Том 12
Автоматизація та інформаційні технології

УДК 681.3.06

Нікітіна Є.О., студентка гр. УБіт-14-1
Науковий керівник: Тимофєєв Дмитро Сергійович, ст. викладач кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

СОЦІАЛЬНА ІНЖЕНЕРІЯ В СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У роботі розглянуто схеми та методи соціальної інженерії; види шахрайства, основою яких є соціальна інженерія; способи захисту від загроз, основою яких є соціальна інженерія.

Ключові слова – соціальна інженерія, соціальний хакер, соціоінженер, соціотехніка.

ВСТУП

В майбутньому найбільшу загрозу інформаційній безпеці як великих компаній, так і звичайних користувачів, будуть представляти методи соціальної інженерії, що застосовуються для злому існуючих засобів захисту.

Основною причиною цього є те, що застосування соціальної інженерії не вимагає значних фінансових витрат і досконалого знання інформаційних технологій.

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Соціальна інженерія – метод несанкціонованого доступу до інформації або до систем зберігання інформації без використання технічних засобів.

Метод заснований на використанні слабкостей людського фактору. [1]

Дослідження показують, що людям притаманні деякі поведінкові схильності, які можна використати для маніпулювання. Більшість зломів систем безпеки відбуваються завдяки використанню соціальної інженерії, а не електронному злому. [2]

БАЗА ДЛЯ СОЦІАЛЬНИХ ІНЖЕНЕРІВ (СОЦІАЛЬНИХ ХАКЕРІВ)

Першим етапом будь-якої атаки є дослідження. Соціоінженер повинен знати хто з працівників компанії має доступ до інформації, яка його цікавить, хто в якому підрозділі працює, де розташовані підрозділи, яке програмне забезпечення встановлено на корпоративних комп`ютерах і т.д.

Соціальний хакер повинен орієнтуватися в термінології, володіти професійним жаргоном, знати внутрішні порядки компанії-жертви.

Наступним етапом в діяльності соціоінженера є розробка плану атаки.

Найпоширенішими методами атак є:

- отримання, передача або несанкціонована зміна паролів;
- створення облікових записів (з правами користувача або адміністратора);
- запуск шкідливого ПЗ;
- отримання інформації про способи віддаленого доступу до корпоративної інформаційної мережі;
- несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи;
- передача або поширення конфіденційної інформації. [3]

СХЕМА ДІЇ ТА МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Схема дії соціальної інженерії:

- визначення мети впливу на об`єкт;
- збір інформації про об`єкт;

- виявлення найбільш зручної мішені впливу;
- створення необхідних умов для впливу;
- примус до виконання потрібної дії;
- досягнення потрібного результату. [4]

Методи соціальної інженерії

Віртуальні методи

Соціальні хакери, як правило, використовують електронну пошту або спливаючі вікна. У більшості випадків атаки спрямовані на конкретну особу і основною метою їх здійснення є отримання ідентифікаційних даних жертви.

Телефонні технології дають змогу встановити менш масові, але більш особисті контакти з жертвами.

Фізичні методи

Встановлення особистого контакту з жертвою є менш популярним, але ефективнішим способом підготовки до здійснення атаки.

Фізичні методи є більш ризикованими, але вони надають ряд переваг.

Поширення мобільних технологій, які дають змогу користувачам підключатись до корпоративних мереж вдома або в дорозі, є серйозною загрозою для компаній.

Організація безпеки систем співробітників, які працюють вдома, у більшості випадків, обмежується технічними засобами. Політика безпеки повинна вимагати, щоб домашні системи даних працівників були захищені брандмауерами (міжмережевими екранами), які блокуватимуть спроби зловмисників отримати доступ по мережі ззовні. [2]

ВИДИ ШАХРАЙСТВА, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Фішинг – процес відправки електронних або паперових листів, які начебто надходять від достовірного джерела. Мета – отримання конфіденційної інформації адресата.

Фармінг – встановлення на комп`ютери користувачів шкідливих програм, які після запуску збирають дані платіжних сайтів і надсилають їх зловмиснику.

Вішинг – процес отримання інформації за допомогою телефону. Зловмисники використовують phone spoofing, тобто підміну телефонного номеру.

Уособлення – вид шахрайства, у якому соціальний хакер виступає в ролі іншої людини. Його метою є отримання потрібної інформації. [4]

Зворотна соціальна інженерія. Мета соціоінженера – змусити жертву звернутися до нього за «допомогою». Соціальний хакер може використовувати диверсію або рекламу. [1]

ЗАХИСТ ВІД ЗАГРОЗ, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Основним способом захисту від соціальної інженерії є навчання.

Персонал підприємства повинен мати чіткі інструкції щодо спілкування зі сторонніми людьми.

Всім працівникам у день прийому на роботу необхідно повідомити, що видані їм паролі є власністю компанії і їх не можна використовувати у власних цілях.

Повинен існувати алгоритм для встановлення особи відвідувача.

Компанія може витрачати значні кошти на удосконалення технічних засобів забезпечення інформаційної безпеки, але вони будуть марними, якщо персонал буде нехтувати заходами з протидії соціальним хакерам. [1]

ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ ВІД ЗАГРОЗ, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Для створення системи захисту персоналу від загроз, основою яких є соціальна інженерія, потрібно виконати три дії.

I. Розробка стратегії управління процесом забезпечення безпеки. Потрібно визначити завдання захисту від соціотехічних загроз і призначити працівників, відповідальних за їх виконання.

II. Оцінка ризику. Необхідно проаналізувати всі соціотехнічні загрози і визначити ступінь небезпеки.

III. Інтеграція принципів захисту від соціотехнічних атак в політику безпеки. Потрібно розробити та перевірити політики і процедури, які регламентують дії персоналу в ситуаціях, які можуть бути соціотехнічними атаками. [3]

РЕАЛІЗАЦІЯ ЗАХОДІВ ЗАХИСТУ ВІД ЗАГРОЗ, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Для реалізації заходів захисту від загроз, основою яких є соціальна інженерія, використовують інформування та управління інцидентами.

Інформування. Потрібно ознайомити персонал з розробленою політикою безпеки. Для інформування можна обрати структуровані навчальні курси, неформальні зустрічі і т.д.

Управління інцидентами. Працівники служби підтримки повинні знати порядок дій у разі соціотехнічної атаки. Одним з принципів управління інцидентами є те, що у відповідь на атаку проводиться аудит безпеки.

При реєстрації інциденту керівний комітет із забезпечення безпеки повинен з`ясувати представляє він нову загрозу або є зміненою загрозою. Після цього необхідно створити або оновити політики і процедури.

Для управління інцидентами служба підтримки повинна використовувати затверджений протокол, який містить відомості про: жертву атаки; підрозділ жертви; дату атаки; опис атаки; результат атаки; наслідки атаки; рекомендації.

Реєстрація інцидентів дає змогу визначити шаблони атак і покращити захист від майбутніх атак. [5]

ВИСНОВОК

Навіть найбільш надійні технології безпеки малоефективні у боротьбі з хакери, які користуються методами соціальної інженерії. Робота з персоналом та навчання працівників застосуванню політики безпеки і технікам протистояння соціальним хакерам є необхідною складовою комплексної системи безпеки.

Стратегія управління процесом забезпечення безпеки повинна давати загальне уявлення про загрози, основані на соціальній інженерії, яких зазнає компанія, і визначити працівників, які будуть відповідальними за розробку політик і процедур для блокування цих загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Краткое введение в социальную инженерию [Електронний ресурс] – Режим доступу https://habrahabr.ru/post/83415/. Назва з екрана.

2. М. В. Кузнецов, И. В. Симдянов. Социальная инженерия и социальные хакеры. Учебник / М. В. Кузнецов, И. В. Симдянов. - СПб.: БХВ-Петербург, 2007. – 10 с.

3. Социальная инженерия - методы, которыми хакеры пользуются, чтобы обмануть корпоративных пользователей и обойти самые мощные системы информационной безопасности. [Електронний ресурс] – Режим доступу https://www.eos.ru/eos_delopr/eos_delopr_intesting/detail.php?ID=11199. Назва з екрана.

4. Старостина Е., Хрусталева Е. Мишень социальной инженерии – это вы сами. IT Manager, 2015, 142, 64-67.

5. Как защитить внутреннюю сеть и сотрудников компании от атак, основанных на использовании социотехники [Електронний ресурс] – Режим доступк https://technet.microsoft.com/ru-ru/library/cc875841.aspx#EBAA. Назва з екрана.

УДК 32.019.51

Діденко К.О., студентка гр. УБіт-14
Науковий керівник: Мілінчук Ю.А., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ЧОРНИЙ ПІАР ТА ЧОРНА РИТОРИКА В СУЧАСНИХ ВІДНОШЕННЯХ У ПОЛІТИЦІ ТА СЕКТОРІ БЕЗПЕКИ

У PR-програмах і PR-акціях політика формується, як певна послідовність дій, що зумовлює вибір позицій, розробку відповідних стратегій і тактичних кроків. [1] З усіх видів піару, чорний піар є найганебнішим, але найдієвішим, бо охоплює усі «брудні» методи та шляхи досягнення мети (шахрайство, хабар, плітки). Слід зауважити, що в основі піару в сучасних відношеннях у політиці лежить інформаційно-психологічний вплив, спрямований на привернення уваги, зміну ставлення слухачів до цікавої для них інформації. Причому інформація найчастіше носить явно переконливий характер, що позначається на поглядах споживача.

Необізнаність споживачів інформації в сучасних методах ведення боротьби між політиками обумовлює актуальність даної теми.

Чорний PR – це будь-якого виду інформаційні атаки, основне завдання яких:

- ліквідувати бізнес конкуруючої сторони;
- похитнути корпоративні зв'язки;
- зіпсувати імідж конкретної особи.

Метод нападу в чорному PR – ведення інформаційної війни. Жертвами подібних технологій найчастіше стають поважні юридичні, консалтингові та страхові компанії. [2]

Чорна риторика, за словами відомого тренера в області комунікативної техніки Карстена Бредемайєра, – це вміння маніпулювати всіма риторичними засобами і методами для того, щоб в процесі дебатів або промови конкурент або слухачі прийшли до необхідного для вас заключення. [3]

Згідно зі статистикою середній споживач інформації витрачає на перегляд телебачення майже сорок годин, а перебуває в Інтернеті й того довше. Загалом вдосталь цього часу для того, щоб за допомогою звуку й відеофрагментів професіонали у сфері нейролінгвістичного програмування сформували у свідомості частини глядачів і слухачів потрібні замовникам переконання, навіть якщо вони суперечать дійсності. У результаті чого, взагалі, трансформується громадська думка. Це формування протилежного уявлення про дійсність конкуруючої сторони у споживачів інформації за допомогою ЗМІ і є інформаційною війною.

Так, спеціалісти з інформаційних війн розцінюють PR як спеціальний прийом управління інформацією, якщо під управлінням вбачати процес породження інформаційних підстав й інформації стороною, зацікавленою в ній, розповсюдження готової інформаційної продукції засобами комунікації для цілеспрямованого формування бажаної громадської думки. [4]

Чорна риторика та чорний PR є значущими в сучасному суспільстві та секторі безпеки. Так, під час війни на Донбасі, Україна має справу не просто з пропагандою та чорною риторикою, а з тим, що спеціалісти в інформаційній сфері належним чином визначають як «війну сенсів». Для ретрансляції цих сенсів вжито всю безліч каналів донесення інформації. Основним структурним елементом у цій війні стають симулякри – зображення того, чого в дійсності не існує. Прикладом таких симулякрів є: «фашисти», «звірства каральних батальйонів», використання Україною заборонених озброєнь. Стратегічна мета створення та використання цих симулякрів – витісняти

об'єктивне уявлення цільових груп про характер конфлікту «інформаційними фантомами», необхідними противнику. Все це транслюється споживачеві через ЗМІ. Тобто, інформаційні технології, стали, таким собі, транспортним засобом, що доносять політичні ідеї до громадян. В політиці найбільш впливовішими засобами розповсюдження чорного піару та чорної риторики є ток-шоу.

На сьогоднішній день ток-шоу належать до списку найбільш рейтингових передач, тому їх автори виявляють інтерес до збереження аудиторії. Для виконання такої задачі нерідко вживається прийом маніпулятивного впливу на глядацьку аудиторію - «чорна риторика».

Певною мірою, PR - вказана в інформаційних технологіях внутрішня культура сучасних політичних відносин.

Важливим транскордонним простором проведення інформаційного протиборства стала глобальна мережа Internet. Всілякі реальні та віртуальні «хактівісти», «кіберпартизани», «кіберополчення», а також спеціальні підрозділи різних відомчих органів безпеки для ведення ворожнечі в кіберпросторі – всі вони стали значним елементом кібератак, а також ведення спеціальних психологічних операцій в соціальних мережах та мережі Internet загалом.

З усього переліченого випливають такі висновки:

– Чорний PR - це складна наука, що стала невід'ємною частиною сучасної політики;

– в Україні має сенс провести детальне вивчення практики використання «чорних» та маніпулятивних PR-методик і в подальшому розробку дієвих правових і суспільних механізмів протидії застосуванню «брудних» політ-технологій;

– необхідно активізувати роботу діючих національних PR-асоціацій щодо розробки національних професійних стандартів, що базуються на відповідних міжнародних стандартах, а також засад професійної репутації фахівців PR і дієвих санкцій за їх порушення на правовому, громадському та внутрішньо професійному рівнях.

ПЕРЕЛІК ПОСИЛАНЬ

1. Чорний та білий піар, «брудні» технології як механізм масового інформаційно-психологічного впливу. [Електронний ресурс] – Режим доступу: http://pidruchniki.com/1753060737015/politologiya/chorniy_biliy_piar_brudni_tehnologiyi_mehanizmi_masovogo_informatsiyno-psihologichnogo_vplivu#645

2. Чорний піар: типи, методи впливу та нейтралізації наслідків. Методи захисту та нейтралізації наслідків. [Електронний ресурс] – Режим доступу: http://r-morhan.vkursi.com/9258.html

3. К. Бредемайєр «Чорна риторика: Влада та магія слова»/ Альпіна Паблішер. 2017. – 2с.

4. В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева. Сугестивні технології маніпулятивного впливу. Навчальний посібник. 2011. – 132с.

УДК 004.65

Колгін Володимир Андрійович, студент гр. 125м-16-1,
Науковий керівник: Начовний І.І., ст. викладач кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ОБХІД АУТЕНТИФІКАЦІЇ СУБД MARIADB ТА MYSQL ЧЕРЕЗ «CVE-2012-2122»

Ця стаття дає ознайомитися з вразливістю CVE-2012-2122, яка була знайдена в СУБД MariaDB та MySQL, що дозволяє обійти механізм аутентифікації.

Ключові слова – MariaDB, MySQL, memcmp (), glibc, аутентифікація.

ВСТУП

Фахівці з інформаційної безпеки проекту MariaDB надали детальні відомості про серйозну уразливість в популярній СУБД MySQL, а також в СУБД MariaDB, яка ділить з MySQL загальну технологічну базу. В MySQL вразливість отримала номер CVE-2012-2122.

В офіційних заявах розробників спочатку наводилося дуже мало даних про усунення вразливості, що було зроблено навмисно, щоб не провокувати інтерес хакерів. Коли значна частина користувачів MySQL і MariaDB отримали досить часу для обновлення, розробники MariaDB заявили про виявлення в СУБД MySQL досить простий в використання критичної уразливості CVE-2012-2122, що дозволяє обійти авторизацію і отримати доступ до вмісту БД.

ПРИЧИНА ВИНИКНЕННЯ ВРАЗЛИВОСТІ

Вразливим виявився модуль "sql / password.c", в якому для повернення результату порівняння хеш пароля застосовується функція "memcmp ()". Наявність уразливості залежить не тільки від версії СУБД, але і від компілятора, за допомогою якого була проведена збірка. Так, популярні компілятори (gcc і BSD libc) і оригінальні дистрибутиви мають безпечну реалізацію вразливою функції "memcmp ()", що робить систему невразливою для виявленої помилки. У разі, якщо значення, що повертається функцією "memcmp ()" не піддається додатковій перевірці, зловмисникові достатньо здійснити близько 300 спроб авторизації з відомим ім'ям користувача (наприклад, "root") і випадковими значеннями пароля для отримання доступу до СУБД.

Суть в тому, що при підключенні користувача MariaDB / MySQL обчислюється токен (SHA від пароля і хеша), який порівнюється з очікуваним значенням. При цьому функція memcmp () повинна повертати значення в діапазоні -128..127, але на деяких платформах (в glibc в Linux з оптимізацією під SSE) повертаєме значення може випадати з діапазону. У підсумку, в 1 випадку з 256 процедура порівняння хеша з очікуваним значенням завжди повертає значення true, незалежно від хеша. Іншими словами, система вразлива перед випадковим паролем з ймовірністю 1/256. [1]

Проста команда на bash дає зловмисникові рутовий доступ до уразливому сервера MySQL, навіть якщо він не знає пароль.

