УДК 004.056.53(045) **Юдін О.К, Коновалов Е.О., Рогоза І.Є.**

МЕТОДИ ВИЯВЛЕННЯ АТАК ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ АВТОМАТИЗОВАНИХ СИСТЕМ

Вступ

Проблема захисту ресурсів інформаційно-комунікаційних систем та мереж (ІКСМ), стає ще більш актуальною у зв'язку з розвитком і поширенням глобальних обчислювальних мереж, територіально розподілених інформаційних комплексів та систем з віддаленим управлінням доступом до інформаційних ресурсів.

Вагомим аргументом для підвищення уваги до питань безпеки ІКСМ є бурхливий розвиток програмно-апаратних методів та засобів, здатних потай існувати в системі і здійснювати потенційно будь-які несанкціоновані дії (процеси), що перешкоджає нормальній роботі користувача й самої системи та безпосередньо завдає шкоди властивостям інформації (конфіденційності, доступності, цілісності).

Незважаючи на розробку спеціальних програмно-апаратних засобів захисту від впливу загроз інформаційним ресурсам автоматизованих систем, кількість нових методів реалізації атак постійно зростає. Зазначений вплив може бути реалізовано технічно або організаційно, тільки в тому випадку, коли відома інформація про принципи функціонування ІКСМ, її структуру, програмне забезпечення, тощо.

На даний час існує декілька класичних визначень поняття *"атака"* (вторгнення, напад) на інформаційну систему та її ресурси. Даний термін може визначатись, як процедура вторгнення, що приводить до порушення політики безпеки або дія (процес), що приводить до порушення цілісності, конфіденційності й доступності інформації системи. Однак, більш поширене трактування, безпосередньо зв'язано з терміном «уразливість», або «можливість реалізації загрози». Під атакою (attack, intrusion) на інформаційну систему, будемо розуміти - дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційним ресурсам ІКСМ, шляхом використання уразливостей цієї інформаційної системи.

Постановка задачі

Базовими причинами порушення функціонування інформаційної системи є збої й відмови в роботі інформаційної системи, які частково або повністю перешкоджають функціонуванню ІКСМ, можливостям доступу до інформаційних ресурсів та послуг системи. Крім того, збої й відмови в роботі є однією з основних причин втрати даних.

Метою даною статті є аналіз методів реалізації загроз інформаційним ресурсам в ІКСМ, а також визначення характерних ознак реалізації різного класу атак. На основі проведеного аналізу необхідно визначити основні методи і засоби виявлення й ідентифікації існуючих загроз.

Аналіз існуючих методів реалізації атак

Існують різні методи класифікації атак. Наприклад, розподіл на пасивні й активні, зовнішні й внутрішні атаки, навмисні й ненавмисні. Однак, в даній статті, наведемо більш характерні типи атак на інформаційні системи та проведемо їх короткий опис реалізації й визначимо характерні ознаки [1,2].

- *Вилучене проникнення (remote penetration)*. Тип інформаційних атак, які дозволяють реалізувати вилучене керування комп'ютером користувача інформаційних ресурсів системи через мережу на базі віддаленого доступу. Прикладом такої програми є NetBus або BackOrifice.
- *Локальне проникнення (local penetration)*. Атака, що приводить до одержання несанкціонованого доступу до вузла ІКСМ, на якому вона запущена. Прикладом такої програми є GetAdmin.
- *Вилучена відмова в обслуговуванні (remote denial of service)*. Атаки, які дозволяють порушити функціонування інформаційної системи з умов реалізації її послуг або мають

можливість котрольованного перезавантаження системи шляхом віддаленого доступу. Прикладом такої атаки є Teardrop або trin00.

