативний інформаційно-психологічний вплив на людину здійснюється переважно не через канали її особистого спілкування, як це було раніше, а через інтелектуальні інформаційні системи (наприклад, пошукові сервери, які підстроюються під конкретну людину - і, тим самим, змінюють пріоритетність інформації). Широко застосовується використання каналів ЗМІ (особливо це небезпечно для України, в якій переважна більшість телеканалів належить певним олігархічним угрупуванням), Інтернет (де власники веб-ресурсів не несуть практично ніякої відповідальності за контент), різноманітні гаджети мобільних пристроїв, кількість яких стрімко зростає (наприклад, сьогодні гаджети активно формують у населення емоційне ставлення до ряду понять та факторів соціального життя, - більш того, різномовні варіанти одного й того ж гаджету можуть формувати протилежні емоційні оцінки у користувачів), тощо. Сформоване таким чином емоційне прийняття або неприйняття певних факторів соціального життя суттєво впливає на результати діяльності людини та соціальної групи.

Список використаних джерел

1. Модель Харрисона-Руззо-Ульмана [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Модель_Харрисона-Руззо-Ульмана

2. Мандатная модель Белла-Лападулы [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/1854771/page:7/

3. Модель Миллена распределения ресурсов (MPP). [Електронний ресурс] – Режим доступу до ресурсу: https://studopedia.org/1-29163.html

4. Кларк-Вилсон модель - Clark–Wilson model. [Електронний ресурс] – Режим доступу до ресурсу: https://ru.qwe.wiki/wiki/Clark–Wilson_model