$ For i in `seq 1 1000`; do mysql -u root --password = bad -h 127.0.0.1 2> / dev / null; done

mysql> [2]

УМОВИ АТАКИ

Уразливість CVE-2012-2122 може бути проексплуатовано тільки в тому випадку, якщо продукт встановлений на системі, яка дозволяє функції memcmp () повертати значення за межами діапазону від -128 до 127. Серед таких систем можна відзначити

Linux платформи, які використовують SSE-оптимізований glibc (бібліотека GNU C). Бінарні версії MySQL, які поширюються виробником, уразливості не схильні. Якщо MySQL працює на системі даного типу, код, який порівнює криптографічний хеш введеного користувачем пароля з хешем, розміщеним в базі даних для конкретної облікового запису, буде здійснювати аутентифікацію навіть в разі надання некоректного пароля. Імовірність спрацьовування даної проломи, якщо продукт відповідає зазначеним вище вимогам, становить 1 до 256. [3]

МОЖЛИВІ ЗБИТКИ

Після успішної експлуатації уразливості модуль копіює таблицю користувачів сервера бази даних, яка містить всі хеші паролів. Зловмисник може згодом зламати хеші паролів і надалі отримувати неавторизований доступ до сервера навіть після усунення вразливості.[3]

ЯК ЗАХИСТИТИСЯ

Уразливими виявилися всі версії MySQL і MariaDB до версії 5.1.61, 5.2.11, 5.3.5, 5.5.22 включно. Перелік операційних систем, на які поширюється дана уразливість:

- Ubuntu Linux 64-бит (10.04, 10.10, 11.04, 11.10, 12.04);
- OpenSuSE 12.1 64-бит MySQL 5.5.23-log;
- Нестабильная ветка Debian 64-бит MySQL 5.5.23-2;
- Fedora;
- Arch Linux.

ВИСНОВКИ

Будьте обачливими, навіть те програмне забезпечення, якому Ви повністю довіряєте, може бути вразливим. Ніколи не довіряйте користувачу, бо він є потенційним зловмисником. Частини програмного забезпечення були самостійними і не вразливими і тільки коли вони об’єдналися з’явилася вразливість. Ці речі неможливо передбачити, але це не означає, що ми не повинні реагувати та вирішувати поставленні перед нами цілі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Стаття: Обхід авторизації (Електрон. ресурс) / Спосіб доступу: URL: http://sitesco.ru/thread-11627.html

2. Стаття: Вразливість MySQL під Ubuntu 64-bit (Електрон. ресурс) / Спосіб доступу: URL: https://rdot.org/forum/archive/index.php/t-2218.html.

3. Доклад: Вразливість MySQL (Електрон. ресурс) / Спосіб доступу: URL: https://www.securitylab.ru/news/425688.php

УДК 65.012.45:658.114

Твердохліб І.С., студент гр. 125м-16-1,
Ковальова Ю.В., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ НА МАЛИХ КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ

Питання забезпечення інформаційної безпеки на малих комерційних підприємствах актуальне в наш час, як ніколи раніше. Відповідно, і питання запобігання появи небажаних або несподіваних подій ІБ, інцидентів, з якими пов'язана значна вірогідність компрометації бізнес-операцій та створення загроз ІБ, теж актуальні. А виходячи з того, що значна частина існуючих організацій та підприємств складають малі приватні підприємства, даний питання стає особливо гострим і важливим, якому необхідно приділити належну увагу.

Малі комерційні підприємства є невід'ємною частиною соціально-економічної країни. По-перше, вони сприяють підтримці стабільності ринкових відносин, оскільки значна частина населення втягується в цю систему відносин

По-друге, вони забезпечують необхідну мобільність виробництва в умовах ринку, поглиблення спеціалізації та широке розвиток кооперації виробництва, без яких немислима його висока ефективність. В підсумку це веде до динамічності господарського розвитку та зростання національній економіки.

По-третє, роль малих підприємств у діяльності крупних та середніх підприємств постійно зростає. Велика значення має здатність малих підприємств розширювати сфери доповнення трудової діяльності, створювати нові можливості не тільки для працевлаштування, а перш за все для підприємницької діяльності населення та використання вільних виробничих можливостей.

Інцидент інформаційної безпеки - один або кілька небажаних або несподіваних подій інформаційної безпеки, які з значною ступенем ймовірності піддають небезпеки ділову діяльність та загрожують інформаційної безпеки

В даній таблиці представлені завдання та засоби їх реалізації, безпосередньо пов'язані з управлінням інцидентами інформаційної безпеки. Основна інформаційна частина взята з міжнародного стандарту ІБ 27001. [таб.1]

Управління ризиками інформаційної безпеки вимагає відповідають оцінки ризиків і методу обробки ризиків, які можуть включати оцінку втрат і вигод, законодавчі вимоги, питання, що викликають заклопотаність зацікавлених осіб та інші відповідні вихідні дані. Оцінка ризиків повинна виявляти, кількісно оцінювати і пріоритезувати ризики відповідно до критеріїв прийнятності ризиків і цілями, істотними для організації.

Ці результати повинні служити орієнтиром і визначати відповідні дії і пріоритети для управління ризиками інформаційної без-пеки і впровадження засобів управління, обраних для захисту від цих ризиків. Оцінка ризиків повинна включати систематичний підхід до оцінки величини ризику (аналіз ризику) і процес порівняння прогнозної оцінки ризику з критеріями для визначення значущості ризиків (визначення ступеня ризику). Оцінка ризиків повинна виконуватися періодично для урахування змін у вимогах інформаційної безпеки і ситуації з ризиками, наприклад, для активів, погроз, вразливостей, впливів, оцінки ступеня ризику, а також коли відбуваються істотні зміни.

В першу чергу, компанія повинна мати чітко визначену політику безпеки, адже без документованих принципів, правил, процедур і багато чого іншого неможливо регулювати інформаційні потоки.

Якщо прислухатися до рекомендацій і порад міжнародних стандартів ІБ, можна значно поліпшити безпеку системи в області управлінні інцидентами інформаційної безпеки.

Таблиця 1.

Завдання	**Засоби реалізації**
Обов'язки та процедури	Повинні бути встановлені обов'язки керівництва та процедури, щоб гарантувати швидкий, результативний і належну відповідь на інциденти інформаційної безпеки.
Оповіщення про події, пов'язані з інформаційною безпекою	Оповіщення про події інформаційної безпеки повинно доводитися по відповідних каналах управління якомога швидше.
Оповіщення про уразливість в інформаційній безпеці	Від співробітників і працюють за контрактом, що використовують інформаційні системи і сервіси організації, необхідно вимагати фіксувати і повідомляти про будь-які виявлені або передбачуваних вразливості в інформаційній безпеці систем і сервісів
Оцінка і рішення щодо подій інформаційної безпеки	Події інформаційної безпеки повинні оцінюватися і потім прийматися рішення, чи слід їх класифікувати як інцидент інформаційної безпеки.
Відповідні заходи на інциденти інформаційної безпеки	Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до документально оформленими методиками.
Лікування уроків з інцидентів інформаційної безпеки	Знання, отримані з аналізу та дозволу інцидентів інформаційної безпеки, повинні використовуватися для зменшення ймовірності інцидентів в майбутньому або їх впливу.
Збір свідчень	Організація повинна визначити і застосовувати процедури для ідентифікації, збору, комплектування і збереження інформації, яка може служити в якості свідчень

Основою для цих рекомендацій служив міжнародний, які більш детально описує не тільки питання в області УІІБ, а й основні правила менеджменту ІБ. Резюмуючи, хочеться сказати про те, що якщо керівництво комерційних підприємств буде приділяти належну увагу питанням УІІБ, то воно може заощадити фінанси, які були б витрачені на виправлення наслідків інцидентів і зберегти чисту репутацію своєї фірми.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls.

УДК 65.011.3

Ігнатьєва І.Д. студентка групи 125м-16-1
Науковий керівник: Галушко С.О., ст. викладач безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

МЕТОДИ АНАЛІЗУ РИЗИКІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Оцінка ризику ІБ є частиною процесу менеджменту ризику і являє собою структурований процес, в рамках якого виявляють способи досягнення поставлених цілей, проводять аналіз наслідків та ймовірності виникнення небезпечних подій для прийняття рішення щодо необхідності обробки ризику. Інакше кажучи, оцінка ризику є процесом, що об'єднує ідентифікацію, аналіз ризику і порівняльну оцінку ризику. Спосіб реалізації цього процесу залежить не тільки від сфери застосування процесу ризик-менеджменту, але також і від методів оцінки ризику. Стандарт ДСТУ IEC/ISO 31010:2013 "Керування ризиком. Методи загального оцінювання ризику" є загальним для всіх областей ризику і призначений для різних цілей організації. Менеджмент ризику допомагає в прийнятті рішень в умовах невизначеності і можливості виникнення подій або обставин (планових і непередбачених), що впливають на досягнення цілей організації.

Стандарт визначає 31 метод аналізу ризиків, з яких і будуть обиратися оптимальні методи для аналізу ризиків інформаційної безпеки. Перерахуємо їх найменування: "Мозкова атака", "Структуроване чи напівструктуроване опитування", "Метод Делфі", "Переліки контрольних запитань", "Попереднє аналізування небезпечних чинників (PHA)", "Дослідження небезпечних чинників і працездатності (HAZOP)", "Аналізування небезпечних чинників і критичні точки контролю (HACCP), "Загальне оцінюванная екологічного ризику", "Структурований метод "Що - якщо" (SWIFT)", "Аналізування сценаріїв", "Аналізування впливу на діяльність (BIA)", "Аналізування першопричини (RCA)", "Аналізування видів і наслідків відмов (FMEA)", "Аналізування дерева відмов (FTA)", "Аналізування дерева подій (ETA)", "Аналізування причин і наслідків", "Аналізування причинно-наслідкових зв'язків", "Аналізування рівнів захисту (LOPA)", "Дерево рішень", "Загальне оцінювання надійності людини (HRA)", "Аналізування за схемою "краватка-метелик", "Технічне обслуговування, зорієнтоване на забезпечення безвідмовності", "Аналізування паразитних схем (SA)", "Марковське аналізування", "Імітаційне моделювання за методом Монте-Карло", "Байєсова статистика і мережі Байєса", "Криві FN", "Показники ризику", "Матриця "наслідок-ймовірність", "Аналізування витрат і вигод (CBA)", "Багатокритерійне аналізування рішень (MCDA)".

Завдання вибору методу можна розділити на 2 етапи:

1) вибір придатного методу відповідно до галузі інформаційної безпеки за допомогою оцінки;

2) вибір оптимального методу оцінки ризику.

З вище перелічених методів такі не придатні для аналізу інформаційної безпеки: "Дослідження небезпечних чинників і працездатності (HAZOP)", "Аналізування небезпечних чинників і критичні точки контролю (HACCP)", "Загальне оцінюванная екологічного ризику".

Далі розглянемо методи які стосуються кожного етапу оцінки ризиків. Для ідентифікації ризиків не підходять такі методи: "Аналізування першопричини (RCA)", "Дерево рішень", "Аналізування за схемою "краватка-метелик", "Імітаційне

моделювання за методом Монте-Карло", "Байєсова статистика і мережі Байєса". Таким чином, вибір зменшується і тепер вибираємо з 23 методів.

Оптимальність методів розглядається показниками наступних властивостей:

- ресурсомісткість (необхідні ресурси: тимчасові, інформаційні та інші);
- характеру і ступеня невизначеності оцінки ризику, заснованої на доступній інформації і відповідностям цілям;
- складності проблеми і методів, необхідних для аналізу ризиків.

З таблиці А.2 Додатка А, стандарту ДСТУ IEC/ISO 31010:2013 вибираємо найоптимальніші за наведеними властивостями: "Структуроване опитування", "Мозковий штурм" та "Переліки контрольних запитань". Таким чином, для етапу ідентифікації ризику ми вибрали три методи, які можна комбінувати або використовувати найкращий з них.

Для етапу аналізу ризику не підходять такі методи: "Структуроване чи напівструктуроване опитування", "Переліки контрольних запитань", "Мозкова атака", "Метод Делфі", "Попереднє аналізування небезпечних чинників (PHA)", "Імітаційне моделювання за методом Монте-Карло", "Байєсова статистика і мережі Байєса". Таким чином залишається 21 метод. оптимальні з них: "Структурований метод "Що - якщо", "Аналізування впливу на діяльність (BIA)", "Аналізування першопричини (RCA)", "Аналізування видів і наслідків відмов (FMEA)", "Аналізування дерева подій (ETA)", "Аналізування причинно-наслідкових зв'язків", "Аналізування рівнів захисту (LOPA)", "Загальне оцінювання надійності людини (HRA)", Технічне обслуговування, зорієнтоване на забезпечення безвідмовності", "Аналізування паразитних схем (SA)", "Матриця "наслідок-ймовірність".

Для порівняльної оцінки ризику не підходять такі методи: "Переліки контрольних запитань", "Структуроване чи напівструктуроване опитування", "Мозкова атака", "Метод Делфі", "Попереднє аналізування небезпечних чинників (PHA)", "Аналізування дерева подій (ETA)", "Аналізування причинно-наслідкових зв'язків", "Аналізування рівнів захисту (LOPA)", "Аналізування паразитних схем (SA)", "Марковске аналізування". З 21 вибираємо оптимальні, грунтуючись також на можливості отримання кількісних вихідних даних: "Аналізування дерева відмов (FTA)", "Аналізування причин і наслідків", "Аналізування за схемою "краватка-метелик", "Технічне обслуговування, зорієнтоване на забезпечення безвідмовності", "Імітаційне моделювання за методом Монте-Карло", "Байєсова статистика і мережі Байєса".

Висновок. У цій статті було проведено відбір методів оцінки ризику інформаційної безпеки по кожному етапу загального процесу на базі стандарту ДСТУ IEC/ISO 31010:2013

Практичний досвід побудови моделі загроз інформаційній безпеці виявив, що запропонований підхід значно спрощує завдання застосування методів оцінки ризику для конкретних інформаційних систем і заданого рівня безпеки інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Смогунов В.В., Вершинин Н.Н., Авдонина Л.А.Классификация методов управления риском // Труды международного симпозиума Надежность и качество. 2009 Т. 2. С. 235-238.

2. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику.

УДК 004.056

Лимарчук-Яциковська Т.О., студентка гр. 125м-16-1,
Науковий керівник: Мілінчук Ю.А., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

АРХІТЕКТУРНІ МЕТОДИ В КІБЕРБЕЗПЕЦІ

У наш час більшість підприємств вже замислюється над тим, що їм треба захищати свою інформацію та інформаційні ресурси. В Україні швидкий зріст кількості місць працевлаштування, був зумовлений масивною атакою 27 червня 2017 року. Після нечуваної для України кібератаки, майже всі зрозуміли, що їм треба фахівець з ІБ.

Але, навіть з розумінням, поведінка керівників відрізняється в залежності від рівня розвитку підприємства. У представників великих підприємств (з річним доходом більше суми 50 мільйонів євро та середньою кількістю працівників рівною 250 особам [1]) такі спеціалісти зазвичай включені до складу працівників; у представників малого бізнесу та мікропідприємств (з річним доходом менше суми у 10 мільйонам євро та середньою кількістю працівників не більше 50 осіб [1]) проблеми ІБ не є першочерговими та інформація яка циркулює на підприємстві, частіше за все, коштує менше ніж засоби захисту інформації. А усі інші підприємства, що включені до поняття «середнього підприємства» вже вважають доцільним піклуватись за свою інформацію та ще не знають, що для цього потрібно. Тому вони потребують уваги та великих трудовитрат .

Для вирішення їх завдань може використовуватися архітектура підприємства (Enterprise Architecture), що дозволяє сформувати набір принципів, підходів і технологій, які, з огляду на поточний стан організації, закладають основу її подальшої трансформації, зростання і розвитку. Сьогодні існує чимало підходів до створення таких архітектур. Але який би з підходів не був вибраний, в сучасних умовах просто неможливо розвиватися без використання інформації та інформаційних технологій, які повинні не тільки підтримувати будь-які зміни в бізнесі, але і передбачати їх, готуватися до них заздалегідь , а в ряді випадків і сприяти появі нових бізнес-можливостей. Однак не завжди бізнес розвивається передбачуваним чином. Ризики різної природи можуть порушити зростання і розвиток підприємства і поставити його на грань вимирання. Чималу роль в цьому відіграють інформаційні та операційні ризики, пов’язані з витоками даних, виведенням з ладу елементів IT-інфраструктури і т.п. Для того щоб підготувати себе до ризиків сьогодення і майбутнього необхідна архітектура інформаційної безпеки, що пронизує всі інші архітектури підприємства. [2]

Завдяки архітектурному підходу про ІБ тяжче буде забути іншим підрозділам та IT-спеціалісти не нароблять помилок на етапі побудови моделі не питаючись в ІБ-фахівців. Архітектура IT систем підприємства дозволяє побачити усі процеси компанії та побудувати оптимізовані алгоритми роботи різних підрозділів. У чому ж полягає оптимізація? Наприклад, хоча теоретично грамотна розробка архітектури та стратегії повинна здійснюватися зверху вниз (спочатку визначаються цілі, потім способи їх досягнення і тільки потім накуповується різне ПЗ і апаратура, можлива реалізація проектів і т.д.), на практиці ж все зазвичай відбувається навпаки: спочатку здійснюється закупівля «потрібних» засобів захисту, які у всіх на слуху, потім починається їх експлуатація, виявляються недоліки при впровадженні та підтримці, ведеться пошук шляхів оптимізації наявних ресурсів і оцінки ефективності використовуваних технологій і захисних заходів і тільки після цього хтось починає замислюватися про стратегію та архітектуру ІБ.

Другим за поширеністю після відсутності архітектури і стратегії є підхід, що полягає у виробленні бачення або плану застосування технічних рішень або організаційних заходів: аудиту безпеки, підвищення обізнаності, тощо. І хоча це краще, ніж нічого, до розробки реальної архітектури такий підхід не дотягує з двох причин: відсутні цілепокладання і прив'язка до бізнесу та відсутні метрики ефективності досягнення заявлених цілей.