- *Локальна відмова в обслуговуванні (local denial of service).* Атаки, що дозволяють порушити функціонування системи або перевантажити систему, на якій вони реалізуються. Як приклад такої атаки, можна привести використання несанкціонованих апплетів, які завантажують центральний процесор нескінченним циклом, що унеможливлює обробку запитів інших додатків.
- *Мережні сканери (network scanners).* Програми, які аналізують топологію мережі й виявляють сервіси, доступні для атаки. Прикладом такої програми можна назвати систему nmap.
- *Сканери уразливостей (vulnerability scanners).* Програми, що здійснюють пошук уразливостей на вузлах мережі, що можуть бути використані для реалізації атак. Приклади: система SATAN або Shadow Security Scanner.
- *Зломщики паролів (password crackers).* Програми, які підбирають паролі авторизованих користувачів інформаційних ресурсів системи та її послуг. Прикладом зломщика паролів може служити несанкціоноване програмне забезпечення : L0phtCrack для Windows або Crack для Unix.
- *Аналізатори протоколів (sniffers).* Програми, які "прослуховують" мережний трафік. За допомогою цих програм можна автоматично відшукати таку інформацію, як ідентифікатори й паролі користувачів, інформацію про кредитні карти й т.д. Аналізатором протоколів можна назвати програмні продукти : Microsoft Network Monitor, NetXRay компанії Network Associates або LanExplorer.

Компанія Internet Security Systems, Inc. ще більше скоротила число можливих категорій атак на інформаційну систему, довівши їх до мінімуму [4]:

- збір інформації про характеристики ІС (Information gathering);
- спроби несанкціонованого доступу до інформаційних ресурсів системи (Unauthorized access attempts);
- відмова в обслуговуванні (Denial of service);
- підозріла активність (Suspicious activity);
- системні атаки (System attack).

Ознаки атак на інформаційну систему та її ресурси

Атаки на інформаційні ресурси системи та її послуги, можна виявити або знизити ризики їх реалізації, знаючи характерні ознаки несанкціонованих дій (НСД), а саме [3] присутність повтору певних подій у системі;

- неправильні або невідповідні встановленим процесам поточні ситуації та команди;
- використання уразливостей;
- невідповідні параметри мережного трафіка;
- непередбачені атрибути;
- непояснені проблеми;
- додаткові знання про порушення.

Стандартні засоби захисту інформаційних ресурсів системи (міжмережні екрани, сервери аутентифікації, системи розмежування доступу й т.п.) використовують у своїй роботі одну або дві ознаки, у той час як спеціалізовані системи виявлення атак, впроваджують для ідентифікації несанкціонованих дій практично весь зазначений перелік.

Повтор певних подій

Повтор певних подій, як процедура, використовується порушником при умові невдалих попередніх спроб вилучити потрібну інформацію про характеристики системи або авторизованого користувача. Прикладом таких дій може служити сканування портів у пошуку доступних мережних сервісів або підбор пароля.

Виявлення повторних подій — дуже потужний підхід до ідентифікації атаки. Даний метод дозволяє виявити атаки, що не підлягають стандартній класифікації та не мають фіксованих сигнатур. На даний час існує три основних методи виявлення повторів.

Контроль повторів, як граничних значень: даний метод засновано на статистичних правилах прийняття рішень при встановлених порогах ідентифікації атаки, що дозволяє відрізнити санкціоновані повтори від несанкціонованих. Несанкціоновані повтори можуть відповідати, як звичайним помилкам, так і реальним атакам. Неправильний вибір граничного значення статистичного порогу присутності атаки в системі, може привести або до проблеми пропуску атаки (false negative), або до проблеми так званої «фальшивої тривоги» (false positive).

Контроль повторів, як тимчасових інтервалів: зазначений метод формується на базі процедур виявлення процесу сканування портів, тобто контролю підлягає кількісне значення числа звертань до портів вузла за певний проміжок часу.

Контроль повторів, як шаблонів сигнатури: як шаблон сигнатури розглядається запит на встановлення з'єднання (посилка SYN-пакета). Повтор декількох запитів на встановлення з'єднання приведе до того, що черга вузла, з яким установлюється з'єднання, буде переповнений і вузол не зможе приймати нові запити від користувачів системи.

Неправильні команди.

Іншим методом ідентифікації несанкціонованої діяльності є виявлення неправильних запитів або відповідей, очікуваних від автоматизованих процесів або програм. Невідповідність заздалегідь очікуваним реакціям чи діям (процесам), дозволяє зробити висновок про підміну одного з учасників інформаційного обміну - або запитуючого інформацію, або того, хто формує відповіді на запити.

Використання уразливостей

Всі описи ознак атаки є ознаками уразливостей інформаційним ресурсам системи. З метою пошуку уразливостей інформаційної системи, використають різного роду сканери безпеки. Метою зазначених процесів є фіксація факту використання уразливості даної системи, протягом короткого періоду часу після виявлення стандартних процедур сканування однієї із підсистем. Дана ознака може бути свідченням про присутність несанкціонованих дій в системі.

Невідповідні параметри мережного трафіка - характерною ознакою атаки на інформаційну систему, можуть виступати порушення стандартних технічних характеристик мережного трафіка. Порушення встановлених технічних процесів системи - ознака НСД.

Параметри вхідного трафіка.

Найбільш яскравим прикладом ознаки атаки на інформаційні ресурси системи є ідентифікація вхідних ззовні в локальну мережу інформаційних пакетів даних, що мають адресу джерела повідомлень, яка відповідає діапазону адрес внутрішньої мережі. В даному випадку, якщо система виявлення атак або інший засіб розмежування доступу (міжмережний екран або маршрутизатор) не може визначити чи контролювати напрямок трафіка, то можлива реалізація так званої атаки типу "підміна адреси" ("address spoofing").

Параметри вихідного трафіка.

Ознакою НСД є вихідні з локальної мережі пакети даних, що містять в собі адресу джерела повідомлення, яка відповідає діапазону адрес зовнішньої мережі. Однак, у цьому випадку внутрішній порушник замаскує свої дії таким чином, щоб інформаційний пакет даних містив в собі адресу із зовнішньої мережі. Даний тип атаки визначається, як процедура маскування адреси повідомлення.

Непередбачені адреси інформаційних пакетів

Ознакою атаки у цьому випадку, можуть служити інформаційні пакети даних з непередбаченим адресою джерела (або портом одержувача для протоколів на базі TCP/UDP). Першим прикладом можна назвати виявлення пакета, що надійшов із зовнішньої мережі з недоступним або неможливим для, зовнішньої мережі IP-адресою. Наприклад, існують

адреси, які не маршрутизуються в глобальній або корпоративній мережі. Крім зазначених категорій адрес, існує певний ряд не стандартних діапазонів адрес, для яких інформаційні пакети не можуть з'являтися у мережі ззовні.

Наступним прикладом методу непередбачених адрес є атака Land, у якій адреса й порт джерела збігаються з адресою й портом одержувача . Вплив такого пакета при обробці даних приводить до зациклення роботи процесора або програмного забезпечення.

Другий приклад стосується запитів на з'єднання по протоколу Telnet від невідомого вузла або від вузла, з яким відсутні довірені відносини. Класичним прикладом реалізації методу непередбачених адрес є - виявлення невідповідності MAC- і IP-адрес мережних пакетів.

Непередбачені параметри мережних пакетів

Можна назвати безліч прикладів атак з непередбаченими параметрами мережних пакетів. Ймовірність реалізації таких атак дуже висока, тому що порушник використовує уразливості в реалізації стека протоколу TCP/IP у різних ОС. Наприклад, якщо виявлено мережний пакет із установленими бітами SYN й інформаційним повідомленням (другий етап установлення віртуального TCP-з'єднання), і при цьому не було ніякого попереднього пакета з бітиами SYN (перший етап установлення віртуального TCP-з'єднання), те це може приховувати під собою несанкціоноване вторгнення.

Інформаційний пакет даних, що не відповідає стандартам RFC, може привести до виходу з ладу комунікаційного устаткування. До такого устаткування відносяться не тільки маршрутизатори або комутатори мережі, але й засоби захисту інформації й безпосередньо системи виявлення атак. Велика кількість мережних атак використають заборонені комбінації TCP-прапорів у мережних пакетах. Деякі комбінації приводять до виходу з ладу вузла, що здійснює обробку таких пакетів, а завдяки іншим комбінаціям інші пакети залишаються не замічеными деякими системами виявлення атак або міжмережними екранами.