Отже, якщо зрозуміло, що є потреба у комплексному підході та у найбільш щільному «вбудуванні» ІБ в процеси компанії, допоміжним інструментом може стати архітектурний метод будування ІТ-систем, але і його треба доробляти з огляду на вимоги ІБ. Архітектура ІБ повинна розроблятися зверху вниз, відштовхуючись від цілей та стратегії підприємства, в яких зафіксовано, що і як має бути зроблено в контексті всієї компанії. Архітектура, в свою чергу, присвячена тому, як ці цілі реалізуються з точки зору інформаційної безпеки. Облік стратегії бізнесу дозволяє зрозуміти в цілому, на чому необхідно сконцентруватися в архітектурі ІБ. Якщо перед компанією стоїть завдання географічної експансії та серйозного зростання, то впроваджувані рішення в області інформаційної безпеки повинні сприяти цій меті. Зокрема, велику увагу потрібно приділити VPN-рішень, захищеному віддаленого доступу і т.п. На етапі стабілізації бізнесу акцент зміщується в бік підвищення якості обслуговування, зростання лояльності клієнтів, і інформаційна безпека повинна бути спрямована саме на це. В умовах нестабільної економічної ситуації і бізнес-рішення докорінно змінюються, і система безпеки вже вирішує зовсім інші завдання: захист від витоків і крадіжки інформації з боку співробітників, що звільняються, безпеку аутсорсингу і т.п. Тому потрібно розробляти архітектуру повинні фахівець з інформаційної безпеки та керівник підрозділу ІТ разом, запрошуючи керівників різних підрозділів для розуміння їх потреб та зважати на потреби бізнесу. У такому разі ризики ІБ будуть зменшені, проблеми масштабованості зустрічатися рідше, а рядовий персонал буде більш спокійно реагувати на обмеження висунуті політикою інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Лист ДФС від 08.11.2016 № 24033/6/99-99-14-03-03-15
2. Архітектура і стратегія інформаційної безпеки Cisco. https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/Cisco_Security_Architecture.pdf

УДК 007:658
Легенченко К.О., студентка групи 125м-16-1
Науковий керівник: Тимофєєв Д.С., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

УПРАВЛІННЯ ОБІЗНАНІСТЮ ПЕРСОНАЛУ В ПИТАННЯХ ПРОТИДІЇ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Важливим фактором захисту інформації на підприємствах є акцент на протидії методам соціальної інженерії. Будь-яка інформація, незалежно від її формату та стану - обробляється вона процесором, передається по каналах зв'язку, зберігається на диску - повинна входити в межі контролю системи забезпечення ІБ. Але технічні засоби, крім основного функціоналу, мають інтерфейси взаємодії з людиною, тому важливим елементом захисту інформації є сам співробітник компанії. Якщо по відношенню до технічних засобів завжди можна описати можливі ситуації, визначити і оцінити ризики, знайти способи захиститися (обмежити доступ, зашифрувати і т.п.), то в разі дій людини виникає проблема.

Виходячи з цього внутрішні загрози можуть утворюватися внаслідок:

- непрофесійних дій працівників;
- низького стану виховної та профілактичної роботи в організації;
- недосконалої системи заробітної плати та стимулювання праці персоналу;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;
- психологічних та комунікаційних особливостей працівників;
- відсутності нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу. [1]

До сих пір не існує чіткої, всеосяжної математичної моделі, яка описує поведінку людей в різних ситуаціях, реакцію на той чи інший вплив або сформовані умови, можливі помилки. Природно, що цей фактор відіграє на руку зловмисникам.

В атаках, що використовують методи соціальної інженерії, можна виділити 3 основних етапи: збір, профілювання і реалізація.

1. Збір даних про мету атаки є найбільш важливою стадією. Роботи полягають у визначенні характеристик об'єктів атаки, в тому числі шляхом зовнішнього впливу. Джерелом даних можуть бути соціальні мережі, публічно доступна інформація і ін. Також ефективними є спілкування з членами сім'ї, друзями і колегами, спостереження за діяльністю мети і навіть взаємодія з нею.

2. На етапі профілювання виконується аналіз зібраної інформації для побудови моделі атаки. Виділяються характеристики, що властиві цілі, а також її слабкості, на підставі чого вибираються канали взаємодії (пошта, телефонні дзвінки, особисте спілкування і т.п.), методи реалізації (вербування, неформальне спілкування, тиск і т.п.) і можливі вектори атаки, які можуть бути ефективними проти конкретної мети.

3. На етапі виконання атаки реалізується її модель, вироблена на стадії профілювання. Тут вступають в повну силу психологія, НЛП і технічні засоби. У разі вдалої реалізації першої хвилі атаки можна повернутися до етапу збору інформації з новими вхідними даними і ітеративно повторювати виконання етапів до тих пір, поки продовжує виявлятися нова інформація, або поки атака не досягне бажаної глибини. [2]

Активне використання інтернету, крім плюсів, має ряд значних мінусів. Це і додаткові канали комунікації з жертвою, і залишені жертвою «сліди», вивчивши які, можна скласти портрет потенційної мети атаки. Інтернет дає зловмисникам можливість автоматизувати свою роботу, що значно скорочує «трудовитрати» на виконання атаки.

У той же час багато компаній і бояться, і не розуміють, навіщо їм потрібна оцінка свого персоналу, заснована на застосуванні методів соціальної інженерії. Бояться зазвичай внаслідок того, що такий процес не регламентований законодавством або міжнародними стандартами. Він більшою мірою експертний, часто його результативність залежить від навичок конкретного виконавця. [3]

Крім застосування технічних заходів захисту інформації (розмежування доступу, мінімізації повноважень, моніторингу подій і трафіку і т.п.), які протидіють відомим шаблонами атак, основним заходом захисту від використання прийомів соціальної інженерії є метод «Безпека через навчання». Навчання має бути регулярним, простим і зрозумілим. Часто в організаціях до процесу навчання вимогам і практикам ІБ підходять формально. Тому виникає ситуація, коли працівники компаній мають низький рівень поінформованості та грамотності з питань інформаційної безпеки. Це тягне за собою їх халатне, неуважне ставлення до вхідних інформаційних потоків. Крім навчання, також варто підвищувати пильність співробітників шляхом їх періодичного тестування. [4]

На завершення необхідно відзначити, що гуманітарну проблему не можна вирішити виключно технічними методами. Тільки комплексний підхід може захистити від атак із застосуванням методів соціальної інженерії. Шляхом збору, обробки, порівняння та аналізу досліджень в сфері протидії атакам з використанням методів соціальної інженерії, необхідно описати і організувати систему заходів і методів підвищення кваліфікації персоналу в сфері протидії атакам з використанням методів соціальної інженерії.

Напрямок досліджень:

- вивчити раніше проведені дослідження в області протидії атакам з використанням методів соціальної інженерії;
- розробити теоретичну базу, де слід викласти основні поняття в сфері протидії атакам з використанням методів соціальної інженерії;
- класифікувати типи і види атак з використанням методів соціальної інженерії (з прикладами);
- проаналізувати існуючі методи протидії атакам даного типу;
- запропонувати унікальні методи протидії атакам з використанням соціальної інженерії;
- проаналізувати ефективність запропонованих методів протидії;
- розробити ряд методик для підвищення кваліфікації персоналу протидії методам соціальної інженерії;
- розробити спеціальне програмне забезпечення, що дозволяє дохідливо і ефективно піднести дані методики для персоналу підприємств.

ПЕРЕЛІК ПОСИЛАНЬ

1. Будник М.М. ,Тимофєєв Д.С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації (Електрон. ресурс) / Спосіб доступу: URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1666/7.pdf?sequence=1

2. Резник Ю.М. Соціальна інженерія: предметна область і межі застосування // Соціологічні дослідження, 1994, № 2.

3. Соціальна інженерія // Сучасна західна соціологія: Словник. М., 2015.

4. Романенко Е.А., Тимофеев Д.С. Методы обучения персонала по вопросам информационной безопасности (Електрон. ресурс) / Спосіб доступу: URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1667/14.pdf

УДК 004.415.53

Кот Леонид Леонидович, ст. гр. 125м-16-1
Научный руководитель: Кручинин Александр Владимирович, ст. преп. кафедры безопасности информации и телекоммуникаций
(Государственное ВУЗ «Национальный горный университет», г. Днепр, Украина)

УЯЗВИМОСТИ ВЕБ – ПРИЛОЖЕНИЙ И СРЕДСТВА ИХ ОБНАРУЖЕНИЯ

В данных тезисах выполнен обзор и анализ уязвимостей веб - приложений, существующих баз данных уязвимостей, их оценок и средств обнаружения.

Ключевые слова: уязвимость, CVE, vulnerability.

ВВЕДЕНИЕ

В современном обществе и бизнесе высока роль веб – приложений в построении эффективной работы.

Увеличение количества разнообразных веб – приложений приводит к возникновению в них уязвимостей, поскольку как в процессе разработки, так и эксплуатации приложений могут происходить ошибки их функционирования, приводящие к уничтожению или утечке информации.

Согласно данным отчета компании Trustwave [1], [2]:

- 98% протестированных приложений имели уязвимости;
- 95% мобильных приложений, имели уязвимости (из которых 35 % имели критические уязвимости);
- в 2015 году была обнаружена 21 уязвимость нулевого дня;

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ УЯЗВИМОСТИ

Уязвимость программного обеспечения (ПО) – недостаток, который может привести к нарушению конфиденциальности, целостности или доступности информации.

Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании, эксплуатации, а также ненадежных паролей, вирусов, скриптовых и SQL-инъекций[3].

Уязвимости можно классифицировать по этапам жизненного цикла ПО, на которых они появляются:

- уязвимости этапа проектирования;
- уязвимости этапа реализации;
- уязвимости этапа эксплуатации.

Для обнаружения и использования уязвимостей злоумышленники используют эксплойты.

Эксплойт – это программа, фрагмент кода программы или последовательность команд, которые используют уязвимости в ПО.

Целями атак могут быть: кража личных данных, захват контроля над системой (повышение привилегий), использование компьютера в качестве элемента ботнета для рассылки спама или выполнения DDoS-атак и т.д. [3].

Следует отметить, что существует временной интервал между открытием уязвимости и выходом патча ее исправления. Данный факт свидетельствует о дополнительной угрозе, поскольку в этом интервале эксплойты могут без проблем функционировать в системе.

Также существует понятие уязвимости нулевого дня или 0day эксплойты.

0day - уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы. Это означает, что у разработчиков было 0 дней на

исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем программного обеспечения исправлений ошибки [4].

ОБЗОР БАЗ ДАННЫХ УЯЗВИМОСТЕЙ

Информация про уже найденные уязвимости содержится в специально созданных базах данных.

Одной из баз уязвимостей является Common Vulnerabilities and Exposures (CVE) компании MITRE [5].

CVE является единым промышленным стандартом описания уязвимостей. Каждой уязвимости присваивается свой идентификатор, который имеет следующий формат: CVE-YYYY-NNNN, где:

- CVE – префикс;
- YYYY – год обнаружения уязвимости;
- NNNN – порядковый номер (последовательность из 4 и более цифр);

Каждая запись об уязвимости включает:

- CVE – идентификатор;
- краткое описание уязвимости;
- ссылки на другие ресурсы, имеющие отношение к обнаружению уязвимости (отчеты, рекомендации и т.д.);

Процесс добавления уязвимости в базу содержит три этапа [5]:

- обработку – анализ, исследование и процесс приведения уязвимости к формату CVE;
- присвоение – назначение конкретной записи уязвимости идентификатора CVE;
- публикацию – добавление новой записи и публикация ее на Интернет-ресурсе CVE;

Краткое описание уязвимости составляется сотрудниками специального отдела компании MITRE (MITRE's CVE Content Team), которые анализируют отчеты о найденных уязвимостях, исследуют любую противоречивую информацию или несовместимое использование терминологии, а затем составляют описание уязвимости, включающее всю необходимую информацию, чтобы пользователи могли легко найти уязвимость по идентификатору или различить похожие уязвимости [5].

Список известных уязвимых мест в ПО содержится в CWE (Common weakness enumeration) [6].

К другим крупным центрам детектирования уязвимостей относятся:

- национальный институт стандартов и технологий (National Institute of Standards and Technology – NIST) и его Национальная база данных уязвимостей (National Vulnerabilities Database – NVD) [7];
- группа чрезвычайного компьютерного реагирования Соединенных Штатов (United States Computer Emergency Readiness Team – US-CERT) с базой данных записей уязвимостей (Vulnerability Notes Database – VND) [8];
- проект SecurityFocus [9];
- компания Secunia [10];

ОБЗОР СИСТЕМЫ CVSS

Критичность уязвимостей, содержащихся в базах данных уязвимостей, рассчитывается с помощью системы CVSS [11].

Общая система оценки уязвимостей (CVSS) – это открытая схема, которая позволяет обмениваться информацией об IT-уязвимостях. Система оценки CVSS состоит из 3 метрик: базовая метрика, временная метрика и контекстная метрика. Каждая метрика представляет собой число (оценку) в интервале от 0 до 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки.

Цель системы состоит в расставлении приоритетов для уязвимостей, чтобы в первую очередь исправлять те из них, которые представляют наибольшую опасность.

СРЕДСТВА ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ

Современные средства обнаружения уязвимостей представлены в виде сканеров уязвимостей, как бесплатных, так и коммерческих, где бесплатно предоставляется только пробная версия. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак.

Современный сканер уязвимостей выполняет основные задачи:

- идентификацию доступных сетевых сервисов;
- идентификацию имеющихся уязвимостей сетевых сервисов;
- выдачу рекомендаций по устранению уязвимостей.

Немаловажной характеристикой сканера уязвимостей является совместимость с существующими базами данных уязвимостей (CVE). В этом случае при обнаружении в системе уязвимости сразу отображается актуальная информация по найденной уязвимости со ссылкой на ее описание в базе уязвимостей.

Эффективнее всего производить поиск уязвимостей с помощью специальных методик, таких как OWASP Testing guide [12] и инструментов, включенных в операционную систему Kali Linux [13].

Kali Linux содержит много полезных инструментов для тестирования защищенности веб – приложений путем проверки их отдельных компонентов, функций. Методика OWASP Testing guide содержит перечень компонентов/функций приложения, которые обязательны для проверки защищенности, а также рекомендованный набор инструментов для тестирования защищенности. Цель методик тестирования защищенности – определить последовательность использования инструментов для тестирования, чтобы промежуточные результаты одного этапа тестирования могли использоваться как входные данные для следующего этапа. Например, Metasploit Framework позволяет имитировать сетевую атаку и выявлять уязвимости системы. Для проведения атаки необходима информация об установленных на удаленном сервере сервисах и их версии, т.е. нужно дополнительное исследование с помощью таких инструментов, как Nmap.

ВЫВОД

Эффективность тестирования защищенности и результат поиска уязвимостей зависит от правильности выбора методик тестирования и инструментов тестирования, что подразумевает адаптацию существующих методик для тестирования конкретных веб – приложений.

СПИСОК ИСТОЧНИКОВ

1. Отчет Trustwave [Электронный ресурс]. – [Режим доступа]:http://www2.trustwave.com/rs/815-RFM-693/ /images/2015_TrustwaveGlobalSecurityReport.pdf

2. Блог Trustwave [Электронный ресурс]. – [Режим доступа]: https://www.trustwave.com/Resources/Trustwave-Blog/Introducing-the-2016-Trustwave-Global-Security-Report/

3. Уязвимости. Википедия. [Электронный ресурс]. – [Режим доступа]: https://ru.wikipedia.org/wiki/Уязвимость_ (компьютерная_безопасность)

4. Уязвимость нулевого дня. Википедия. [Электронный ресурс]. – [Режим доступа]: https://ru.wikipedia.org/wiki/Уязвимость_нулевого_дня

5. CVE Mitre [Электронный ресурс]. – [Режим доступа]: http://cve.mitre.org

6. CWE Mitre [Электронный ресурс]. – [Режим доступа]: http://cwe.mitre.org

7. База уязвимостей NIST [Электронный ресурс]. – [Режим доступа]: https://nvd.nist.gov

8. Vulnerability Notes Database [Электронный ресурс]. – [Режим доступа]: http://www.kb.cert.org/vuls

9. База уязвимостей SecurityFocus [Электронный ресурс]. – [Режим доступа]: http://www.securityfocus.com

10. База уязвимостей Secunia [Электронный ресурс]. – [Режим доступа]: https://secuniaresearch.flexerasoftware.com /community/research/

11. Система CVSS [Электронный ресурс]. – [Режим доступа]: https://www.first.org/cvss/

12. OWASP Testing Guide [Электронный ресурс]. – [Режим доступа]: https://www.owasp.org/index.php/OWASP_ Testing_Guide_v4_Table_of_Contents

13. Kali Linux [Электронный ресурс]. – [Режим доступа]: https://www.kali.org

14. Metasploit framework [Электронный ресурс]. – [Режим доступа]: https://www.metasploit.com

15. Сканер Nmap [Электронный ресурс]. – [Режим доступа]: https://nmap.org

УДК 004.056
Дзюба Євгеній Андрійович, студент гр. 125м-16-1,
Науковий керівник: Войцех Сергій Іванович, ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ЛІНІЯМИ ЕЛЕКТРОЖИВЛЕННЯ

Проаналізовано причини виникнення електричного каналу витоку інформації лініями електроживлення. Розглянуто переваги та недоліки пасивних та активних методів і засобів технічного захисту від витоку інформації лініями електроживлення. Зроблено висновок щодо підходів до їх застосування.