Заборонені комбінації можна виявити на базі наступних ознак.

- Можливість поєднання у одному пакеті команд SYN + FIN, оскільки це два взаємовиключних прапори. Перший установлює з'єднання, а другий завершує його. Багато систем виявлення атак відслідковують подібні комбінації прапорів. Але додавання ще одного прапора до даної комбінації приводить до того, що деякі системи виявлення атак не розпізнають видозмінене сканування.
- TCp-пакети ніколи не повинні містити тільки один прапор FIN. Звичайно один установлений прапор FIN свідчить про схований (stealth) FIN-скануванні.
- TCp-пакети повинні мати хоча б один прапор (але не FIN).

Характерною ознакою атаки може служити розмір мережних пакетів, що відрізняється від стандартного. Наприклад, більшість запитів ICMP Echo Request мають 8-байтовый заголовок й 56-байтовое поле даних. З появою в мережі пакетів нестандартної довжини, можна говорити про присутність несанкціонованої діяльності.

Ще однією класичною ознакою, що дозволяє в більшості випадків розпізнати атаку, може бути поява в мережі фрагментованих пакетів. Багато засобів мережної безпеки не вміють правильно збирати фрагментовані пакети, що приводить або до виходу цих засобів з ладу або до пропуску таких пакетів усередину захищеної мережі.

Непередбачені атрибути профілю системи

Запити будь-якої системи, мережі або користувача характеризуються деякими атрибутами, які описують так званий профіль системи, мережі або користувача. Такі профілі використаються для спостереження й аналізу контрольованого суб'єкта інформаційної діяльності. Найбільше що часто зустрічаються параметри, які допомагають виявити потенційну атаку на базі виявлення порушень політики безпеки.

Непояснені проблеми

До числа таких непояснених проблем можна віднести наступні приклади ознак: проблеми із програмним й апаратним забезпеченням (вихід з ладу маршрутизатора, перезавантаження сервера або неможливість запуску системних послуг); проблеми із системними ресурсами; проблеми із продуктивністю системи, тощо

Аудит системи виявлення атак. Журнали реєстрації

Аудит системи виявлення атак – класичний метод виявлення та регістрації порушень політики безпеки. Особливість цього методу в тім, що він є незамінним тоді, коли не існує можливості застосувати інші методи виявлення атак. У журналах реєстрації згідно процедурі аудиту, фіксуються різного роду події.

На даний час існують певні види журналів реєстрації найбільш типових компонентів інформаційної системи, а саме журнали реєстрації:

- комунікаційного встаткування (на прикладі маршрутизаторів Cisco;
- операційної системи (на прикладі Windows NT);
- міжмережних екранів (на прикладі Check Point Firewall-1);
- Web-сервера (на прикладі Apache);
- мережного аналізатора (на прикладі TCPdump);
- системи виявлення атак (на прикладі RealSecure).

Мережний трафік

Мережний трафік є одним з основних джерел інформації, що використовується системами виявлення атак, для здійснення ними аналізу й ідентифікації відповідних ознак НСД. Мережний трафік, як ознаковий простір атаки, складається з інформаційних ознак переданих мережних пакетів (кадрів, фреймів) різних мережних архитектур. Однак, за одиницю інформаційної ознаки мережного трафіка приймемо пакет, що у загальному випадку складається із трьох частин:

- заголовка пакета (службової інформації, адреси джерела й призначення й інших полів);
- поля даних пакета;
- кінцівки пакета (контрольної суми, обмежника й т.д.).

На підставі аналізу зазначених трьох частин мережного пакета, система виявлення атак може ухвалювати рішення щодо присутності або відсутності порушення політики безпеки.

Зазначене джерело ознак відбиває всі дії, виконувані суб'єктами контрольованої системи (користувачами, процесами й т.д.) у реальному режимі часу. Ці дії можна також аналізувати на основі журналів реєстрації.

Етапи процесу виявлення атак

Перший етап реалізації процесу виявлення атак - *це збір інформації про атакуючу систему та її параметри*. Він включає такі дії як, визначення мережної топології, типу й версії операційної системи вузла, що атакує, а також належність доступних мережних й інших сервісів і т.п. Ці дії реалізуються різними методами.