Ключові слова: електричний канал, витік інформації, методи та засоби захисту.

ВСТУП

Інформаційна безпека являє собою сукупність офіційних взглядів на цілі, задачі, принципи та основні напрями забезпечення інформаційної безпеки. Захищеність ліній електроживлення технічних засобів, що входять до складу інформаційно-телекомунікаційних систем різного рівня – це важлива складова підтримання відповідного рівня інформаційної безпеки.

Причини виникнення електричних каналів витоку інформації:

- наявність гальванічних зв’язків з’єднувальних ліній ТЗПІ з лініями ДТЗС і сторонніми провідниками;
- наведення побічних електромагнітних випромінювань ТЗПІ на з’єднувальні лінії ДТЗС та сторонні провідники, лінії електроживлення та заземлення ТЗПІ;
- «просочування» інформаційних сигналів в лінії електроживлення та заземлення ТЗПІ.

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ

Для забезпечення захисту об’єктів інформаційно-комунікаційних систем від витоку інформації лініями електроживлення використовуються як активні, так і пасивні методи та технічні засоби протидії.

До переваг пасивних методів захисту можно віднести:

- можливість оптимізації схемотехнічних та конструкторсько-технологічних рішень з метою мінімізації або повного усунення паразитних генерацій та побічних випромінювань;
- зниження сприйнятливості апаратних засобів до впливу зовнішніх електромагнітних полів та імпульсних сигналів;
- підвищення надійності та завадозахищеності апаратних засобів.

Пасивні засоби захисту інформації – це в першу чергу, мережеві протизавадні фільтри для однофазних та трифазних електричних мереж із змінною напругою до 380 В, постійною до 500 В, частотами 50 Гц/ 400 Гц, з максимальним робочим струмом до 200 А, що забезпечують захист від впливу індустріальних та високочастотних перешкод у різних смугах радіочастотного спектру.

Протизавадні фільтри застосовуються для забезпечення електромагнітної розв’язки ліній електроживлення електричних мереж різної приналежності, радіоелектронних пристроїв, засобів обчислювальної техніки та високоточних електронних приладів.

Перевагами активних методів захисту являються:

- відсутність впливу на роботу ПЕВМ та іншої офісної техніки;
- нечутливість до значних сплесків напруги живлення;

- можливість подачі шумового сигналу безпосередньо в електромережу через власний кабель живлення (лінійне зашумлення).

До недоліків можна віднести:

- відносно високу ціну пристроїв;
- погіршення завадної обстановки в захищаємих мережах.

Активні засоби захисту інформації від її витоку електромережами здійснюють захист шляхом подачі протизавадного сигналу безпосередньо в електричну мережу. При цьому вони не повинні створювати перешкоди роботі ПЕВМ та пристроям побутової електроніки. Генератори завад призначені для захисту від витоку інформації лініями електроживлення у випадках застосування пристроїв несанкціонованого зняття інформації, що використовують електромережу як канал передачі інформації. Вони також здійснюють маскування паразитних наведень від засобів оргтехніки як можливої причини витоку інформації, що оброблюється.

ВИСНОВКИ

Несанкціонований витік інформації, що циркулює у кіберпросторі, може статися ще до її потрапляння туди через наявність технічних каналів витоку інформації, серед яких суттєву загрозу становить канал витоку інформації лініями електроживлення. Тому при проектуванні нових об’єктів інформаційної діяльності та реконструкції старих потрібен комплексний підхід щодо захисту ліній електроживлення від несанкціонованого витоку інформації із використанням технічних можливостеймережевих протизавадних фільтрів та генераторів завад.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ленков С.В. Методы и средства защиты информации: учеб. пособие / [Д.А. Перегудов, В.А. Хорошко]. — 2008. — 344 с.

2. Хорев А.А. Способы и средства защиты информации. — М.: МО РФ, 2000. — 316 с.

УДК 681.3
Бублик Олександр Борисович, студент гр. 125м-16-1,
Науковий керівник: Войцех Сергій Іванович, ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ЕКРАНУВАННЯ СКЛАДОВИХ ЕЛЕКТРОМАГНІТНОГО ПОЛЯ

У цих тезах розглянуті види електромагнітного екранування. Наведено класифікацію електромагнітних екранів. Сформульовано рекомендації щодо використання різних видів екранування з урахуванням їх особливостей.

Ключові слова – екранування; електромагнітне поле; екран; види екранування; ефективність екранування.

ВСТУП

Екрануванням називається локалізація електромагнітного поля в певному просторі шляхом обмеження його поширення всіма можливими способами. Під екрануванням в загальному випадку розуміється як захист приладів від впливу зовнішніх полів, так і локалізація випромінювання будь-яких засобів, що перешкоджає прояву цих випромінювань у навколишньому середовищі. Слід зазначити, що екранування є одним з найефективніших методів захисту від електромагнітних випромінювань. Для запобігання витоку інформації каналами ПЕМВН (побічних електромагнітних випромінювань та наводок) і через використання радіозакладних пристроїв застосовуються електромагнітні екрани. [1]

КЛАСИФІКАЦІЯ ЕЛЕКТРОМАГНІТНИХ ЕКРАНІВ

Електромагнітний екран – це конструкція, призначена для послаблення електромагнітних полів, що створюються будь-якими джерелами в деякій області простору, що не містить цих джерел.

Класифікувати екрани можна таким чином:

- екрани з внутрішнім збудженням електромагнітного поля - локалізація джерела перешкод;
- екрани зовнішнього електромагнітного поля, у внутрішній порожнині яких вміщуються чутливі до цих полів пристрої для захисту від впливу зовнішніх перешкод.

Що стосується роботи екранів, то виділяють три основних види:

- електростатичний - коли переважає електрична складова;
- магнітостатичне - коли переважає магнітна складова;
- електромагнітний - коли обидві складові рівноцінні.

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ВИДІВ ЕКРАНУВАННЯ

Перший вид екранування – електростатичний. Він застосовується для зниження паразитної ємності між електричними ланцюгами. Важливим є те, що ефективність не залежить від товщини та металу екрану (часто електростатичні екрани - тонкий шар металізованого діелектрика, а в трансформаторах часто екран виконують у вигляді не замкнутого кільця з мідної фольги або обмоток, один кінець яких заземлений). Під час екранування електричного поля дуже важливо створити низький опір екрану до корпусу не більше 4 Ом. [2]

Магнітостатическое екранування застосовується для придушення паразитних індуктивних зв’язків між двома електричними ланцюгами через близьке магнітне поле. Магнітостатическое екранування (екранування шунтуванням магнітного поля) використовується переважно для наведень низької частоти в діапазоні від 0 до 3 ... 10 Гц. Ефективність екранування таких полів залежить від магнітної проникності екрану і його товщини, а також від наявності стиків та швів, розташованих перпендикулярно

силовим лініям магнітного поля. Екрани виготовляють в основному з феромагнітних матеріалів (пермаллой, сталь, ферити) з великою магнітною проникністю.

Принцип дії електромагнітного екранування полягає в тому, що змінне магнітне поле послаблюється по мірі проникнення до металу, так як внутрішні шари екрануються вихровими струмами зворотного напрямку, що виникають в шарах, розташованих ближче до поверхні. Тобто, під дією джерела електромагнітної енергії на стороні екрану, зверненої до джерела, виникають заряди, а в його стінках - струми, що утворюють в зовнішньому просторі поля, по напруженості близькі до поля джерела, а по напрямку - протилежні йому. [2]

В результаті всередині екрану відбувається взаємна компенсація полів, а зовні його - витіснення зовнішнього поля полями вихрових струмів (ефект віддзеркалення).

Екрануюча дія вихрових струмів визначається двома факторами:

- зворотним полем, створюваним струмами (протікають в екрані);
- поверхневим ефектом в матеріалі екрану.

Слід зазначити, що змінне магнітне поле послаблюється по товщині матеріалу екрану внаслідок екранування внутрішніх шарів вихровими струмами, циркулюючими в поверхневих шарах. В цілому, електромагнітне екранування застосовується на високих частотах.

З підвищенням частоти сигналу застосовується виключно електромагнітне екранування, тому очевидно, що електромагнітне екранування є найбільш загальним і часто вживаним. Цей спосіб екранування може послаблювати як магнітні, так і електричні поля, тому називається електромагнітним.

ВИСНОВКИ

Екранування електромагнітних полів є одним із найдієвіших засобів захисту об’єкта від витоку інформації. Екранування електромагнітних полів проводиться не тільки для забезпечення вимог стосовно електромагнітної сумісності об’єкта, яка включає в себе й протидію несанкціонованому доступу до інформації з використанням спеціальних технічних засобів, але і для створення сприятливого електромагнітного середовища. [3] Однак слід пам’ятати, що кожний вид екранування має свої особливості, які необхідно враховувати. Дуже важливу роль відіграють електромагнітні екрани. Застосування якісних екранів дозволяє вирішувати багато завдань, серед яких захист інформації в приміщеннях і технічних каналах, завдання забезпечення правильного функціонування обладнання та приладів при їх спільному використанні, завдання захисту персоналу від підвищеного рівня електромагнітних полів та забезпечення сприятливої екологічної обстановки навколо діючих електроприладів та НВЧ-пристроїв.

ПЕРЕЛІК ПОСИЛАНЬ

1. Хорев А.А. Техническая защита информации. Том 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008, - 250 с.

2. Технические средства и методы защиты информации: Учебник для вузов/ Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО «Издательство Машиностроение», 2009, - 508 с.

3. Князев А. Д. Елементи теорії та практики забезпечення електромагнітної сумісності РЕЗ. – М.: Радио и связь, 1984., - 335 с.

УДК 681.3
Білоусова Вікторія Русланівна, студентка гр. 125м-16-1,
Науковий керівник: Войцех Сергій Іванович, ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ВІД ВПЛИВУ НЕНАВМИСНИХ ЕЛЕКТРОМАГНІТНИХ ЗАВАД

Наявність ненавмисних електромагнітних випромінювань може впливати на рівень захищеності інформації, що циркулює в інформаційно-комунікаційних системах. Проаналізовано можливості впливу ненавмисних електромагнітних завад та методи технічного захисту інформації від їх впливу. Сформульовані рекомендації щодо забезпечення електромагнітної сумісності технічних засобів та їх захисту від впливу ненавмисних електромагнітних завад.

Ключові слова – завада, сумісність, електромагнітні випромінювання, екранування.

ВСТУП

Електромагнітна завада (електромагнітна перешкода) — небажане фізичне явище або вплив електричних, магнітних або електромагнітних полів, електричних струмів та напруг зовнішніх або внутрішніх джерел, через що порушується нормальна робота технічних засобів або погіршується їх технічні характеристики та параметри[2].

Через вплив електромагнітної завади може статися спотворення інформації, що зберігається, перетворюється, передається або обробляється.

ЕЛЕКТРОМАГНІТНА СУМІСНІСТЬ ТЕХНІЧНИХ ЗАСОБІВ

Електромагнітна сумісність – це здатність радіоелектронних засобів і випромінювальних пристроїв одночасно функціонувати з обумовленою якістю в реальних умовах експлуатації з урахуванням впливу ненавмисних радіозавад і не створювати неприпустимих радіозавад іншим радіоелектронним засобам.

Сумісність може бути електромагнітна, електрична, інформаційна, конструктивна та програмна[2].

КЛАСИФІКАЦІЯ ЗАВАД

За походженням завади діляться на навмисні, ненавмисні, природничі та штучні.

1. Навмисні завади – створюються шляхом формуванням середовищ їх поширення з метою забезпечення умов для несанкціонованого витоку або спотворення інформації з обмеженим доступом.
2. Ненавмисні завади – утворюються, як результат побічного виникнення фізичних полів і середовищ їх поширення.
3. Природничі завади:

- Космічні шуми, реліктове випромінювання
- Радіовипромінювання Землі й об’єктів Сонячної системи
- Атмосферні завади Землі;

4. Штучні завади:

- Індустріальні або промислові завади електромагнітні випромінювання промислових машин, побутових електроприладів тощо;
- Станційні завади випромінювання від інших радіоелектронних засобів: радіостанцій, радіолокаторів тощо[2].

ПАРАМЕТРИ НЕНАВМИСНИХ ЕЛЕКТРОМАГНІТНИХ ЗАВАД

Для визначення імовірного відношення сигнал-завада при дії завади на рецептор, встановлення стандартів щодо вимог до допустимих рівнів завад, розробки пристроїв, які послаблюють (пригнічують) завади на шляху їх розповсюдження, а також при проведені контролю та діагностування по електромагнітній обстановці (ЕМО) окремого пристрою чи в цілому комплексу технічних засобів, що входять до складу інформаційно-комунікаційної системи, необхідно знання параметрів ненавмисних електромагнітних завад (НЕМЗ).

Знання параметрів необхідно, як у випадку детермінованих значень параметрів НЕМЗ, так і тоді, коли вони ґрунтуються на поняттях про випадкові стаціонарні і нестаціонарні електромагнітні процеси та у випадках одночасної дії на рецептор завад декількох джерел, коли значення одного параметру виявляється недостатнім.

ЗАХИСТ ВІД НЕНАВМИСНИХ ЗАВАД

Одним з найефективніших методів захисту від впливу електромагнітних випромінювань є екранування електромагнітних випромінювань[3].

Екранування передбачає розміщення елементів інформаційно-комунікаційних систем, що створюють електричні, магнітні та електромагнітні поля, в просторово замкнутих конструкціях. Способи екранування залежать від особливостей полів, що створюється елементами ІКС через протікання в них електричних струмів[5].

В залежності від параметрів створюваного електромагнітного поля розрізняють наступні види екранування:

- екранування електричного поля;
- екранування магнітного поля;
- екранування електромагнітного поля.

Екранування електричного поля, заземленим металевим екраном забезпечує нейтралізацію електричних зарядів, які стікають по заземлюючому контуру. Контур заземлення повинен мати опір не більше 4 Ом. Електричне поле може екрануватися за допомогою діелектричних екранів, що мають високу відносну діелектричну проникність

Екранування може здійснюватися на п’яти рівнях:

- рівень елементів схем;
- рівень блоків;
- рівень пристроїв;
- рівень кабельних ліній;
- рівень приміщень.

Починаючи з рівня блоків, екранування здійснюється за допомогою використання конструкцій з листової сталі, металевих сіток та шляхом напилення. Екранування кабелів здійснюється за допомогою металевої сітки, сталевих коробів або труб. При екрануванні приміщень використовуються: листова сталь товщиною до 2 мм, сталева (мідна, латунна) сітка з осередком до 2,5 мм. У захищених приміщеннях екрануються двері і вікна. Вікна екрануються сіткою, металізованими шторами, шляхом металізації стекол і обклеювання їх струмопровідними плівками. Двері виконуються зі сталі або покриваються струмопровідними матеріалами (сталевий лист, металева сітка). Особлива увага звертається на наявність електричного контакту струмопровідних шарів двері і стін по всьому периметру дверного отвору. При екранування полів неприпустимо наявність зазорів, щілин в екрані. Розмір осередку сітки повинен бути не більше 0,1 довжини хвилі випромінювання[4].

Вибір числа рівнів і матеріалів екранування здійснюється з урахуванням:

- характеристик випромінювання (тип, частота і потужність);
- вимог до рівня випромінювання за межами контрольованої зони і розмірів зони;
- наявності або відсутності інших методів захисту від ПЕМВН;

- мінімізації витрат на екранування.

У захищеної ПЕОМ, наприклад, екрануються блоки управління електронно-променевою трубкою, корпус виконується зі сталі або металізується зсередини, екран монітора покривається токопровідною заземленою плівкою і (або) захищається металевою сіткою.

Екранування, крім виконання своєї прямої функції захисту від ПЕМВН, значно знижує рівень шкідливого впливу електромагнітних випромінювань на організм людини. Екранування дозволяє також зменшити вплив електромагнітних завад на роботу пристроїв[3].

ВИСНОВКИ

Захист від впливу ненавмисних електромагнітних випромінювань залежить насамперед від електромагнітної сумісності пристроїв. Необхідно здійснювати організаційні та технічні заходи для вирішення проблеми електромагнітної сумісності технічних засобів та їх захисту від впливу ненавмисних електромагнітних завад. Наприклад, збільшення дистанції між технічними засобами; виконання електричної мережі живлення комп'ютерної техніки окремо від побутової електромережі; прокладання кабелів високовольтних електромереж та встановлення високовольтного електротехнічного обладнання з урахуванням вимог щодо рівня ЕМО у прилеглих приміщеннях.

ПЕРЕЛІК ПОСИЛАНЬ

1. Постанова КМ від 24.06.2009р. №679 "Про затвердження Технічного регламенту радіообладнання і телекомунікаційного кінцевого (термінального) обладнання"

2. Князев А. Д. Елементи теорії та практики забезпечення електромагнітної сумісності РЕЗ. – М.: Радио и связь, 1984. – 336 с

3. Уайт Д. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи: Пер. с англ. / Под ред. А.И. Сапгира. – М.: Сов. радио,1979. – В. 3. – 464 с.

УДК 004.056.5

Стародубець О.В., студент групи 125м-16-1,
Науковий керівник: Тимофєєв Д. С., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ВПРОВАДЖЕННЯ СИСТЕМ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

В наш час серйозно ускладнюється інфраструктури організацій всіх можливих галузей, від банків і до державних організацій. В першу чергу це пов'язано з швидким розвитком технологій і різновидів електронних пристроїв які оброблюють інформацію, тому така тенденція формує потребу в захисті та автоматизації інформаційних активів.

На даний момент підхід до контролю потенційно небезпечних подій у вигляді декількох незалежних засобів захисту інформації з самостійними консолями, які як правило контролюються різними людьми, стає надмірно ресурсномістким і неефективним, в результаті чого адекватна і своєчасна реакція на них стає все більш трудомісткою. Складність забезпечення відповідної реакції на потенційно небезпечні події неминуче призводить до зниження ефективності системи інформаційної безпеки організації. Рішенням такого завдання є створення центру моніторингу і реагування, який будується на регламентах, процесах, кваліфікованих кадрах і грамотному технічному рішенні.

Компанії, впроваджуючи основні елементи безпеки, часто не приділяють належної уваги такому важливому елементу забезпечення інформаційної безпеки, як моніторинг системи інформаційної безпеки.

В результаті, витративши сили і засоби на впровадження засобів захисту, компанії вважають завдання виконаним, але на перевірці виявляється, що:

- критичні системи уразливі і доступні для зловмисників;
- на робочих станціях встановлено недозволене ПО;
- конфігурації не відповідають розробленим політикам;
- події, які свідчать про інцидент ІБ, залишаються непоміченими;
- виявивши інцидент ІБ, немає чітко визначеної процедури, що з ним робити далі і хто цим повинен займатися;
- у адміністраторів інформаційної безпеки немає повної і цілісної картини про стан ІБ, є тільки фрагментарні уявлення;
- і т.д.

Комплексний моніторинг ІБ передбачає збір та аналіз подій безпеки від різних систем захисту, пристроїв і додатків, збір конфігураційних даних, даних про уразливість і т.д. Це дозволяє отримати повну і достовірну інформацію про наявні події і вразливості ІБ, поточних налаштуваннях, тобто мати цілісну картину поточної захищеності компанії. Здійснюючи такий контроль, організації мають можливість оперативного управління інформаційною безпекою, виявляючи відхилення, своєчасно вирішуючи інциденти ІБ, усуваючи уразливості, вживаючи заходів щодо корегування засобів захисту і т.д.

Підтвердження важливості і необхідності комплексного моніторингу знайшло відображення в різних стандартах в області інформаційної безпеки, таких, як: PCI DSS, ISO / IEC 27001: 2013, SOX.

Прикладом системи комплексного моніторингу ІБ на підприємстві є SOC.

SOC – Security Operations Center, або Центр оперативного управління, основними завданнями якого є консолідація подій з багатьох джерел, проведення певної аналітики і оповіщення уповноважених співробітників про інциденти інформаційної безпеки чи інших подіях. На основі отриманих даних співробітники

центру проводять розслідування, вживають заходів, щоб виключити можливість повторення події, мінімізують втрати. [1]

Ситуаційний центр являє собою комплексне організаційно-технічне рішення, що дозволяє:

• автоматизовано виявляти події, що представляють потенційну загрозу для організації, її інформаційних систем або інформаційних активів;

• забезпечити тривале зберігання всього обсягу зібраних подій і зафіксованих інцидентів ІБ для можливості проведення постінцідентного розслідування;

• реалізувати процес обробки виявлених інцидентів, який би дозволив в гарантований час (залежне від рівня критичності інциденту) оповіщати відповідальні підрозділи організації про те, що сталося, і рекомендувати необхідні заходи для запобігання впливу інциденту інформаційної безпеки на бізнес.

Зібрана в ході комплексного моніторингу інформація надходить в єдиний центр, де вона обробляється і представляється в наочному і зручному вигляді. Тут же здійснюється реагування та вирішення інцидентів ІБ, усунення виявлених відхилень. Побудова такого Центру оперативного управління ІБ (Security Operations Center, SOC) є не простим завданням.

Центр оперативного управління ІБ дозволяє контролювати і оперативно управляти інформаційною безпекою компанії в режимі реального часу, бути впевненим в тому, що необхідний рівень забезпечення ІБ досягнутий і підтримується, відстежувати виконання заданих цільових показників ефективності (KPI) забезпечення ІБ.

Центр оперативного управління ІБ дозволяє відстежувати відповідні в інформаційній системі події, пов’язані з ІБ, аналізувати і зіставляти їх з іншими даними, представляти зібрану інформацію в наочному і зручному вигляді, контролювати наявні уразливості, здійснювати контроль конфігурацій, відстежувати ступінь виконання вимог законодавства, нормативних актів і корпоративних політик, а також оперативно реагувати на виявлені інциденти ІБ. Тобто представлять повну картину поточного стану інформаційної безпеки компанії, що дозволяє оперативно усувати виявлені відхилення і забезпечувати заданий рівень ІБ.

На завершення необхідно відзначити основні переваги, які дає створення SOC ІБ, - це швидкість реакції на інциденти і підвищення керованості процесу забезпечення ІБ.

Час протікання більшості інцидентів у сфері інформаційної безпеки становить не більше секунди, а наслідки цих секундних збоїв можуть бути катастрофічні. У свою чергу, побудова SOC ІБ, за даними західних досліджень, знижує затримки реагування на інциденти ІБ через людський фактор на 80-90%.

Другим важливим перевагою є можливість бачити зріз стану інформаційної безпеки в комплексі, в режимі реального часу.

Можна виділити і більш приватні переваги, такі як:

• зниження ризиків і часу простою в критичних бізнес-процесах;

• контроль і запобігання інцидентів безпеки. Скорочення термінів робіт з розслідування інцидентів та надання звітів керівництву;

• вивільнення ресурсів фахівців інформаційної безпеки та IT-служби, оскільки вони витрачають багато часу на консолідацію і аналіз інцидентів, пов’язаних з порушеннями політики інформаційної безпеки компанії;

• відповідальність за процес;

• розстановка пріоритетів по ризиках для прийняття адекватних заходів захисту.

ПЕРЕЛІК ПОСИЛАНЬ

1. Єршов В.О. SOC vs CERT: Подібність і відмінності (Електрон. ресурс) / Спосіб доступу: URL: https://www.anti-malware.ru/node/16464

УДК 004.056
Колісниченко М.А., студентка групи 125м-16-1,
Науковий керівник: Тимофєєв Д.С., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА ВНЗ УКРАЇНИ

У наш час в умовах загальної інформатизації та розвитку інформаційних технологій посилюються загрози національній безпеці України в інформаційній сфері.

Концепцію національної безпеки України стосовно інформаційної сфери розвиває Доктрина інформаційної безпеки України .

Доктрина інформаційної безпеки визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [1]. У Доктрині зазначено, що забезпечення інформаційної безпеки України грає ключову роль в забезпеченні національної безпеки України. Слід відмітити, що одним із пріоритетних напрямків державної політики в галузі забезпечення інформаційної безпеки України є розвиток освіти в області інформаційної безпеки та вдосконалення підготовки кадрів. Особливу роль у вирішенні цих завдань відіграють вузи.

Система вищої освіти України перебуває у процесі постійного вдосконалення, що зумовлено трансформаційними змінами в суспільстві. Українська вища школа переживає період адаптації не тільки до об'єктивних процесів інформаційного суспільства, а й до нових соціально-політичних умов з різноплановими проявами конкурентної боротьби.

На сьогоднішній день створення ефективних механізмів управління інформаційними ресурсами системи вищої освіти в сучасних умовах неможливо без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки вузу, яка може бути сформована на основі вирішення наступних завдань [2] :

− аналіз процесів інформаційної взаємодії в усіх сферах основної діяльності українського технічного вузу: інформаційних потоків, їх масштабу і якості, протиріч, конкурентної боротьби з виявленням власників і суперників;

− розробка якісного і кількісного опису інформаційної взаємодії;

− введення кількісних індикаторів і критеріїв відкритості, безпеки і справедливості інформаційного обміну;

− розробка сценаріїв необхідності і значущості балансу в інформаційній відкритості і конфіденційності;

− визначення ролі і місця політики інформаційної безпеки в управлінні інформаційними ресурсами вузу і створення узгоджених принципів і підходів;

− формулювання основних складових політики: цілей, завдань, принципів і ключових напрямків забезпечення інформаційної безпеки;

− розробка базових методик управління процесом забезпечення політики інформаційної безпеки;

− підготовка проектів нормативно-правових документів.

У сьогочасному вузі зберігається і обробляється величезна кількість різних даних, які пов'язані не тільки із забезпеченням навчального процесу, а й з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація.

ВНЗ являє собою публічний заклад з непостійною аудиторією, а також є місцем підвищеної активності «початківців кіберзлочинців», у цьому і полягає специфіка захисту інформації в освітній системі .

Основними загрозами безпеки інформації у вузі можуть бути:

- спроби несанкціонованого адміністрування баз даних;
- дослідження мереж, несанкціонований запуск програм з аудиту мереж;
- видалення інформації, в тому числі бібліотек;
- запуск ігрових програм;
- установка вірусних програм і троянських коней;
- спроби злому АС «ВНЗ»;
- сканування мереж, в тому числі інших організацій, через Інтернет;
- несанкціонована відкачка з Інтернету неліцензійного софту і установка його на робочі станції;
- спроби проникнення в системи бухгалтерського обліку;
- пошук «дірок» в ОС, firewall, Proxy-серверах;
- спроби несанкціонованого віддаленого адміністрування ОС;
- сканування портів і т. п.

Особливості вузу як об'єкта інформатизації пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторовим розгалуженням інфраструктури (філії, представництва). Сюди ж можна віднести і різноманіття джерел фінансування, наявність розвиненої структури допоміжних підрозділів і служб (будівельна, виробнича, господарська діяльність), необхідність адаптації до мінливого ринку освітніх послуг, потреба в аналізі ринку праці, відсутність загальноприйнятої формалізації ділових процесів, необхідність електронної взаємодії з вищестоящими організаціями, часта зміна статусу співробітників і учнів.

У результаті зростання кількості злочинів у сфері інформаційних технологій з'являється велика кількість вимог до захисту ресурсів обчислювальних мереж навчальних закладів і виникає потреба у постановці завдання побудови власної інтегрованої системи безпеки. Її рішення припускає наявність нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної роботи, проектування, реалізацію і супровід технічних засобів захисту інформації в рамках освітнього закладу. Ці складові визначають єдину політику забезпечення безпеки інформації в вузі.

На жаль, роботи по кожному з перерахованих елементів носять фрагментарний характер і пов'язано це з:

- недостатнім фінансуванням робіт із захисту інформації;
- відсутністю єдиної политики інформаційної безпеки вузів, регіональних органів та самого міністерства освіти ;
- відсутність у адміністрації освітніх установ чітких уявлень про те, що саме і як необхідно захищати.

Можна зробити висновок, що тільки комплексна робота усіх складових процесу управління інформаційною безпекою ВНЗ може привести до створення безпечного інформаційного освітнього середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс] .- Режим доступу: http://www.president.gov.ua/documents/472017-21374

2. Труфанов А. И. Политика информационной безопасности вуза как предмет исследования // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004 [Електронний ресурс] .- Режим доступу: / library.istu.edu/civ/default.htm.

УДК 006.042

Хоменко І.І., студентка гр. УБіт-14-1,
Науковий керівник: Галушко С.О., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет» м. Дніпро, Україна)

РОЗВИТОК СТАНДАРТІВ БЕЗПЕКИ

Існує єдиний спосіб оцінити захищеність систем – розробити стандарт, що регламентує концепції інформаційної безпеки, вимоги до систем і шляхи їх реалізації, надає систему критеріїв і процедуру оцінювання систем за цими критеріями.

Розроблені та затверджені стандарти інформаційної безпеки створюють базу для погодження вимог розробників систем, споживачів і експертів, що оцінюють захищеність інформації.

Стандарти інформаційної безпеки існують трохи більше двадцяти років. У світі розробка стандартів, технічних звітів, керівництв та рекомендацій в галузі ІБ проводиться безперервно; послідовно публікуються проекти і версії стандартів, присвячених тим чи іншим аспектам інформаційної безпеки на різних стадіях узгодження і затвердження. Деякі стандарти поетапно заглиблюються і деталізують у вигляді сукупності взаємозв'язаних концепціями і структурами груп стандартів. Розробка нормативних документів з інформаційної безпеки, повністю або частково присвячених керуванню інцидентами інформаційної безпеки, здійснюється низькою спеціалізованих міжнародних організацій і консорціумів, таких як, наприклад: CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute тощо. Значна робота щодо стандартизації питань інформаційної безпеки, зокрема керування інцидентами, проводиться спеціалізованими організаціями і на національному рівні, в першу чергу в США – NIST, CMU/SEI; Німеччині та Великобританії – BSI. Все це дозволило сформувати обширну нормативно - методологічну базу у вигляді міжнародних, національних та галузевих стандартів, а також нормативних і керівних матеріалів, що регламентують діяльність в сфері керування інцидентами інформаційної безпеки. Проте, як свідчить сучасна практика, найважливішу роль в світі відіграють стандарти ISO. Основні з них: ISO 9000, ISO 9001, ISO 9004 (менеджмент якості); ISO 10001, ISO 10002, ISO 10003, ISO 10004 (задоволеність споживачів); EN 9100 (СМК в аерокосмічній галузі); ISO/TS 16949 (СМК в автомобілебудуванні); ISO 14001 (екологічний менеджмент); OHSAS 18001 (професійна безпека); ISO 31000 (менеджмент ризиків); ISO 20000 (СМК IT- послуг); ISO 22000 (продовольча безпека); ISO 26000 (соціальна відповідальність); ISO 50000 (системи менеджменту в енергетиці); ISO 27001 (інформаційна безпека). Усі вони, як основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як процес, а саме як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього.

У порівнянні з динамікою розвитку міжнародних стандартів, технічних звітів та рекомендацій з керування інцидентами інформаційної безпеки, в України використання та створення відповідної нормативно-методологічної бази знаходиться на початковій стадії та потребує подальшого розвитку. Несистематична та неістотна підготовка до реагування та обробки інцидентів інформаційної безпеки призводить до того, що на практиці реагування виявляється хаотичним, невпорядкованим та неефективним, істотно ускладнюючи відновлення бізнес-процесів (технічної експлуатації, менеджменту якості, надання послуг тощо) і через це – потенційно підсилює завданий збиток. Без своєчасної реакції на інциденти інформаційної безпеки та усунення їхніх

наслідків неможливо ефективне функціонування системи керування інформаційною безпекою. Суть методологічно-правильного процесу керування інцидентами ІБ – це чітке визначення ролей та розподіл відповідповідальності щодо якісного та своєчасного реагування на інциденти інформаційної безпеки. Стандартизований методологічний підхід до впровадження процесів керування інцидентами інформаційної безпеки дає можливість організаційно-технічній системі одержати наступні переваги:

•зниження негативного впливу інцидентів інформаційної безпеки на інформаційні процеси;

•прозорість контролю за ефективністю функціонування системи керування інформаційною безпекою;

•доступність моніторингу та оперативної управлінської інформації щодо функціонування системи керування інформаційною безпекою;

•превентивне визначення заходів щодо поліпшення системи керування інформаційною безпекою;

•ефективність взаємодії взаємопов’язаних підсистем керування якістю, послугами, ІБ та інцидентами.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO 9000, ISO 9001, ISO 9004 (менеджмент якості); ISO 10001, ISO 10002, ISO 10003, ISO 10004 (задоволеність споживачів); EN 9100 (СМК в аерокосмічній галузі); ISO/TS 16949 (СМК в автомобілебудуванні); ISO 14001 (екологічний менеджмент); OHSAS 18001 (професійна безпека); ISO 31000 (менеджмент ризиків); ISO 20000 (СМК ІТ- послуг); ISO 22000 (продовольча безпека); ISO 26000 (соціальна відповідальність); ISO 50000 (системи менеджменту в енергетиці); ISO 27001 (інформаційна безпека).

УДК 681.518.54

Доколяса О.С. студент гр. УБіт-14-1
Науковий керівник: Ковальова Ю.В., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

КІБЕРБЕЗПЕКА В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

З'ясовано зміст поняття «кібербезпека». Визначено проблему у необхідності подолання суперечності між наявним станом стрімкого зростання важливості кібербезпекової проблематики та часткової готовності Української держави відповісти на новітні кіберзагрози. Розглянуто проблему забезпечення державою кібербезпеки в інформаційному просторі, через ряд вдало проведених кібератак на інфраструктуру України.

Ключові слова: кіберпростір, кібербезпека, кіберзагроза.

За останні 6–8 років глобальний кіберпростір усе більшою мірою розглядається всіма державами світу як один із найважливіших безпекових пріоритетів, оскільки його функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів. У таких умовах виняткового значення для забезпечення національних інтересів та їх захисту на міжнародному рівні набуває ефективність механізмів забезпечення кібербезпеки держави та вирішення тих проблем, які виникають на шляху їх розбудови. Саме через більш широке використання комп'ютерних і телекомунікаційних технологій у найрізноманітніших сферах життєдіяльності соціуму України, у тому числі інтернет-технологій, разом з великою кількістю переваг принесло також і чималу кількість загроз. Реалізація цих загроз може завдати значної шкоди інфраструктурі України. Усвідомлення можливих втрат призвело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації загроз кіберпростору України і визначення важливості кібербезпеки в сучасному інформаційному просторі вцілому.

Згадки про перше використання терміну «кібербезпека» виникали у середині 1990-х років, коли уряд США став досліджувати цю тему [1].

За Законом України «Про основні засади забезпечення кібербезпеки України» термін «кібербезпека» означає захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2].