Другий етап - *вивчення оточення*. На цьому етапі порушник досліджує мережну інфраструктуру з урахуванням подальшої реалізації передбаченої загрози. До аналізу областей мережної інфраструктури, ставляться відносяться: серверний простір Internet-провайдера або вузли вилученого офісу компанії, що підлягає атаці. На цьому етапі порушник визначає адреси авторизованих користувачів, власників інформаційних ресурсів системи, авторизовані процеси ІС, тощо. Такі дії досить важко виявити, оскільки вони виконуються протягом досить тривалого періоду часу з зовнішньої області, що контрольована засобами захисту (міжмережними екранами, системами виявлення атак і т.п.).

Третій етап - *ідентифікація топології мережі*. Можна назвати два методи визначення топології мережі (network topology detection), використовуваних зловмисниками: "зміна TTL" ("TTL modulation") і "запис маршруту" ("record route"). Програми traceroute для Unix й tracert для Windows використають перший спосіб визначення топології мережі. Вони використають

для цього поле Time to Live ("час життя") у заголовку IP-пакета, що змінюється залежно від числа пройдених мережним пакетом маршрутизаторів. Також, використання утиліти ping, може бути використано для запису маршруту ICMP-пакета. Найбільш поширеним методом виявлення мережної топології є з'ясування мережного протоколу SNMP, установленого на багатьох мережних пристроях, захист яких невірно сконфігуровано. За допомогою протоколу RIP можна спробувати одержати інформацію про таблицю маршрутизації в мережі й т.д. Багато хто із цих методів використаються сучасними системами керування (наприклад, HP OpenView, Cabletron SPECTRUM, MS Visio і т.д.) для побудови карт мережі [2, 4].

Четвертий етап - ідентифікація вузлів. Ідентифікація вузла (host detection), як правило, здійснюється шляхом посилки за допомогою утиліти ping команди ECHO_REQUEST протоколу ICMP. Відповідне повідомлення ECHO_REPLY говорить про те, що вузол доступний. Існують вільно розповсюджувані програми, які автоматизують і прискорюють процес паралельної ідентифікації великої кількості вузлів, наприклад: fping або nmap. Недоліки даного методу в тім, що стандартними засобами вузла запити ECHO_REQUEST не фіксуються. Для цього необхідно застосовувати засоби аналізу трафіка, міжмережні екрани або системи виявлення атак. Це найпростіший метод ідентифікації вузлів. Наступними недоліками є те, що : по-перше, багато мережних пристроїв і програми блокують ICMP-пакети й не пропускають їх у внутрішню мережу (або навпаки не пропускають їх назовні). Наприклад, MS Proxy Server 2.0 не дозволяє проходження пакетів по протоколі ICMP. У результаті виникає неповна картина. З іншого боку, блокування ICMP-пакета говорить зловмисникові про наявність "першої черги захисту" – наявність марщрутизаторів, міжмережних екранів і т.д. По-друге, використання ICMP-запитів дозволяє з легкістю виявити їхнє джерело, що, зрозуміло, не може входити до завдання зловмисника.

Класичним методом ідентифікації вузлів мережі є так називана розвідка DNS, що дозволяє ідентифікувати вузли корпоративної мережі за допомогою звертання до сервера служби імен авторизованих користувачів.

П'ятий етап - ідентифікація сервисів або сканування портів. Ідентифікація сервісів (service detection), як правило, здійснюється шляхом виявлення відкритих портів (port scanning). Такі порти дуже часто пов'язані із сервісом системи, заснованим на протоколах TCP або UDP. Наприклад, відкритий 80-й порт має на увазі наявність Web-сервера, 25-й порт - поштового SMTP-сервера, 12346 - серверної частини троянського коня NetBus і т.д. Для ідентифікації сервісів і сканування портів можуть бути використані різні програми, у т.ч. і вільно розповсюджувані. Наприклад, nmap або netcat.