З урахуванням того, що проблема кібербезпеки носить глобальний характер, досить цікавою видається позиція міжнародних організацій. Так, Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй рекомендації дає таке визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача [3].

Актуальним питанням сьогодення є вдало здійснені кібератаки на інформаційний простір України. Влітку 2017 року державні установи та українські компанії зазнали масової кібератаки, вірусу Petya. A. Це була одна з найбільш масштабних кібератак в історії України. Атака показала, що держава була абсолютно не готова до кіберзагроз через несвоєчасне їх виявлення і відповідною реакцією основних

суб'єктів національної безпеки України. Основною причиною неготовності полягало у відсутності правового документу, що визначав би основні положення, щодо забезпечення кібербезпеки України.

Для регулювання подібних ситуацій необхідна нормативна база, саме тому в Україні розроблявся Закон «Про основні засади забезпечення кібербезпеки України» понад двох років. 5 жовтня 2017 р. Верховна Рада України ухвалила Закон «Про основні засади забезпечення кібербезпеки України» (Реєстраційний № 2126а), який був підписаний президентом 7 листопада 2017 р. Цей закон є позитивним нормативно-правовим актом, оскільки він визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів української держави в сфері кібербезпеки, забезпечує і надає основні правові повноваження спеціальним службам (державним органам) для забезпечення кібербезпеки. Основними її суб'єктами, тобто ті, на кого ляже відповідальність за гарантування кібербезпеки, мають стати Держспецзв'язок, нацполіція, СБУ, міністерство оборони, генштаб ЗСУ, розвідка та НБУ. Першочергове реагування на кіберзагрози закон покладає на створену ще в 2007 році урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA. Ця структура діє при Державній службі спеціального зв'язку та захисту. Важливим у цьому законі є те, що він впроваджує кримінальну відповідальність, за злочини, вчинені саме в кіберпросторі. А також тлумачить самі поняття "кібербезпека", "кіберзахист" та "кіберзлочинність", які вже понад десяти років використовують у юридичній практиці, у тому числі у зв'язку із вчиненими в мережі злочинами, але які досі не були ніде закріплені в документах.

Таким чином, у контексті вище зазначеного, ми бачимо, що однією з головних проблем забезпечення кібербезпеки в сучасному інформаційному просторі України є брак нормативної бази. Не було зроблено головного - країна і суспільство перейшли у нове сторіччя, у кіберпростір, проте не підготували у свій час відповідних інструкцій та фахівців. Можемо зробити висновок, що Закон «Про основні засади забезпечення кібербезпеки України» має стати першим кроком для подальших значно конкретніших дій у цій сфері. Має бути розроблена низка підзаконних актів, які детальніше регулюватимуть заходи з кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Лисичкин В.А, Третя світова інформаційно-психологічна війна. М.: Ваклер, 2009, с. 265.

2. Закон України «Про основні засади забезпечення кібербезпеки України», документ 2163-19, прийняття від 05.10.2017

3. Крутских А., Федоров А. Про міжнародну інформаційну безпеку / Крутских А., Федоров А. // Міжнародне життя. 2000, № 2, С. 43.

УДК 681.518.54

Зозуля О.Ф. студент гр. УБіт-14-1
Науковий керівник: Мєшков В.І., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У МІСТІ ДНІПРО

Останніми десятиріччями у світі спостерігається стійка тенденція до зростання кількості надзвичайних подій різного походження. Щодня світові ЗМІ повідомляють про природні й техногенні катастрофи, збройні конфлікти, терористичні акти, тяжкі злочини, вчинені і злочинними організаціями, і окремими особами, акти піратства на морі тощо. І дедалі частіше в результаті таких надзвичайних подій жертвами стає велика кількість людей, а життєве важливим для існування держав системам, об'єктам і ресурсам завдається серйозна шкода [1].

На засіданні верховної ради 5 жовтня 2017 року, було прийнято Закон про основні засади кібербезпеки України.

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [2].

Згідно новому закону: критично важливі об'єкти інфраструктури (далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [2].

Також розглянемо визначення поняття: об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [2].

З-поміж загроз критичній інфраструктурі називають пандемії, промислові аварії, терористичну та злочинну діяльності, кібератаки, стихійні лиха тощо. Держава має забезпечувати захист об'єктів критичної інфраструктури від усіх суттєвих загроз, які можна віднести до трьох категорій: техногенні, природного характеру та соціально-політичні [1].

Оскільки на даний момент по відношенню до України проявляється агресія (зона АТО), то можливе ведення диверсійної війни на території міста Дніпро. Мета диверсійної війни в проведенні спеціальних операцій по виведенню з ладу (пошкодження, руйнування, підпал, підрив та інше) критично важливих об'єктів. Наприклад гучного резонансу набула серія вибухів, вчинених у Дніпропетровську 27 квітня 2012 р. (постраждало 29 осіб). Прокурором Дніпропетровської області порушено кримінальну справу за частиною 2 ст. 258 КК (терористичний акт). Терористичні акти завжди мають значний резонанс. Однак при цьому не слід забувати про те, що техногенні аварії часто можуть мати наслідки тяжчі, ніж у випадку деяких терактів. Наприклад, вибух природного газу в 10-поверховому будинку у Дніпропетровську, що

став- ся 13 жовтня 2007 р., забрав життя 23 людей (у т.ч. семи дітей). Кримінальну справу було порушено за ст. 367 КК (службова халатність), а на лаві підсудних опинилися три представника ВАТ «Дніпрогаз» – генеральний директор, його перший заступник і головний інженер.[1]

З наведених вище прикладів робимо висновок, що об'єкти критичної інфраструктури міста Дніпро повинні надавати більшого значення загрозам терористичних атак.

На підтвердження даної думки можна привести наступну інформацію:

Президент України Петро Порошенко прийняв в дію рішення Ради національної безпеки і оборони "Про вдосконалення заходів забезпечення захисту об'єктів критичної інфраструктури ". Про це йдеться в указі Президента №8 від 16 січня. Цим рішенням від 29 грудня 2016 року РНБО доручив Кабінету Міністрів впродовж 2 місяців розробити і прийняти концепцію створення державної системи захисту критичної інфраструктури і план заходів що до їх реалізації.

На території міста Дніпро знаходяться та функціонують наступні об'єкти критичної інфраструктури:

- ДТЕК Дніпрообленерго;
- Південний машинобудівний завод імені О.М. Макарова;
- ПАО "Дніпротяжмаш";
- ПАО "Дніпровський агрегатний завод",

та багато інших підприємств, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторі.

Надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я.

Або є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню.

ВИСНОВОК

На території міста Дніпро діє велика кількість критично важливих об'єктів. Безпека яких є пріоритетною задачею державних служб та відомств. Прийняття Закону про основні засади кібербезпеки України – це великий крок до зміцнення безпеки об'єктів критичної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Аналітична доповідь: «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні», автор Бірюков Д.С., Кондратов С.І.

2. Закон України «Про основні засади забезпечення кібербезпеки України», документ 2163-19, прийняття від 05.10.2017.

УДК 004.42 + 531.1 + 53.087.252 + 531.355

Якунін Є. О., к.ф-м.н., доцент кафедри фізики
Журавльов М. О., старший викладач кафедри фізики
Курнат Н. Л., старший викладач кафедри фізики
(*Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)*

МОДЕЛЮВАННЯ ВІЛЬНОГО ПАДІННЯ ТІЛА У ФІЗИЧНОМУ ЛАБОРАТОРНОМУ ПРАКТИКУМІ

У цій роботі представлена програма, що моделює процес руху тіла, кинутого під кутом до горизонту. Наведено математичне обґрунтування моделі, як без урахування, так і з урахуванням опору середовища. Запропоновані варіанти використання програми в лабораторному практикумі для дистанційного курсу фізики.

Для дистанційного вивчення курсу фізики будуть корисними «комп'ютерні» лабораторні роботи, тобто моделювання реального фізичного процесу, що вивчається, за допомогою обчислювальної техніки.

Представлена програма розроблена в середовищі Visual C++ на основі діалогового застосування. Об'єктна структура моделі включає об'єкт класу Ball, що має такі властивості як радіус, колір, координати, проекції швидкостей на координатні осі. Об'єкт цього класу забезпечений функціями, що дозволяють відображати його на екрані, змінювати значення його координат і швидкості (моделювати рух).

Як об'єкт проекту використовується стек, що доповнюється об'єктом класу Ball при кожному спалаху стробоскопа для запам'ятовування поточного положення кулі. Цей стек використовується при відображенні фотографії з фіксованими положеннями кулі.

Таким чином, в розробленій програмі моделюється рух тіла, кинутого під кутом до горизонту, шляхом розв'язання рівняння руху методом кінцевих різниць:

$$m\frac{d\vec{v}}{dt} = m\vec{g}$$

$$\Delta v_y = -g \cdot \Delta t\,;\; v_y' = v_y + \Delta v_y$$

$$\Delta x = v_x \cdot \Delta t\,; \qquad \Delta y = v_y \cdot \Delta t\,; \qquad x' = x + \Delta x\,; \qquad y' = y + \Delta y\,.$$

У програмі передбачена можливість враховувати сили опору повітря. В цьому випадку рівняння руху прийме вигляд:

$$m\frac{d\vec{v}}{dt} = m\vec{g} + \vec{F}_c\,.$$

У цій моделі було прийнято розмір тіла (кулі) порядку d = 0,1 м, середня швидкість біля v = 10 м/с, щільність повітря ρ = 1,2 кг/м^3, динамічна в'язкість повітря η = 1,8 Па с.

Оцінимо число Рейнольдса:

$$R_e = \frac{\rho v d}{\eta} \approx 10^5\,.$$

При такому значенні числа Рейнольдса основний вклад в силу опору вносить не сила в'язкого тертя, а сила лобового опору, що визначається за формулою

$$F_c = C_x \frac{\rho v^2}{2} S\,,$$

де C_x – коефіцієнт форми, який для кулі дорівнює $0{,}5$; $S = \pi r^2$ – площа поперечного перерізу кулі.

З урахуванням цього рівняння для приросту проекцій швидкостей тіла приймуть вигляд:

$$\Delta v_x = -C_x \frac{\rho v}{2} v_x \frac{3}{4 r \rho_ш} \Delta t ; \qquad \Delta v_y = -g \cdot \Delta t - C_x \frac{\rho v}{2} v_y \frac{3}{4 r \rho_ш} \Delta t$$

$\rho_ш$ – щільність матеріалу кулі, r – радіус кулі.

При моделюванні роботи стробоскопа з регульованою частотою спалахів «фотознімок» (результат роботи стробоскопа) виводиться на друк і на екран (Рис. 1).

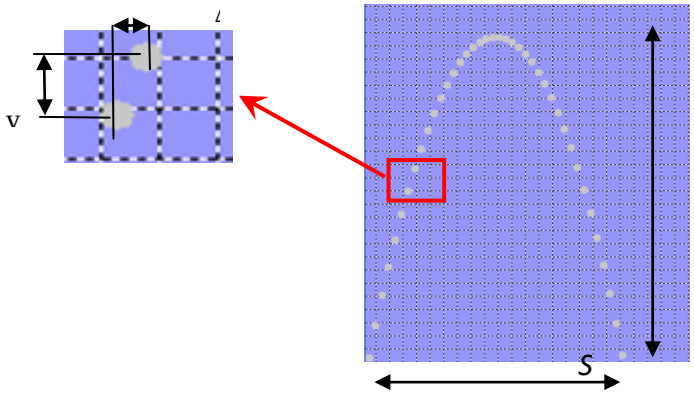

Рисунок 1- Відображення положення тіла за допомогою стробоскопа.

На «фотознімок» накладається координатна сітка в масштабі з кроком 20 метрів. По максимальній висоті підйому на «фотознімку» можемо визначити вертикальну проекцію початкової швидкості:

$$v_{0y} = \sqrt{2 g h_m} .$$

Визначивши максимальну дальність польоту, знаючи число спалахів N і інтервал Δt між ними, можна розрахувати горизонтальну проекцію початкової швидкості:

$$v_{0x} = \frac{S_m}{N \cdot \Delta t} .$$

Можемо приблизно розрахувати швидкість на кожному інтервалі часу між спалахами:

$$v_x = \frac{\Delta x}{\Delta t} ; \qquad v_y = \frac{\Delta y}{\Delta t} .$$

За цими даними можна побудувати залежності вертикальної проекції швидкості від часу і модуля швидкості від висоти.

Можемо також у разі врахування сили опору оцінити розмір кулі і щільність матеріалу кулі. Для цього необхідно розрахувати для декількох тимчасових інтервалів горизонтальні проекції швидкості. Потім, визначивши зміну горизонтальної проекції швидкості для різних тимчасових інтервалів, скласти для цих інтервалів наступний вираз

$$\frac{\Delta v_x}{\Delta t} = C_x \frac{3 \rho v v_x}{4 \cdot 2 \cdot r \rho_ш} .$$

Звідси можна виразити добуток щільності матеріалу кулі на його радіус для декількох точок траєкторії кулі:

$$r \rho_ш = C_x \frac{3 \rho v v_x \cdot \Delta t}{4 \cdot 2 \cdot \Delta v_x} .$$

Цей алгоритм розрахунку наочно показує і пояснює рух тіла, що вільно падає, без урахування і з урахуванням сил тертя (або опору).

УДК 007.51

Ковальова Ю.В., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ МОНІТОРИНГУ

Сучасні тенденції, спрямовані на розвиток розподілених систем управління, вказують, що незважаючи на значні успіхи в області безпеки АСКОЕ, недостатня увага приділяється питанням захисту та безпеки бездротових сенсорних мереж [1]. У зв'язку з цим набуває значення ступінь уразливості мереж енергозабезпечення, порушення цілісності яких несе за собою колосальний економічний і соціальний збиток на державу в цілому.

Для бездротових мереж моніторингу основною метою безпеки є збереження конфіденційності, гарантія недоторканності і забезпечення доступності інформації. Для того щоб вжити заходів для захисту розгорнутої мережі необхідно провести оцінку основних видів загроз безпеки. Загрози конфіденційності на рівні передачі комерційної та технологічної інформації можуть принести серйозної шкоди. За ступенем важливості виділяються атаки за допомогою яких визначається несуча частота, розмір повідомлення, рівень сигналу і відомості про маршрутизації інформації.

Ці дані виходять за допомогою мережевого сніфферу, який здійснює прослуховування інформації про маршрутизації даних. Зловмисники можуть встановити голкові контакти з кожного боку чіпа інтелектуального лічильника, щоб перехоплювати і аналізувати електричні сигнали для розуміння програмної начинки пристрою. Аналогічним чином можуть бути перехоплені і радіосигнали.

Дослідниками [2] було встановлено, що в поширених інтелектуальних лічильниках можливо провести реверс-інжиніринг комунікаційних протоколів, а також атаки типу «маскарад» (spoofing). Це дозволяє втручатися в роботу лічильника, спотворювати показання і керувати ним. Атаки типу «маскарад» призводять до втрати цілісності даних і їх спотворення. В системах інтелектуального обліку не передбачена аутентифікація. Крім того, перевірка на вході також відсутня. При отриманні кількох пакетів з однаковим ID і різними показниками лічильника, зчитувач приймає пакет з найсильнішим сигналом. При використанні більш сучасної моделі зчитувача, який виробляє таку перевірку, існує можливість простого блокування пакетів з легітимного лічильника і перенаправлення зчитувача на прийом пакетів з підставного пристрою.

Одним з можливих рішень захисту інтелектуальних лічильників є Smartsynch Universal Communications Model – модель інтелектуального лічильника в збірці, що дозволяє замінювати застарілі контролери на нові, що підтримують аутентифікацію і шифрування, без необхідності видалення з мережі лічильника.

При вивченні схеми проходження трафіку сенсорної мережі можна простежити розташування базової станції або іншого стратегічно розташованого вузла. Більш того, протоколи маршрутизації многоскачкового зв'язку надають можливість зловмиснику простежити весь потік повідомлень і визначити джерело інформації. Будь-який аналіз мережевого трафіку або декодування пакетів може бути здійснений в реальному часі, або в режимі офлайн (при відсутності підключення) за допомогою наявної бази даних

описів пакетів. Більшість бездротових атак підпадають під одну з наступних категорій [3]:

- Атаки на конфіденційність: дані атаки намагаються перехопити секретну інформацію, що надсилається засобами бездротової передачі.
- Атаки на недоторканність: дані атаки посилають фрейми (структурні одиниці інформації) помилкового контролю, управління або містять дані для виникнення збою на одержувача, або використовуються для полегшення проведення іншого типу атак.
- Атаки на доступність: ці атаки перешкоджають доставці бездротових повідомлень для легалізації користувачів за допомогою виводу з ладу мережевих ресурсів.

Формування неправдивих команд локальної автоматики, в загальному випадку, може привести до аварійної ситуації, так як віддалене управління в більшості випадків зводиться тільки до зміни налаштувань, що призводить до неоптимального режиму роботи обладнання.

Найбільш вірогідним є загрози трафіку, які полягають у введенні шкідливої зайвої інформації в мережу, поява «лавини» повідомлень. Даний вид погроз може привести до збільшення затримок при передачі даних або до втрат пакетів, що призведе до недостовірної оцінки стану об'єкта і, відповідно, призведе до можливості прийняття катастрофічних рішень.

Для випадку системи моніторингу та управління об'єктом, втрата якості управління E оцінюються формулою:

$$E = (1 - B) * N_A * z_e$$
$$B = N_S / N_A \qquad (1.1)$$

де *ze* – середнє значення збитку при втраті одного абонента;

NS – кількість обслужених абонентів за час експлуатації;

NA – загальна кількість даних абонентів в системі за час експлуатації.

Система повинна забезпечити виконання умови:

$$B \geq B_{tr} \qquad (1.2)$$

де *B, Btr* – відповідно поточний і необхідний баланс споживання в системі.

Втрата пакетів від кінцевих вузлів *D* досягається зловмисником двома основними способами:

- введення сенсора SD рівня кінцевих вузлів, який проводить DDOS-атаку;
- введення сенсора SM рівня маршрутизаторів, який порушує роботу механізму маршрутизації.

Введення в систему зловмисником вузла SD призводить до збільшення навантаження на маршрутизатор і не здатності виконувати задані функції. Поява вузла *SM* призводить до втрати даних кінцевих сенсорів, підключених до даного маршрутизатора. Одним з ефективних способів боротьби з даними видами атак є використання шифрування даних на різних рівнях і механізмів аутентифікації. При цьому необхідно враховувати обмеження, пов'язані з невеликими обчислювальними

ресурсами вузлів і невеликим об'ємом пам'яті. Це не дозволяє використовувати асиметричні алгоритми шифрування. Симетричні алгоритми шифрування володіють такими перевагами, як низькі вимоги до продуктивності вузлів і енергоспоживанню, мають низьку захищеність, пов'язану з тим, що, дізнавшись ключ, зловмисник може отримати доступ до всіх вузлів мережі.

Для боротьби зі складними і швидко зростаючими загрозами питання безпеки повинні бути ретельно розглянуті на кожному етапі розробки продукту - від проектування і тестування до установки і обслуговування. Для захисту важливих секторів інфраструктури необхідно забезпечити сучасні вимоги з безпеки для інсталяції захищених пристроїв і систем, готових протистояти найскладнішим атакам. Захист польових пристроїв «Інтернету речей» має пріоритетний характер, так як уразливі саме вони, а не встановлені на них додатки. Цим покладено новий етап в індустрії захисту інформації - захист мереж збору даних інтелектуальних датчиків і пристроїв обліку енергоресурсів, що володіють обмеженими обчислювальними ресурсами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Почта Ю.В. Управление энергоресурсами на базе беспроводных технологий передачи данных.- Materialy VIII mezinarodni vedecko-prakticka koference.-Dil 27 Technicke vedy, 20.01.2012-05.02.2012, Praha, s.78-81

2. 34 Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu, Rob Miller: Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems.- Proceeding CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security. Pages 462-473 . ACM New York, NY, USA ©2012

3. 35 Joe Biron and Jonathan Follett. - Foundational Elements of an IoT Solution.- Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA95472. Copyright ″ 2016 O'Reilly Media, Inc.

УДК 004.43

Скринник Д., студентка КаДЕТ гр. ПК14-1/9,
Науковий керівник: Козорог О.В.

МОВИ ПРОГРАМУВАННЯ LAD, STL, FBD ЛОГІЧНИХ КОНТРОЛЕРІВ В ПРОГРАМІ SIMATIC STEP 7

Одними з найважливіших функцій управління є облік результатів діяльності, їх аналіз і регулювання на їх основі діяльності програмістів. Слід зазначити, що в автоматизованій системі управління необхідно знати через яких помилок можуть виникнути проблеми у виробництві. Можливість запису сигналів надходять від датчиків і аналіз їх через великі проміжки часу. Розглянемо програмування логічних контролерів в програмі Simatic Step 7, що дозволяє написання програми на трьох мовах. Це такі як Lad, STL, FBD. Програмовані логічні контролери фірми Siemens – це промислові контролери і використовуються для автоматизації технологічних процесів. У нашому випадку це технологічна лінія, в якій працює більше десяти двигунів одночасно. Вся технологічна лінія повинна працювати, як єдиний механізм. Припустимо зменшилася швидкість на одній з машин - повинна зменшиться і на інших для продовження виробництва без його зупинки. Перед машинами стоять датчики, які контролюють стан металу, дійшов він чи ні. Натяг цільної заготовки металу між машинами.

Написання програми на одній мові недоцільно через те, що деякі функції можуть бути недоступні.

LAD (Ladder Diagram) – релейні діаграми. Редактор відображає програму в графічному поданні, схожому на електричну монтажну схему. Логічні схеми дозволяють програмі імітувати перебіг електричного струму від джерела напруги через ряд логічних умов на входах, які активізують умови на виходах. Джерелом напруги виступає шина, яка перебуває зліва.

FBD (Function Block Diagram) – функціональні блокові діаграми. Цей редактор відображає програму у вигляді звичайних логічних схем. Контактів немає, але є еквівалентні функціональні блоки. В даному редакторі не використовується поняття «потік сигналу», як в LAD, його висловлює аналогічне поняття потоку управління через логічні блоки FBD.

STL (Statement List) – список інструкцій. Даний редактор дає можливість створювати програми, вводячи мнемонічні позначення команд. У цьому редакторі можна створювати програми, які неможливо створити в редакторах LAD і FBD. Програмування в STL дуже схоже на програмування на Асемблері, кілька специфічне.

Переваги контролера:

- Контролер можна розташувати як в одному, так і в декількох щитах для зручності користування по поверхах.
- Навіть найпростіший контролер має високі інтелектуальні здібності, і може вирішувати мінімально необхідні завдання.
- Можливість використання як дешевого обладнання для виконання завдань з простими інтерфейсами, так і складного з відкритими інтерфейсами.
- Постійна пам'ять для зберігання програми.

Недоліки контролера:

- Якщо виходить з ладу процесор контролера або програма його роботи, то вся робота паралізується.
- Контролер – логічно купувати лише для багатозадачного використання, для виконання простих завдань на нього витрачається недоцільно.

УДК 004.056.53

Смолич Д.С., студент гр. 125м-16-1
Научный руководитель: Кручинин Александр Владимирович, ст. преп. кафедры безопасности информации и телекоммуникаций
(Государственное ВУЗ «Национальный горный университет», г. Днепр, Украина)

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ ДЕТЕКТИРОВАНИЯ ВРЕДОНОСНЫХ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

В данной работе рассматриваются виды вредоносных аккаунтов, риски и последствия их использования в социальных сетях. Также представлены результаты проведенного анализа существующих методов обнаружения и детектирования «социальных ботов».

Ключевые слова: боты, детектирование, обнаружение вредоносных аккаунтов, кластеризация, Captcha, Sms-verification, Ratelimit.

ВВЕДЕНИЕ

В настоящее время социальные сети – неотъемлемая часть большинства сфер жизни человека. Простое общение, поиск людей и необходимой информации, продвижение товаров и услуг, реклама, проведение бизнес-конференций и многое другое возможно в режиме онлайн, В социальных сетях ежедневно общается 40% населения планеты. Здесь сконцентрировано огромное количество информации и денег. Естественно, что некоторые стремятся использовать такие безграничные возможности для наживы и достижения своих далеко не благородных целей.

Одна из основных угроз на сегодняшний день – так называемые «социальные боты». [1] Это вредоносные программы, поддельные аккаунты, способные имитировать поведение людей. Как правило, боты используются для:

- организации информационных вбросов;
- массового хищения персональных данных;
- ухудшения доверия в соц.сетях;
- создания ложных новостей и голосований;
- как средство для легального бизнеса киберпреступности;
- создания проблем в социальном маркетинге.

Так, к примеру, при SMM продвижении в Вконтакте либо Facebook часть целевой аудитории это «мертвые» аккаунты или аккаунты-двойники, [4]

Угрожающие масштабы использования социальных ботов требуют создания эффективных алгоритмов их детектирования. Решением проблемы является развитие методов сетевого анализа, которые предназначены для выявления и кластеризации сообществ в соц.сетях, оценки их связности, степени доверия.

ВИДЫ «СОЦИАЛЬНЫХ БОТОВ»

Виртуальная (онлайн) социальная сеть – структура Интернет-среды, представленная электронными порталами, такими как «Одноклассники», «Вконтакте», «Twitter». «Facebook» и др. Узлами сети являются отдельные люди или организации, связанные корпоративными, политическими, служебными, семейными, дружескими взаимодействиями. Внутри сети образуются группы и сообщества с сильными стабильными связями, некая иерархия (рисунок 1), что позволяет их легко идентифицировать. [9]

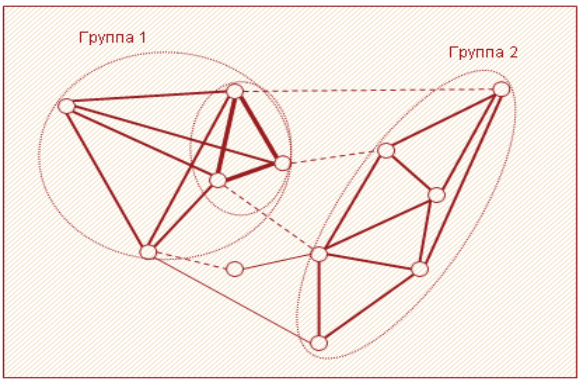

Рисунок 1 - Иерархия групп в соц. сетях.

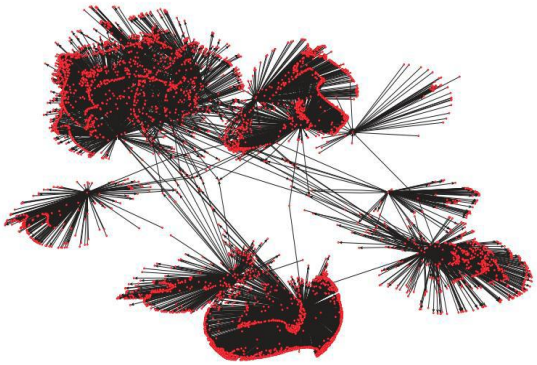

Рисунок 2 - График взаимосвязей пользователей в соц.сети.

Социальные боты классифицируются следующим образом;

1. Аватары – профили с хорошо налаженными социальными связями. [13]
2. Новостные боты – аккаунты, распространяющие как реальные, так и фейковые новости.
3. Боты для организации информационных вбросов, распространяя ложные сообщения реальных людей.
4. Игровые боты используются в играх для накрутки упоминаемости конкретных приложений.
5. Боты, участвующие в накручивании репутации для заработка денег на репостах.
6. Аккаунты, публикующие чужие новости и перепосты.

Основная сложность при детектировании вредоносных аккаунтов – отличить реальных ботов от людей, похожих по поведению на боты.

МЕТОДЫ ДЕТЕКТИРОВАНИЯ БОТОВ

Основой в разработке современных методов выявления вредоносных аккаунтов стал принцип распознавания образов. Научная дисциплина позволяет классифицировать объекты, основываясь на «прецедентах» - образах, правильная классификация которых известна. В зависимости от наличия или отсутствия прецедентной информации различают классификацию с обучением и без обучения (кластеризация).

Существующие алгоритмы по борьбе с ботами являются скорее профилактическими:

- Captcha – автоматизированный тест Тьюринга, определяющий, является пользователь компьютером или человеком.
- Sms-verification – проверка пользователя посредством отправки смс с кодом подтверждения.
- Ratelimit – временное ограничение числа запросов к системе.

Задача классификации – разбиение множества объектов или наблюдений на априорно заданные группы, называемые классами. Внутри каждой из которых они предполагаются похожими друг на друга, имеющими одинаковые признаки и свойства. Если количество классов не более двух, имеет место бинарная классификация. Для классификации сложных моделей применяются традиционные алгоритмы.

К примеру, для исследования проблемы обнаружения спам-ботов в Twitter разработчики применили нейронные сети, деревья решений, машины опорных векторов, наивный байесовский классификатор. [6] и [14]. В качестве признаков использовалось количество подписчиков и читаемых, а также граф-ориентированные взаимосвязи. (рис 2.)

Общий подход при создании алгоритма детектирования социальных ботов (проектирование фреймворка) [7] включает в себя:

- сбор данных;
- выявление признаков (метрик);
- выборка классифицированных данных для обучения классификатора;
- обучение классификатора на данной выборке.

Проблема различения аккаунтов на человека, бота и киборга [13] решается с помощью создания обширной базы аккаунтов и классификации по различным признакам: поведению, содержанию публикаций, характеристик профиля. В результате формируется система, состоящая из 4 частей:

- компонент энтропии (entropycomponent) – анализирует интервал между сообщениями аккаунта;
- компонент обнаружения спама (spamdetectioncomponent) – анализирует содержание сообщений по заданным шаблонам;
- компонент анализа профиля (accountpropertiescomponent) – анализирует признаки профиля;
- компонент классификации (decisionmarkercomponent) – классификация аккаунта на результатах предыдущих компонентов.

Одними из эффективных классификаторов являются:

- алгоритм приманки (Honeypot) [12];
- анализ маштабограмм (scalogram) [15];
- математический алгоритм Байеса, классификатор, основанный на теореме Байеса[18].

Современные разработчики алгоритмов детектирования ботов используют методики, учитывающие особенности контента, краудсорсинг, технологии сетей [17] и многие другие характеристики и признаки аккаунтов социальных сетей, создавая все более универсальные классификаторы.

ВЫВОДЫ

В ходе проведения обзора методологии детектирования социальных ботов были проанализированы наиболее эффективные способы обнаружения, классификации и борьбы с вредоносными аккаунтами. Рассмотрены основные принципы распознавания образов, достоинства и недостатки популярных классификаторов. Увы, имеют скорее профилактический характер. Современные тенденции широчайшего использования социальных сетей в различных сферах требуют создания более гибких и универсальных моделей для распознавания вредоносных программ.

ПЕРЧЕНЬ ИСТОЧНИКОВ

1. Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu. The Socialbot Network: When Bots Socialize for Fameand Money / University of British Columbia Vancouver, Canada, 2011. – 1 с.
2. Korrespondent.net – Продажа ботов в Twitter стала многомиллионным бизнесом – исследование. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: https://korrespondent.net/business/web/1540808-prodazha-botov-v-twitter-stala-mnogomillionnym-biznesom-issledovanie (дата обращения 15.11. 2017)
3. Carlo De Micheli, Andrea Stroppa. Twitter and the underground market / 11th Nexa Lunch Seminar, May, 2013.— 5–9 с.
4. Topmarketing.by – Честное SMM-продвижение, выявляем аккаунты-боты в социальных сетях. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://topmarketing.by/internet-marketing/chestnoe-smm-prodvizhenie-vyyavlyaem-akkaunty-boty-v-socialnyx-setyax.html (дата обращения 14.11. 2017)

5. Cossa.ru – Использование ботов (технических аккаунтов) в работе с отзывами. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://www.cossa.ru/155/12121/ (дата обращения 12.11. 2017)

6. Alex Hai Wang. Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach / College of Information Sciences and Technology The Pennsylvania State University, USA, 2010. — 2–10 с.

7. R. Nithin Reddy, Nitesh Kumar. Automatic Detection of Fake Proles in Online Social Networks / Department of Computer Science and Engineering National Institute of Technology Rourkela, Orissa, India, May, 2012. — 10–15 с.

8. Inosmi.ru – Бот в твиттере оказался настолько убедительным, что люди начали сочувствовать «ей». [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://inosmi.ru/world/20120627/194149517.html (дата обращения 15.11. 2017)

9. Basegroup.ru, BasegroupLabs – Введение в SocialMining. [Электронный ресурс]: [Веб-сайт]. – Режим доступа: http://www.basegroup.ru/library/web_mining/introduction_in_social_mining (дата обращения 16.11. 2017)

10. Wikipedia.org. Сводная энциклопедия – Кластерный анализ. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Кластеризация (дата обращения 15.11. 2017)

11. Wikipedia.org. Сводная энциклопедия – Задача классификации. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Задача_классификации (дата обращения 15.11. 2017)

12. Securitylab.ru SecurityLab – Технология Honeypot. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://www.securitylab.ru/analytics/275420.php (дата обращения 13.11. 2017)

13. Zi Chu, Steven Gianvecchio, Haining Wang, SushilJajodia. Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? / IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2012. – 2-10 с.

14. Alex Hai Wang. DON'T FOLLOW ME: SPAM DETECTION IN TWITTER / College of Information Sciences and Technology, The Pennsylvania State University, Dunmore, USA, 2012. – 2-7 с.

15. Wikipedia.org. Сводная энциклопедия – Scaleogram. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Scaleogram (дата обращения 11.11. 2017)

16. Wikipedia.org. Сводная энциклопедия – JSON. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/JSON (дата обращения 11.11. 2017)

17. J. Ratkiewicz, M. D. Conover, M. Meiss, B. Gonc¸alves, A. Flammini, F. Menczer. Detecting and Tracking Political Abuse in Social Media / Center for Complex Networks and Systems Research School of Informatics and Computing Indiana University, Bloomington, IN, USA, 2011. — 2-5 с.

18. Wikipedia.org. Сводная энциклопедия – Теорема Байеса. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Теорема_Байеса (дата обращения 12.11. 2017)

19. Ibm.comПрограммное обеспечение IBM – Анализ социальных сетей – техническая публикация. [Электронный ресурс]: [Веб-сайт]. – Режим доступа: http://public.dhe.ibm.com/software/dw/ru/download/ZZW03070.pdf (дата обращения 15.11. 2017)

20. Haijian Shi. Best-first Decision Tree Learning / The university of Waikato, Hamilton, NewZealand, 2007. — 5 с.

21. Wikipedia.org. Сводная энциклопедия – Дерево принятия решений. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Дерево_принятия_решений (дата обращения 12.11. 2017)

УДК 004.01

Іващенко Д.С., студент гр. УБіт-14-1
Науковий керівник: Ковальова Юлія Вікторівна, асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

НАЦІОНАЛЬНІ ІНТЕРЕСИ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

На сьогодні Україна перебуває в умовах протиборства, в яких саме забезпечення інформаційної безпеки грає ключовий аспект в формуванні національних інтересів держави. В даній роботі розглянуто сучасний стан інформаційної сфери як пріоритетний напрямок національних інтересів України.