Шостий етап - ідентифікація операційної системи. Основний механізм вилученого визначення ОС (OS detection) - аналіз відповідей на запити, що враховують різні реалізації TCP/IP-стека в різних операційних системах. У кожної ОС по-своєму реалізований стек протоколів TCP/IP, що дозволяє за допомогою спеціально запитів і відповідей на них визначити, яка ОС установлена на вилученому вузлі [2,3,4].

Сьомий етап - визначення уразливостей вузла. Останній крок - пошук уразливостей (searching vulnerabilities). На цьому кроці зловмисник за допомогою різних автоматизованих засобів або вручну визначає уразливості, які можуть бути використані для реалізації атаки. Прикладом таких автоматизованих засобів можуть бути використані Shadow Security Scanner, nmap, Retina програми і т.д.

Восьмий етап - реалізація атаки. Із цього моменту починається спроба доступу до атакуючого вузлу. При цьому доступ може бути як безпосередній, тобто проникнення на вузол, так й опосередкований, наприклад, при реалізації атаки типу "відмова в обслуговуванні". Реалізація атак у випадку безпосереднього доступу також може бути розділена на два етапи: *проникнення та встановлення контролю за системою.*

Проникнення - має на увазі під собою подолання засобів захисту периметра (наприклад: міжмережного екрана). Реалізовується цей процес з урахуванням використання уразливості сервісу системи, шляхом передачі прихованого змісту по електронній пошті (макровіруси)

або через аплети Java, тощо. Даний зміст може організовувати так називані «дири» або «тунелі» у міжмережному екрануванні, через які проникає порушник. До цього ж етапу можна віднести підбор пароля адміністратора системи або іншого авторизованного користувача за допомогою спеціалізованої утиліти (наприклад Crack).

Установлення контролю над системою - після проникнення зловмисник установлює контроль над атакуючим вузлом. Зазначена процедура здійснюється шляхом впровадження програми типу "троянський кінь" (наприклад, NetBus або BackOrifice). Після установки контролю над потрібним вузлом, порушник може здійснювати всі необхідні несанкціоновані дії дистанційно без відома власника інформаційних ресурсів атакованої інформаційної системи. Встановлення контролю над вузлом корпоративної мережі повинне зберігатися й після перезавантаження операційної системи. Даний процес може бути реалізовано шляхом заміни одного із завантажувальних файлів або впровадження вставки посилання на ворожий код у файли автозавантаження або системний реєстр.

Дев'ятий етап - завершення атаки. Етапом завершення атаки є приховування несанкціонованих дії з боку зловмисника. Реалізується дана дія, шляхом видалення відповідних записів з журналів реєстрації й інших дій, що повертають атаковану систему у початковий (з точки зору зовнішньої інформативності показників) стан (Рис.2).

Ідентифікація атак

Підсистема ідентифікації атак є найважливішим компонентом у будь-якій системі виявлення НСД . Ефективність роботи всієї інформаційної системи безпосередньо залежить від цих процесів та у загальному випадку використає три широко відомих методи для розпізнавання атак [4,5].

- *Сигнатурний метод, заснований на використанні шаблонів сигнатур (pattern-based signatures),* що характеризують атаку або іншу підозрілу діяльність. Дані сигнатури містять деякі ключові слова або вирази, виявлення яких і свідчить про атаку. Наприклад, фрагмент "cwd root" в FTP-сеансі однозначно визначає факт обходу механізму аутентифікації на FTP-сервері й спробі перейти в кореневий каталог FTP-сервера. Іншим прикладом є виявлення аплетів Java у мережному трафіку на основі шістнадцятирічного фрагмента "CA FE BA BE". Зазначені сигнатури дозволяють виявляти приховані НСД типу -троянських коней, якщо останні використають стандартні значення портів.
- *Сигнатурний метод, заснований на контролі частоти подій або перевищенні граничної величини.* Дані сигнатури описують ситуації, коли протягом деякого інтервалу часу відбуваються події, число яких перевищує задані заздалегідь показники. Прикладом такої сигнатури є виявлення сканування портів або виявлення атаки SYN Flood. У першому випадку граничним значенням є число портів, що просканово в одиницю часу. У другому випадку - число спроб установлення віртуального з'єднання з вузлом за одиницю часу.
- *Виявлення аномалій.* Даний сигнатур метод дозволяє виявляти події, що відрізняються від попередньо заданих характеристик стандартної роботи інформаційної системи.