Ключові слова: національний інтерес, інформаційна сфера, загрози національній безпеці, політика розвитку.

ВСТУП

В сучасних умовах стрімкого розвитку технологічного світу саме інформаційний простір є невід'ємною складовою національної безпеки держави. На сьогодні інформаційна сфера представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин. Інформаційна сфера є системо утворюючим фактором життя суспільства та активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України.

ОСНОВНА ЧАСТИНА

Національний інтерес являє собою найбільш важливий орієнтир самостійної політичної діяльності національно орієнтованих сил в сфері державної влади та виступає в якості показника визначеності зовнішньої і внутрішньої політики країни [1].

Інформаційна сфера України перетворена на ключову арену протиборства. І саме гібридна війна, яка ведеться на нашій території протягом останніх років, призвела до втілення нових змін та перегляду національних інтересів Україні [2].

На основі національних інтересів України в інформаційній сфері формуються стратегічні та поточні завдання внутрішньої і зовнішньої політики держави щодо забезпечення інформаційної безпеки.

Відповідно до законодавства України [2] можна виділити чотири основні складові національних інтересів України в інформаційній сфері.

Перша складова національних інтересів України в інформаційній сфері полягає в дотриманні конституційних прав і свобод людини і громадянина в області отримання інформації і користування нею, забезпеченні духовного оновлення України, збереженні і зміцненні моральних цінностей суспільства, традицій патріотизму, гуманізму, культурного і наукового потенціалу країни.

Друга складова національних інтересів України в інформаційній сфері полягає в інформаційному забезпеченні державної політики України, доведенні до громадян України і міжнародної громадськості достовірної інформації про державну політику України, її офіційної позиції щодо соціально значущих подій в житті держави і міжнародного життя, із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів.

Третя складова національних інтересів України в інформаційній сфері полягає в розвитку сучасних інформаційних технологій, вітчизняної індустрії інформації, в тому числі індустрії засобів інформатизації, телекомунікації і зв'язку, забезпечення потреб

внутрішнього ринку її продукцією і вихід цієї продукції на світовий ринок, а також; забезпеченні накопичення, зберігання і використання вітчизняних інформаційних ресурсів. У сучасних умовах тільки на цій основі можна вирішувати проблеми створення наукоємних технологій, технологічного переозброєння промисловості, збільшення досягнень вітчизняної науки і техніки. Держава повинна зайняти гідне місце серед світових лідерів мікроелектронної і комп'ютерної промисловості.

Четверта складова національних інтересів України в інформаційній сфері полягає в захисті інформаційних ресурсів від технічних розвідок, несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем.

Відсутність цілісної системи інформаційно-аналітичного забезпечення органів влади і управління значно ускладнює прийняття ними виважених, науково обґрунтованих рішень, що породжує конфліктні ситуації у владних структурах і суспільстві.

Недостатнє, інформаційно-аналітичне забезпечення діяльності характерно для всіх державних органів - як на центральному, так і на регіональному рівнях. Владні структури не мають достатніх можливостей вчасно прогнозувати розвиток подій у державі та навколо неї, приділяє належну увагу сприятливі і обмежувати несприятливі фактори, що визначають результативність прийнятих політичних рішень.

Організація роботи інформаційно-аналітичних підрозділів досі не має системного характеру, а в періоди чергових скорочень чисельності державних органів діяльність деяких з таких підрозділів взагалі припиняється.

Руйнування інтелектуального потенціалу, неготовність системи освіти до підтримки процесів випереджального розвитку держави призводить до того, що з огляду на рівень розвитку цієї галузі за кордоном і той факт, що багато держав світу приділяють особливу увагу інформаційній безпеці (створення спеціальних органів і підрозділів для ведення інформаційних війн і т.п.), Україна досі не має достатньої кількості кваліфікованих фахівців, які б змогли на належному рівні ефективно протидіяти кожен ра більшої інформаційної активності іноземних партнерів в її інформаційному просторі.

ВИСНОВОК

Україна розпочала свій шлях до забезпечення цілісності та протистояння зовнішнім і внутрішнім загрозам. Зміна законодавчої бази є вагомим аспектом для майбутнього держави як в інформаційній сфері, так і в цілому. Але насамперед, основа інформаційної безпеки полягає у вірному виборі національних інтересів та пріоритетів щодо їх розвитку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Соловьев А.И.. Политология: Политическая теория, политические технологии: Учебник для студентов вузов. 2006

2. Доктрина інформаційної безпеки України, від 25 лютого 2017 року

УДК 004.056.5

Мохнін Микита Ігорович, студент гр. 125м-16-1,
Науковий керівник: Святошенко В.О., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕННЯ В РЕАЛЬНОМУ ЧАСІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

Ця стаття дає ознайомитися з вразливістю мереж та методом завдяки якому можна цьому запобігти.

Ключові слова **– Мобільний агент; Комп'ютерні мережі; Модель виявлення вторгнення**

ВСТУП

З мінливої індустрією телекомунікацій і зростанням популярності комп'ютеризованих додатків, велика кількість досліджень було проведено по застосуванню біологічно методів і систем на основі агентів систем комп'ютерного зв'язку, Мотивація даної роботи є дослідити, як біологічними методи в поєднанні з мобільним агентом можна використовувати електронну FFI ciently для розробки майбутніх поколінь систем виявлення вторгнень для комп'ютера комунікативних мереж.

ПРОПОНОВАНА МОДЕЛЬ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Запропонована модель заснована на поєднанні мобільних парадигм агента і біологічно натхненної методики, заснованої на парадигмі імунної системи людини. У нашій моделі для системного аудиту використовується секвенційний аналіз реєстрів журналів, а для цілей моніторингу використовується схема виявлення аномалій. Основні особливості нашої моделі IDS полягають в наступному:

- Модель виявлення аномалій.
- Архітектура на основі розподілених агентів і хостів.
- Компонент генерації відповіді.

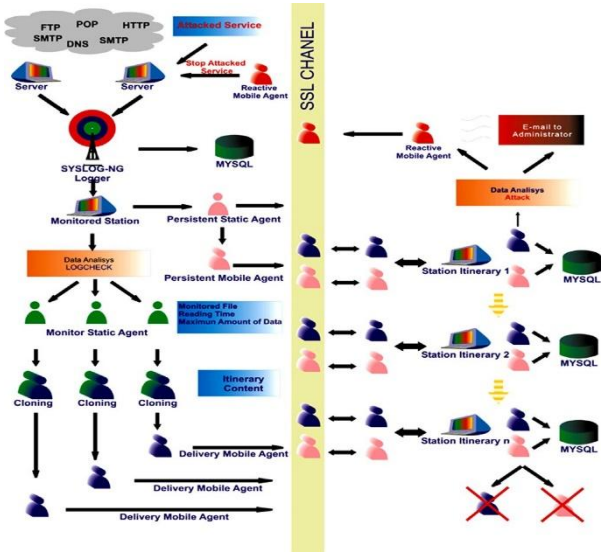

Рисунок 1. Схема моделі

На рисунку 1 зображені основні компоненти пропонованої моделі IDS, яка включає в себе не тільки служби FTP, DNS, HTTP, POP3 е SMTP, але також сервери, на

яких запущено інструмент генерації журналів (Syslog-ng), які відповідають для отримання реєстраційних операцій для різних серверів і сервісів і визначення їх відповідної функції генерації подій.

ЕКСПЕРЕМЕНТАЛЬНІ РЕЗУЛЬТАТИ

В даних експериментах ми розглянули зміни розміру агента, включаючи загальний час передачі в мережі з використанням різних смуг пропускання, тобто Ethernet 10 Мбіт / с, Ethernet 100 Мбіт / с і Ethernet 1000 Мбіт / с. Для кожного мережевого сценарію ми варіювали розміри сегмента агента від 0 КБ до 2000 КБ. Експерименти, які ми проводили, складаються в реєстрації часу передачі агентів між двома комп'ютерами з використанням декартового продукту між розміром агента і швидкістю мережі.

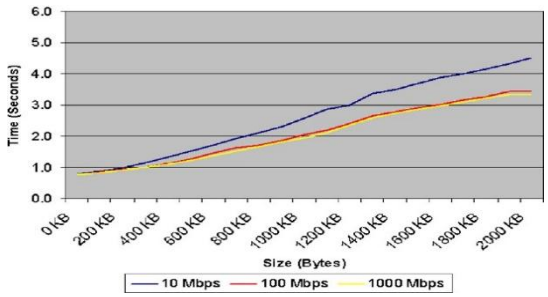

Рисунок 2. Ефективність передачі

На рисунку 2 зображено ефективність передачі агента, змінюючи розміри агентів і швидкість мережі, використовуючи сокет без SSL в якості моделі зв'язку. Як видно, наші результати показують, що продуктивність агента в повному обсязі лінійні, оскільки мережі Ethernet 100 Мбіт / с і 1000 Мбіт / с показують аналогічну продуктивність для передачі агента, в той час як 10 Мбіт / с демонструють аналогічну поведінку в початкових сегментах, а потім значно погіршуються. Щоб довести ці спостереження, було застосовано статистичний метод Круськала-Уолліса для груп результатів, отриманих в інтервалі [0 КВ, 2000. КБ] при використанні декількох значень передачі (10 Мбіт / с, 100 Мбіт / с і 1000 Мбіт / с) з 95% -ним інтервалом узгодження.

ВИСНОВКИ

У цій роботі була розроблена модель виявлення вторгнень, засновану на парадигмі імунної системи людини, та показано, як біологічно натхненні методи в поєднанні з технологіями мобільних агентів можуть поліпшити безпеку складних комп'ютерних комунікаційних мереж, а також те, як ці методи можуть бути використовується для розробки майбутніх поколінь систем виявлення вторгнень для комп'ютерних мереж зв'язку. Дана система виявлення вторгнень і комунікацій на основі реального часу заснована на хості і використовує парадигму виявлення аномалій.

ПЕРЕЛІК ПОСИЛАНЬ

1. A. Boukerche, K.R.L. Jucá, J.B.M. Sobral, M.S.M.A. Notare, Biological inspired based intrusion detection models for mobile telecommunication systems, in: IEEE Proceedings of the Int'l Parellel and Distributed Processing Symposium and Workshops, 2015.

2. J. Kim, P. Bentley, Evaluating negative selection in an artificial immune system for network intrusion detection, in Proceedings of the Genetic and Evolutionary Computation Conference, pp. 1330–1337, 2016.

3. Central loghost mini how to. http://www.campin.net/newlog-check.html#newlogcheck/, 2016.

УДК 004.056.53

Кучер Ростислав Юрьевич, студент гр. 125м-16-1,
Научный руководитель Кручинин А.В., ст. преп. кафедры безопасности информации и телекоммуникаций
(Государственное ВУЗ «Национальный горный университет», г. Днепр, Украина)

СПОСОБЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ЗАПУСКА ПРИЛОЖЕНИЙ С USB-УСТРОЙСТВ

В данных тезисах анализируются способы защиты от несанкционированного доступа в компьютерные системы по USB-каналу, особенности их работы, разработка рекомендаций, которая удовлетворит большинству запросам безопасности.

Ключевые слова: кибербезопасность, операционная система, взлом, Windows, USB.

ВВЕДЕНИЕ

В операционной системе Windows 95 существует функция автозапуска. Целью данного инструмента было упрощение запуска и установки приложений, программного обеспечения и драйверов устройств не квалифицированными пользователями и для уменьшения количества звонков в службу поддержки. Когда записанный особым образом диск вставляли в привод, система Windows определяла наличие специального файла с инструкциями. Но эта функция открыла возможность злоумышленнику модифицировать устройство переносного хранения информации и установить набор инструкций для получения прав администратора с целью хищения, изменения или удаления информации в системе[6].

СПОСОБЫ ЗАЩИТЫ ОС ОТ ВЗЛОМА С ПОМОЩЬЮ USB-НАКОПИТЕЛЕЙ

За реализацию функции автозапуска в Windows системах ответственен файл autorun.inf, с помощью которого злоумышленники достаточно эффективно обходили защиту системы. Компании Microsoft пришлось избавиться от этой функции и уже через 3 месяца после отключения автозапуска, количество атак, использующих его в Windows XP и Vista, снилось на 1.3 миллиона. Теперь, начиная с Windows 7, этот функционал отключен по умолчанию. Это является одним из способов защиты ОС от взлома с помощью ЮСБ носителей. На сегодняшний день, актуальный следующие способы защиты[1,7]:

1. Физическое отключение портов.
2. Отключение портов в BIOS/UEFI.
3. Удаление драйверов контроллера USB[5,8].
4. Блокировка отдельных устройства USB.
5. Ограничение прав на чтение файлов usbstor.inf и usbstor.pnf в каталоге \Windows\Inf.
6. Контроль подключений устройств с использованием дополнительного ПО[4,5].

СРАВНЕНИЕ СПОСОБОВ ЗАЩИТЫ

Для сравнения представленных способов предлагается использовать следующие основные критерии:

- удобство – комфорт работы с примененной мерой защиты;
- простота – соотношение количества ресурсов и времени, необходимых для установки и настройки;
- надежность – насколько хорошо меры безопасности могут защитить от взлома.

Так использование способа редактирования реестра, позволяет заблокировать возможность использования USB-накопителей, однако при этом сканеры, клавиатура, мышь и подобное оборудование продолжит свою роботу. Кроме этого, ошибочные действия могут повлечь повреждение системы. Отключение устройств в диспетчере более удобно, однако очень ненадежно и требует времени для полной реализации. Также неоднозначен и способ с удалением драйверов. Система всегда будет пытаться восстановить свой функционал. Подключая USB-устройство, система проверит наличие драйвера и при их отсутствии предложит установить драйвер. Это в свою очередь откроет доступ к USB-устройству. При физическом отключении на материнской плате кабеля, может заблокировать только переднюю панель, при этом остается активной задняя панель. Необходимо заблокировать доступ к задней панели системного блока, иначе защита не имеет смысла. Ограничение прав на чтение файлов usbstor.inf и usbstor.pnf способ делегирования с правами NTFS. Если невозможно обратиться к этим файлам в ограниченной учетной записи, то не будут подключаться флешки, но необходимо удостоверится что пользователь не получит возможности перемещения файлов в другое место. Способ подключения устройств по USB с использованием дополнительного ПО предлагает сохранить разрешенные флешки по номеру тома (VSN) [2,3]. Существует возможность использовать кремниевые диоды с встречно-параллельным включением. Каждый такой диод понизит напряжение на 0,7 В. В некотором роде это можно использовать в защитных целях, принудительно понижая ток.

На основе выполненного анализа, была составлена сравнительна таблица. В этой таблице критерии ранжируются от 1 до 3.

Таблица 1. Сравнения способов защиты:

Способ	**Критерии**		
	Надежность	**Простота**	**Удобство**
Редактирование реестра	2	3	2
Диспетчер устройств	1	3	3
Удаление драйверов	2	1	2
Физическое отключение	3	2	2
Ограничение прав на чтение файлов	2	3	2
Контроль подключений устройств с помощью доп. ПО	1	1	2

Полученные результаты позволяют выбрать способ или группу способов защиты наиболее подходящих для решения конкретных задач. В большинстве случаев, используя редактирование реестра и контроля подключения устройств с помощью доп. ПО, можно добиться достаточно высокого уровня защиты ОС от взлома с помощью USB-накопителей.

ВЫВОДЫ

В данной работе рассмотрен вопрос о способах реализации несанкционированного доступа с использованием USB-устройств к компьютерной системе под управлением ОС Windows, первопричинах появления данной уязвимости. Выполнен анализ существующих способов защиты, предложены критерии и выполнена их оценка. Предложены рекомендации по выбору способов защиты.

СПИСОК ИСТОЧНИКОВ

1. Википедия: Несанкционированный доступ [Электронный ресурс] – [Веб-сайт]- Режим доступа: https://uk.wikipedia.org/wiki/Несанкціонованийдоступ

2. Способы блокировки клавиатуры ноутбука [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://wd-x.ru/kak-zablokirovat-klaviaturu-na-noutbuke/

3. Способы обхода паролей BIOS [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://habrahabr.ru/post/128466/

4. DeviceLock 5.61: периферия под контролем [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.osp.ru/winitpro/2004/07/177240/

5. Вскрываем Windows. Легкие способы получить права админа на рабочем компьютере [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://xakep.ru/2016/09/29/bypassing-office-pc-restrictions/

6. Чем UEFI лучше обычного BIOS и каковы отличия [Электронный ресурс] – [Веб-сайт] - Режим доступа: http://vindavoz.ru/poleznoe/128-chem-uefi-luchshe-obychnogo-bios-i-kakovy-otlichiya.html

7. Википедия: Доверенная загрузка [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://ru.wikipedia.org/wiki/Доверенная_загрузка_(аппаратные_средства)

8. Википедия: Ubuntu [Электронный ресурс] – [Веб-сайт] - Режим доступа: wiki.ubuntu.com/Security/Features.

9. ShmooCon 2011: USB Autorun attacks against Linux [Электронный ресурс] – [Веб-сайт] - Режим доступа: youtube.com/watch?v=ovfYBa1EHm4.