Висновки

На базі проведених досліджень, щодо аналізу сучасних методів реалізації загроз інформаційним ресурсам в ІКСМ, виявлено характерні ознаки реалізації різного класу атак. На основі проведеного аналізу визначено основні методи і засоби виявлення існуючих загроз інформаційним ресурсам.

На стадії вторгнення виявлення атак можливе за допомогою як сигнатурних, так і поведінкових методів. Будь-яке вторгнення характеризується певними ознаками, які, з одного боку, можна представити у вигляді сигнатури, а з іншої – описати, як деяке відхилення від штатної поведінки інформаційної системи.

Список літератури

1. *Лукацкий А.* Обнаружение атак. — СПб.: БХВ-Петербург, 2001. — 624 с.
2. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. – М.: Горячая линия – Телеком, 2004. – 280 с.

3. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративних сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

4. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. — СПб.: «Наука и техника», 2004. — 384 с.

5. Юдін О.К. Захист інформації в мережах передачі даних / О.К.Юдін, Г.Ф. Конахович, О.Г. Корченко // Підручник МОН України. – К.: Видавництво *DIRECTLINE*, 2009.-714с., іл.

Надійшла 20.01.2010

УДК 004.056.55(043.2) **Стасюк А.И., Корченко А.А., Малофеев А.В.**

ИСПОЛЬЗОВАНИЕ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ ДЛЯ ВЫБОРА КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ШИФРОВАНИЯ

На сегодняшний день существует большое количество различных алгоритмов шифрования. Каждый из них имеет индивидуальные характеристики, такие как количество раундов, длинна ключа, сложность реализации и другие. Поэтому часто, при построении систем защиты информации, возникает проблема выбора криптографического алгоритма отвечающего определенным критериям.

Одним из общепринятых подходов при построении криптосистем в настоящее время является выбор понравившегося разработчикам алгоритма по одному из критериев, например криптостойкость и реализация этого шифроалгоритма без учета других характеристик. Такой однокритериальный подход не всегда является целесообразным и оправданным. В результате недостаточного или некачественного учета других факторов возможно создание нестойких криптосистем. Поэтому необходим другой синтетический многокритериальный подход.

В [6] автор приводит математический аппарат, который позволяет осуществить выбор алгоритма шифрования. Но автор учитывает немногочисленные критерии алгоритмов, в частности длину ключа. В [4] приведено сравнение алгоритмов относительно большого количества характеристик, выделены их слабые и сильные стороны. Однако автор не предоставляет инструменты выбора криптографического алгоритма по заданным критериям. Это важно при построении аппаратных или программных средств криптографической защиты информации.

В этой связи целью данной работы является разработка методики выбора алгоритма шифрования для средств защиты. Очевидно, что такие алгоритмы должны наиболее полно обеспечивать криптостойкость, производительность и эффективность реализации [2]. Однако удовлетворение наилучшим образом, приведенным требованиям, зачастую носит противоречивый и нечеткий характер. Поэтому для решения многокритериальной задачи выбора алгоритма шифрования использована теория нечетких множеств. В [1, 5] рассматривается соответственный математический аппарат, используемый в методах оценки альтернатив.

В данном случае критерии определяют некоторые свойства алгоритмов шифрования, а оценки альтернатив представляют собой степень соответствия этим свойствам. Таким образом, имеется множество альтернатив (алгоритмов шифрования) $X=\{x_1,...x_m\}$ (где x_i ($i=\overline{1,m}$) алгоритм шифрования, m ($m=\overline{1,k}$) – количество алгоритмов шифрования) и множество критериев (параметров алгоритмов шифрования) $Y=\{y_1,...y_n\}$ (где y_j ($j=\overline{1,n}$) критерий алгоритма, n ($n=\overline{1,s}$) – количество критериев) при этом оценки альтернатив по каждому j-му критерию представлены нечеткими множествами: